



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

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
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 .
<code>Computer code</code>	Indicates sample code or text to be typed at a command line.
<code><Computer code italic></code>	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 <code>serialnumber=<your serial number></code> , replace the variable and brackets with the serial number from your device: <code>serialnumber=C0ABC00000321</code> .
<i>Italic</i>	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.

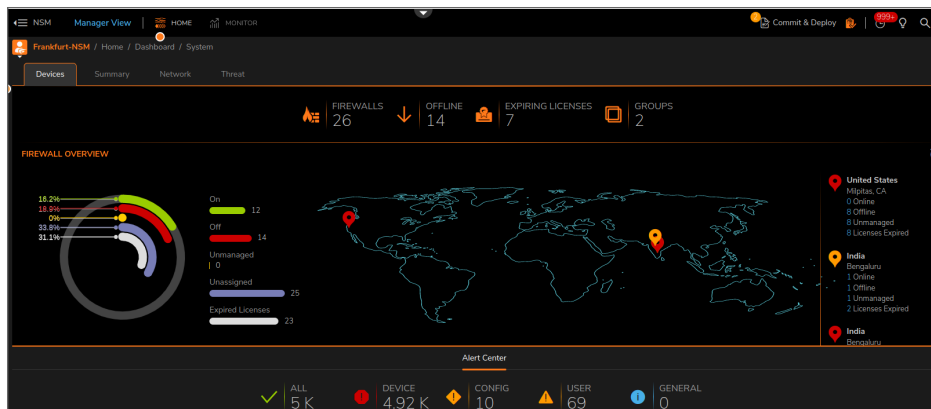
Related Documents

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**.

#	NAME	SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY	CONFIGURATION
1	Dirty-NSV270-172.20.0...	0040103534AF	Unassigned	NSV 270		Offline	Unmanaged
2	NSV-172.20.0.245	00401039D171	Unassigned	NSV 270		Online	Managed
3	Nsv200-172.20.0.141	004010366205	Unassigned	NSV 200	IC	Online	Managed
4	NSV200-172.20.0.189	0040103661DD	Unassigned	NSV 200		Online	Managed
5	NSV200-172.20.0.228	004010391171	Unassigned	NSV 200		Online	Managed
6	Nsv200-172.20.0.90	0040108261C3	Unassigned	NSV 200	IC	Offline	Unmanaged
7	T2300-172.20.1.60	1BB1698FA1EC	Unassigned	T2 300	IC	Online	Managed
8	T2300-172.20.1.85	1BB1698F133C	Unassigned	T2 300	IC	Online	Managed
9	T2300p-172.20.1.78	2CB8ED21AF68	Unassigned	T2 300P		Online	Managed

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.

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.

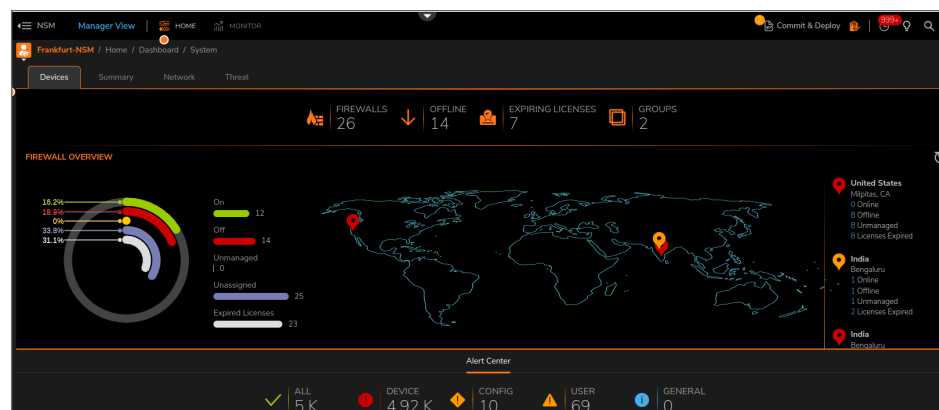
Dashboard enables you to visualize status of the security infrastructure, assess the performances, and monitor the issues that need investigation, at a glance. The analytical dashboard NSM provides is an optimal solution to quickly analyze the cyber security risks and recognize how to resolve them.

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.

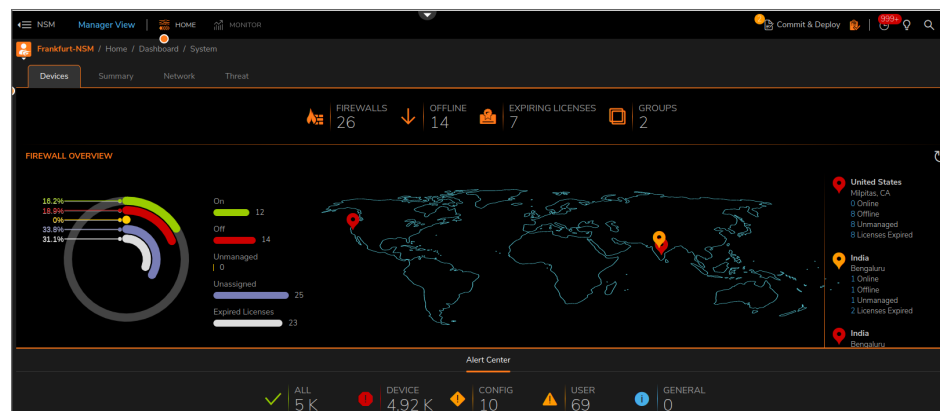
The **Summary** tab shows Traffic Distribution, Top Users, Observed Threats, and Top Devices by Sessions in your network infrastructure for the period selected in the slider at the top. It also shows the Insights section giving information about the number of infected hosts and the number of critical 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.

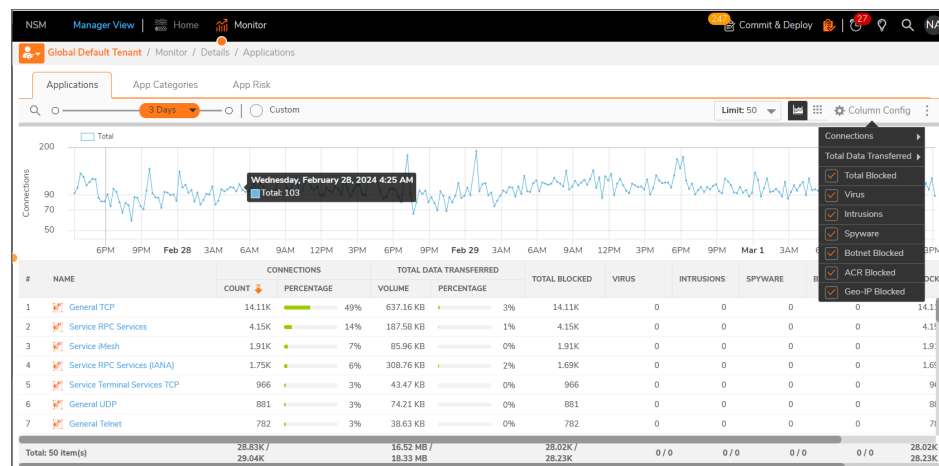
In case of NSM Advance firewalls, the slider will have option from 1 hour to 365 days.

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.

① | **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.



Group and Tenant Reporting

Group and Tenant reporting offers you additional ways in which to combine or filter data so you can learn 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 you 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:

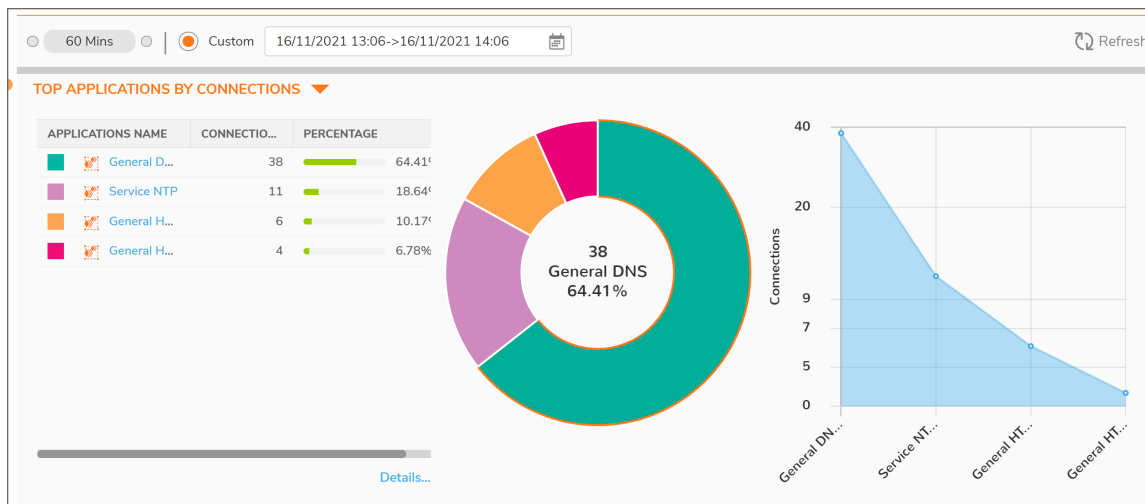
- [Understanding How the NSM License Affects Reporting](#)
- [Navigating Reports](#)
- [Tenant Reports](#)
- [Group Reports](#)
- [Custom Reports](#)

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

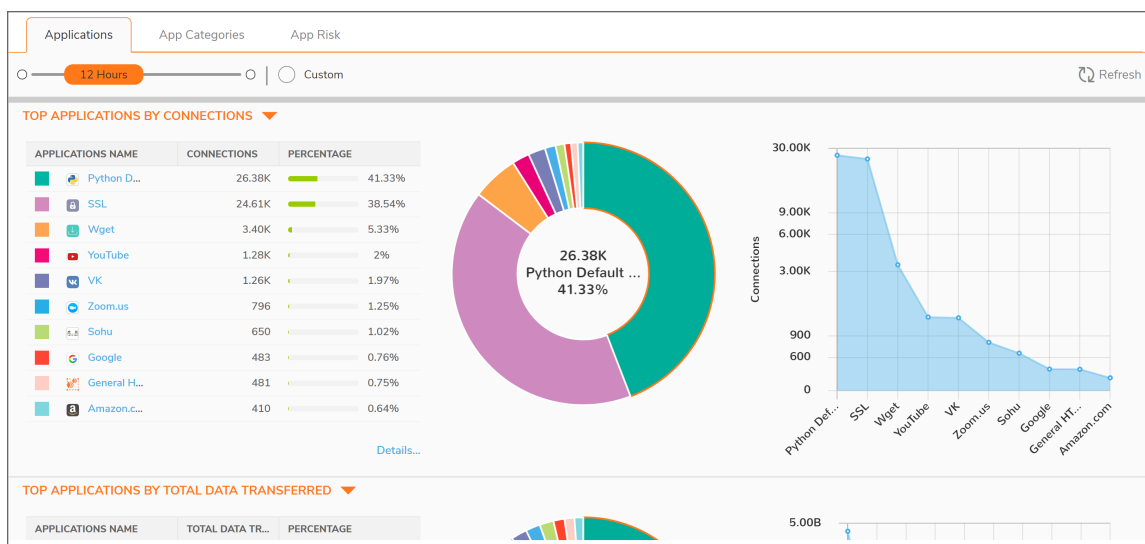
When you have a firewall with an Essential license, only the most basic reporting coverage is provided.



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:

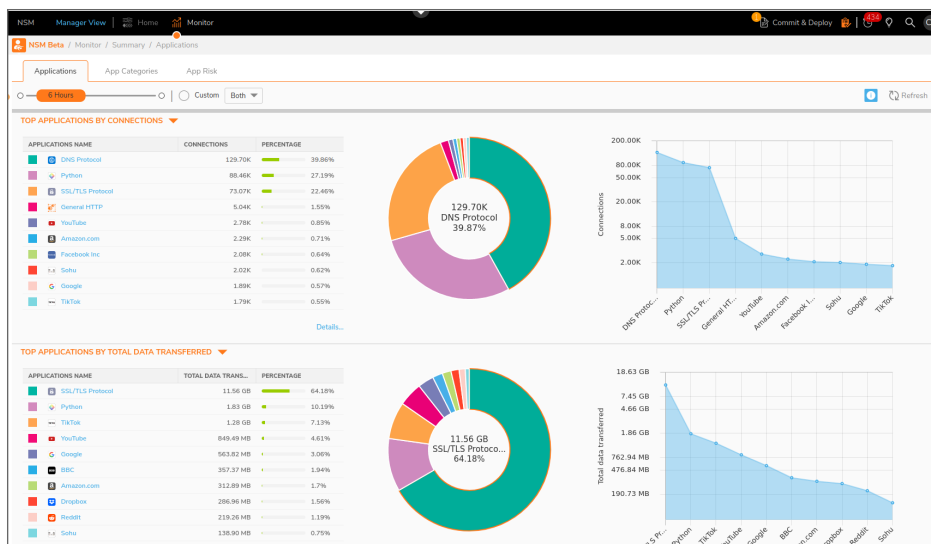
1. Click the tenant name at the top and select the tenant you want to see reporting for. If you have a long list of tenants, you can type a string in the search field to filter the list.
2. Select the **Monitor** option at the top.

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.



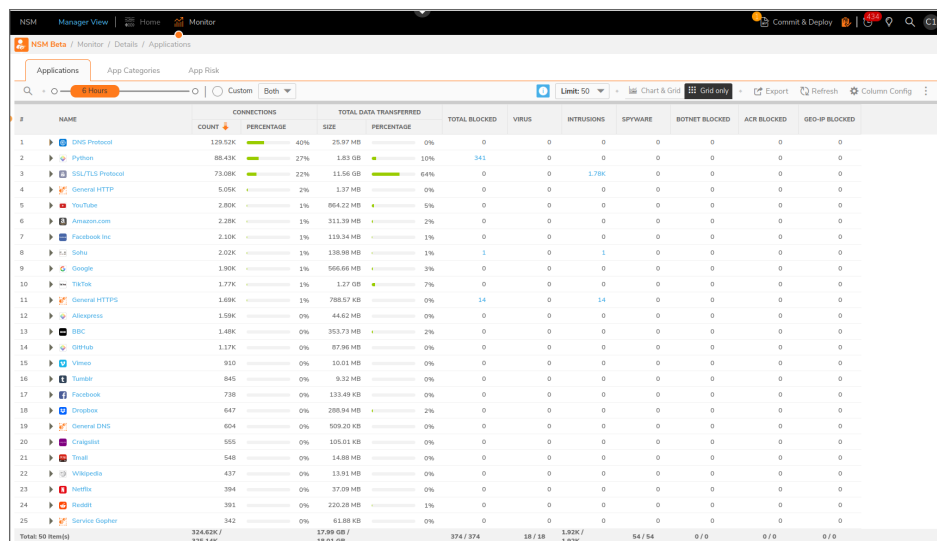
Run your mouse over the graphs. As it runs over an option in the chart or a data point in the graph, additional details pop up about that data. Some of the tables also have links in them that lead to more data. For example,

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.



#	NAME	COUNT	PERCENTAGE	SIZE	PERCENTAGE	TOTAL DATA TRANSFERRED	TOTAL BLOCKED	VIRUS	INTRUSIONS	SPYWARE	BOTNET BLOCKED	ACR BLOCKED	GEO-IP BLOCKED
1	CHS Protocol	129.52K	40%	25.97 MB	0%	0	0	0	0	0	0	0	0
2	Python	86.43K	27%	1.83 GB	10%	343	0	0	0	0	0	0	0
3	SSL/TLS Protocol	75.08K	22%	11.56 GB	64%	0	0	0	1,78K	0	0	0	0
4	General HTTP	5.05K	2%	1.37 MB	0%	0	0	0	0	0	0	0	0
5	YouTube	2.80K	1%	864.22 MB	5%	0	0	0	0	0	0	0	0
6	Amazon.com	2.38K	1%	111.39 MB	2%	0	0	0	0	0	0	0	0
7	Facebook Inc	2.10K	1%	119.34 MB	1%	0	0	0	0	0	0	0	0
8	Self	2.02K	1%	136.98 MB	1%	1	0	0	1	0	0	0	0
9	Google	1.90K	1%	566.66 MB	3%	0	0	0	0	0	0	0	0
10	TikTok	1.77K	1%	1.27 GB	7%	0	0	0	0	0	0	0	0
11	General HTTPS	1.69K	1%	788.57 KB	0%	14	0	0	14	0	0	0	0
12	Allegiance	1.59K	0%	44.62 MB	0%	0	0	0	0	0	0	0	0
13	BBC	1.48K	0%	353.73 MB	2%	0	0	0	0	0	0	0	0
14	GitHub	1.17K	0%	87.96 MB	0%	0	0	0	0	0	0	0	0
15	Vimeo	910	0%	10.01 MB	0%	0	0	0	0	0	0	0	0
16	Tumblr	845	0%	9.32 MB	0%	0	0	0	0	0	0	0	0
17	Facebook	738	0%	133.49 KB	0%	0	0	0	0	0	0	0	0
18	Dropbox	647	0%	288.94 MB	2%	0	0	0	0	0	0	0	0
19	General DNS	604	0%	509.20 KB	0%	0	0	0	0	0	0	0	0
20	Craigslist	555	0%	105.01 KB	0%	0	0	0	0	0	0	0	0
21	Twitter	548	0%	14.88 MB	0%	0	0	0	0	0	0	0	0
22	Wikipedia	437	0%	13.91 MB	0%	0	0	0	0	0	0	0	0
23	Netflix	394	0%	37.09 MB	0%	0	0	0	0	0	0	0	0
24	Reddit	391	0%	220.28 MB	1%	0	0	0	0	0	0	0	0
25	Service Grapher	342	0%	61.88 KB	0%	0	0	0	0	0	0	0	0
Total: 50 Item(s)		324.82K / 326.14K		37.89 GB / 18.61 GB		374 / 374	18 / 18	1,92K / 1,92K	64 / 64	0 / 0	0 / 0	0 / 0	0 / 0

❗ | **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.

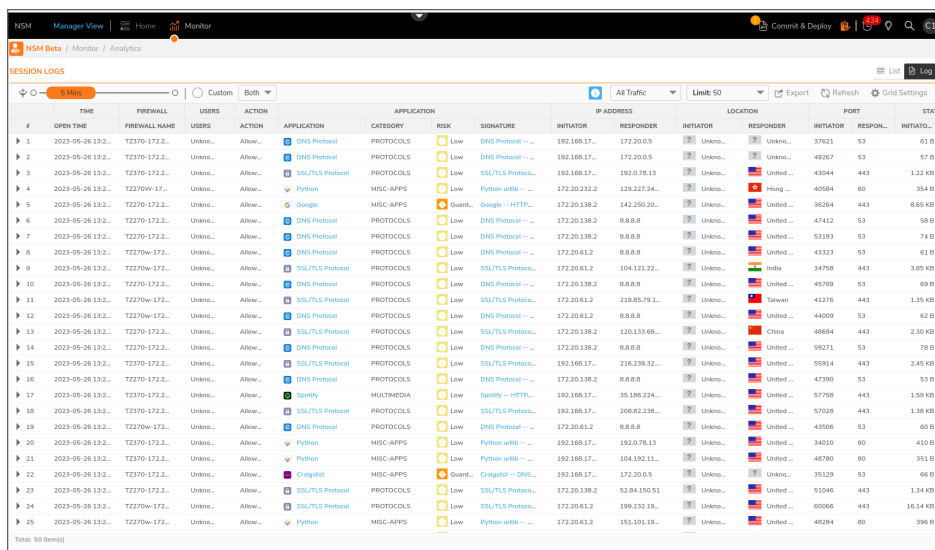
❗ | **NOTE:** The drill-down to session logs, or Analytics, is not available for firewalls with the Essential License.

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.

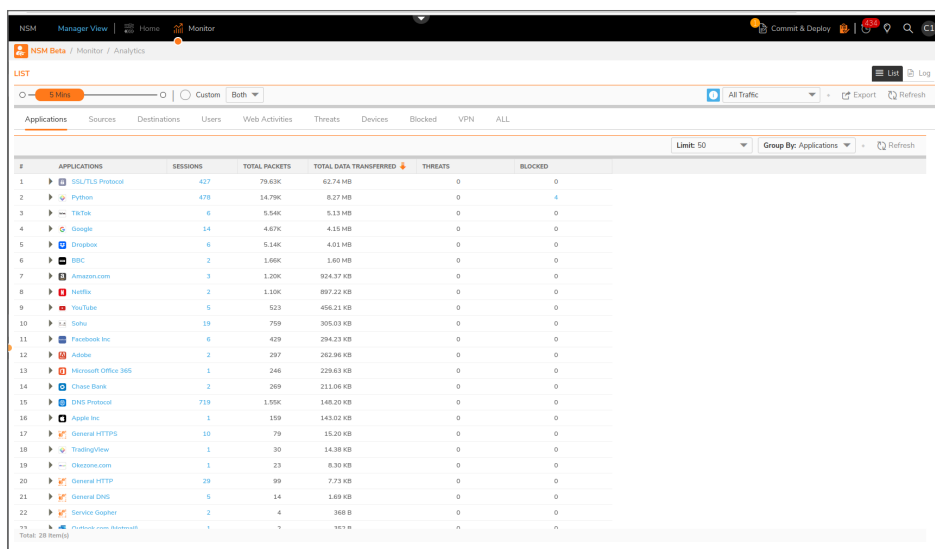
To navigate to the tenant analytics:

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 screenshot shows the NSM Monitor Analytics page. The interface includes a top navigation bar with 'NSM Beta', 'Monitor', and 'Analytics' tabs. Below the navigation bar, there are filters for 'All Traffic', 'Limit 50', and buttons for 'Export', 'Refresh', and 'Grid Settings'. The main table displays session logs with columns: #, OPEN TIME, FIREWALL, USERS, ACTION, APPLICATION, CATEGORY, RISK, SIGNATURE, INITIATOR, IP ADDRESS, RESPONDER, LOCATION, RESPONDER, INITIATOR, PORT, RESPONDER, and STATUS. The table contains 25 rows of data, each representing a network session with details like timestamps, firewall names, user actions, application categories, risk levels, signatures, and IP addresses.

#	OPEN TIME	FIREWALL	USERS	ACTION	APPLICATION	CATEGORY	RISK	SIGNATURE	INITIATOR	IP ADDRESS	RESPONDER	LOCATION	RESPONDER	INITIATOR	PORT	RESPONDER	STATUS
1	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	192.168.17...	172.20.0.5	Unknown...	Unknown...	Unknown...	37621	53	61 B	
2	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	192.168.17...	172.20.0.5	Unknown...	Unknown...	Unknown...	49267	53	57 B	
3	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	192.168.17...	192.0.78.13	Unknown...	Unknown...	Unknown...	43044	443	1.22 KB	
4	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	Python	MISC-APPS	Low	Python urllib -- ...	172.20.232.2	120.227.24...	Unknown...	Unknown...	Unknown...	40584	80	354 B	
5	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	Google	MISC-APPS	Low	Google -- HTTP...	172.20.138.2	142.250.20...	Unknown...	Unknown...	Unknown...	36264	443	8.65 KB	
6	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	47412	53	58 B	
7	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	53193	53	74 B	
8	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	43323	53	61 B	
9	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	172.20.138.2	104.121.22...	Unknown...	Unknown...	Unknown...	34758	443	3.05 KB	
10	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	45709	53	69 B	
11	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	172.20.138.2	219.85.79.1...	Unknown...	Unknown...	Unknown...	41276	443	1.35 KB	
12	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	44009	53	62 B	
13	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	172.20.138.2	120.133.69...	Unknown...	Unknown...	Unknown...	48694	443	2.30 KB	
14	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	59271	53	78 B	
15	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	192.168.17...	216.239.32...	Unknown...	Unknown...	Unknown...	55914	443	2.45 KB	
16	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	47390	53	53 B	
17	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	Spotify	MULTIMEDIA	Low	Spotify -- HTTP...	192.168.17...	35.186.224...	Unknown...	Unknown...	Unknown...	57758	443	1.59 KB	
18	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	192.168.17...	208.82.238...	Unknown...	Unknown...	Unknown...	57028	443	1.38 KB	
19	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	172.20.138.2	8.8.8.8	Unknown...	Unknown...	Unknown...	43506	53	60 B	
20	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	Python	MISC-APPS	Low	Python urllib -- ...	192.168.17...	192.0.78.13	Unknown...	Unknown...	Unknown...	34010	80	410 B	
21	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	Python	MISC-APPS	Low	Python urllib -- ...	192.168.17...	104.192.11...	Unknown...	Unknown...	Unknown...	48780	80	351 B	
22	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	Craigslist	MISC-APPS	Low	Craigslist -- DNS...	192.168.17...	172.20.0.5	Unknown...	Unknown...	Unknown...	35129	53	68 B	
23	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	172.20.138.2	52.84.150.51	Unknown...	Unknown...	Unknown...	51046	443	1.34 KB	
24	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	SSL/TLS Protocol	PROTOCOLS	Low	SSL/TLS Protocol -- ...	172.20.138.2	199.732.19...	Unknown...	Unknown...	Unknown...	60066	443	16.14 KB	
25	2023-05-26 13:2...	T2370-172.2...	Unknown...	Allow...	Python	MISC-APPS	Low	Python urllib -- ...	172.20.138.2	151.101.19...	Unknown...	Unknown...	Unknown...	48284	80	396 B	



The screenshot shows the NSM Monitor Applications page. The interface includes a top navigation bar with 'NSM Beta', 'Monitor', and 'Applications' tabs. Below the navigation bar, there are filters for 'All Traffic', 'Limit 50', and buttons for 'Export' and 'Refresh'. The main table displays applications with columns: #, APPLICATIONS, SESSIONS, TOTAL PACKETS, TOTAL DATA TRANSFERRED, THREATS, and BLOCKED. The table contains 22 rows of data, each representing an application with details like session counts, packet counts, data transfered, and threat/blocked status.

#	APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL DATA TRANSFERRED	THREATS	BLOCKED
1	SSL/TLS Protocol	427	79,63K	62.74 MB	0	0
2	Python	478	14,79K	8.27 MB	0	4
3	Netflix	6	5,54K	5.13 MB	0	0
4	Google	14	4,67K	4.15 MB	0	0
5	Dropbox	6	5,14K	4.01 MB	0	0
6	BBC	2	1,69K	1.60 MB	0	0
7	Amazon.com	3	1,20K	924.37 KB	0	0
8	Netflix	2	1,10K	897.22 KB	0	0
9	YouTube	5	523	456.21 KB	0	0
10	Spotify	19	759	305.03 KB	0	0
11	Facebook Inc	6	429	294.23 KB	0	0
12	Adobe	2	297	262.96 KB	0	0
13	Microsoft Office 365	1	246	229.63 KB	0	0
14	Chase Bank	2	269	211.06 KB	0	0
15	DNS Protocol	719	1,55K	146.20 KB	0	0
16	Apple Inc	1	159	143.82 KB	0	0
17	General HTTPS	10	79	15.20 KB	0	0
18	TradingView	1	30	14.38 KB	0	0
19	Chesapeake.com	1	23	8.30 KB	0	0
20	General HTTP	29	99	7.73 KB	0	0
21	General DNS	5	14	1.69 KB	0	0
22	Service Gopher	2	4	368 B	0	0

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:

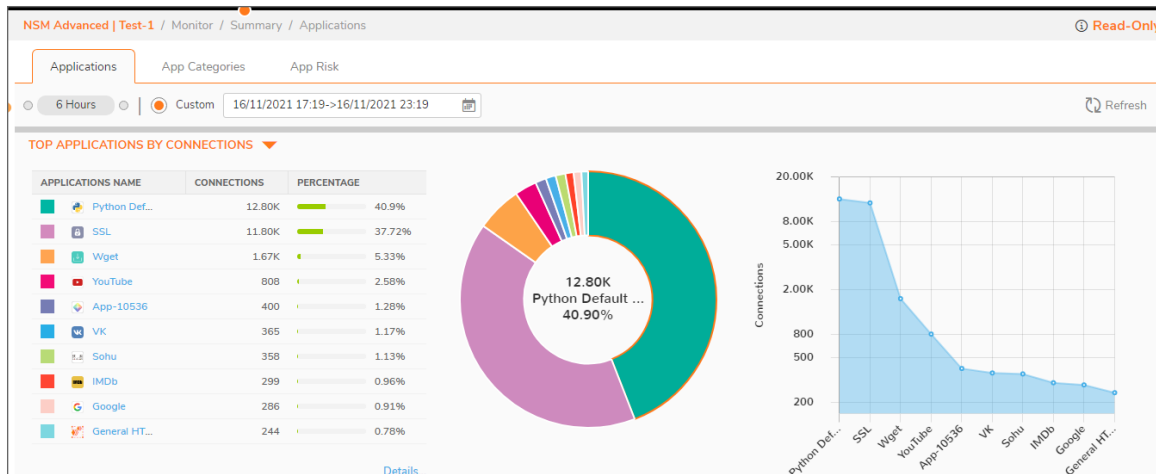
1. On the **Manager View** select **Home > Firewalls > Groups**.
2. Select the group you want to see the reports for.
3. Select the **Monitor** option at the top.

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.

NSM Advanced | Test-1 / Monitor / Details / Applications Read-Only

Applications App Categories App Risk

6 Hours Custom 16/11/2021 17:27->16/11/2021 23:27 Limit: 50 Chart & Grid Grid only Export Refresh Column Config

#	NAME	CONNECTIONS		TOTAL DATA TRANSFERRED		TOTAL BLOCKED	VIRUS	INTRUSIONS	SPYWARE	BOTNET BLOCKED
		COUNT	PERCENTAGE	SIZE	PERCENTAGE					
1	Python Default URL Library	12.87K	41%	132.00 MB	5%	16	0	0	0	0
2	SSL	11.81K	38%	1.88 GB	71%	0	0	0	0	0
3	Wiget	1.69K	5%	1.21 MB	0%	1.52K	0	1.50K	16	0
TRAFFIC DISTRIBUTION BY FIREWALL										
	Root Group	1.69K		1.21 MB		1.52K	0	1.50K	16	0
	Test-1	1.69K		1.21 MB		1.52K	0	1.50K	16	0
4	YouTube	842	3%	59.59 MB	2%	0	0	0	0	0
5	VK	401	1%	13.00 MB	0%	0	0	0	0	0
6	App-10536	399	1%	15.33 MB	1%	0	0	0	0	0
7	Sohu	358	1%	5.14 MB	0%	0	0	0	0	0
8	IMDb	299	1%	126.43 MB	5%	0	0	0	0	0
9	Google	265	1%	79.19 MB	3%	0	0	0	0	0

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.

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

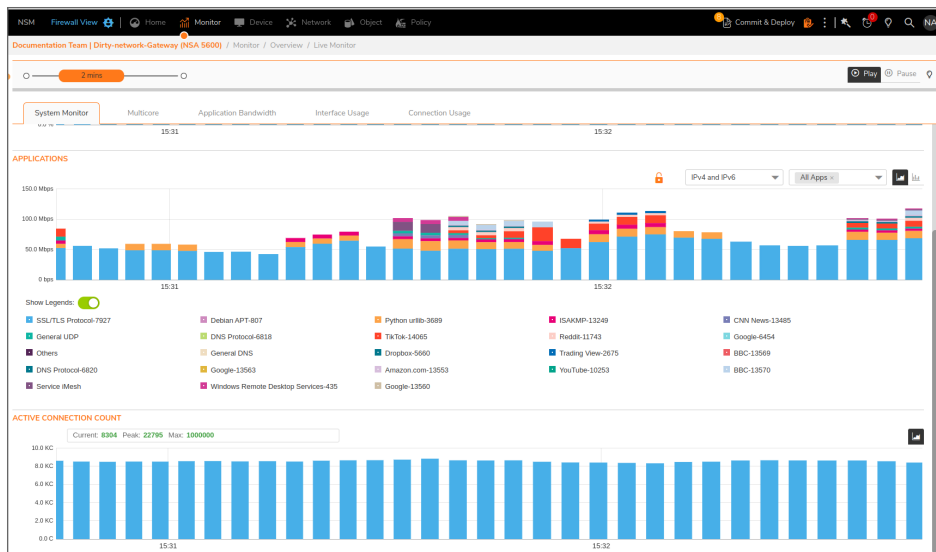
Live Monitor provides a real-time view of the packets forwarded by the firewall and is visible when viewing from individual firewalls. When you select Group View or Global View in the Device Manager, the Live Monitor option is not shown. The Live Monitor is always running, but it shows only the current 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:

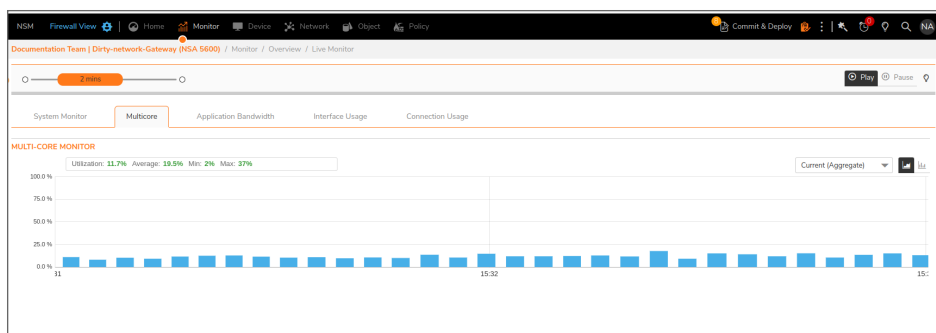
- **System Monitor**
- **Multi-Core Monitor**
- **Application Bandwidth**
- **Interface Usage**
- **Connection Usage**

① **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**.

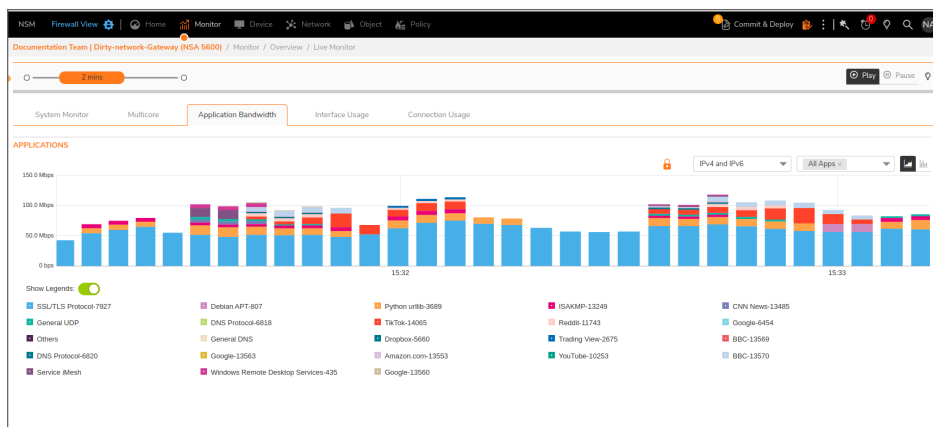
System Monitor



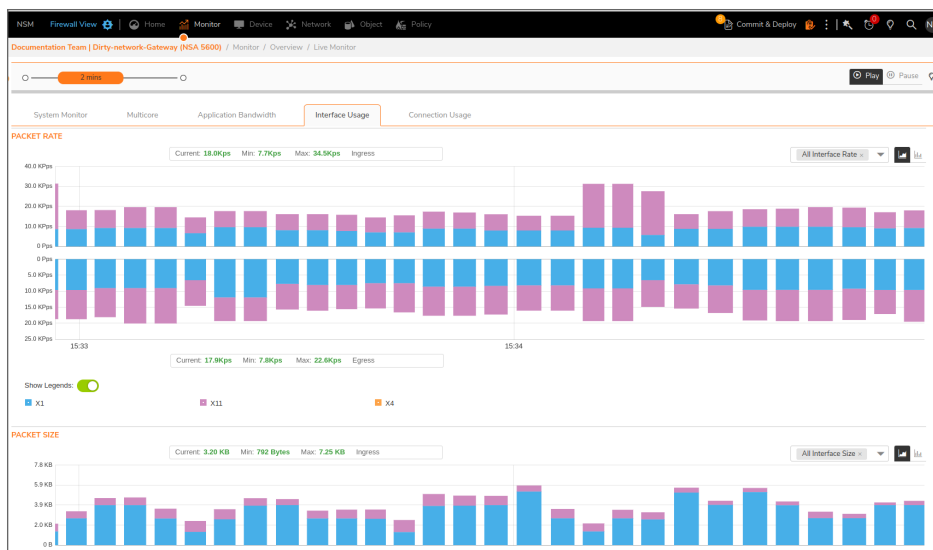
Multi-Core Monitor



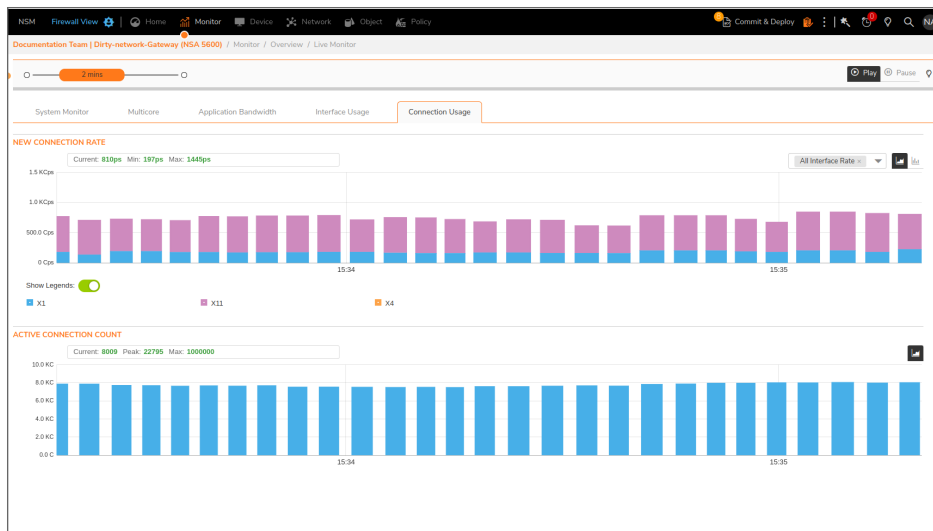
Application Bandwidth



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.

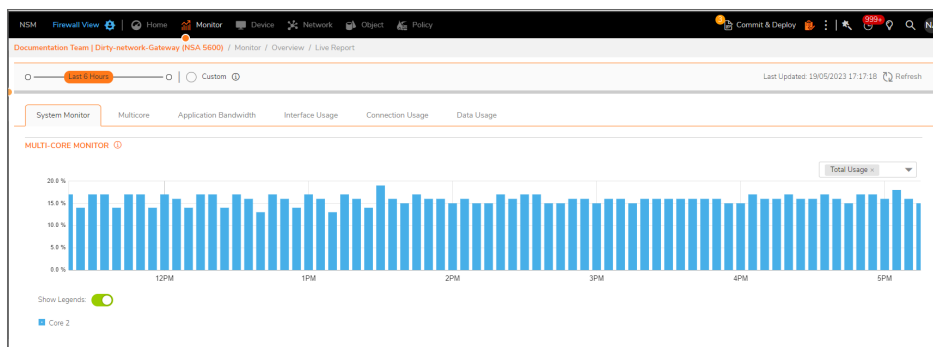
Mouse over a data point to see values at that instant. Select Start Time and End Time in the chart and click Refresh icon to get drill-down data for that particular time.

The following reports are shown in Live Report:

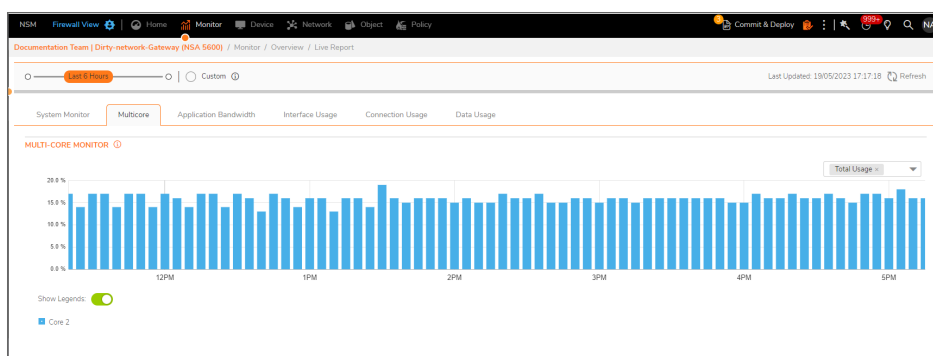
- **System**
- **Multi-Core**
- **Application Bandwidth**
- **Interface Usage**
- **Connection Usage**
- **Data Usage**

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**.

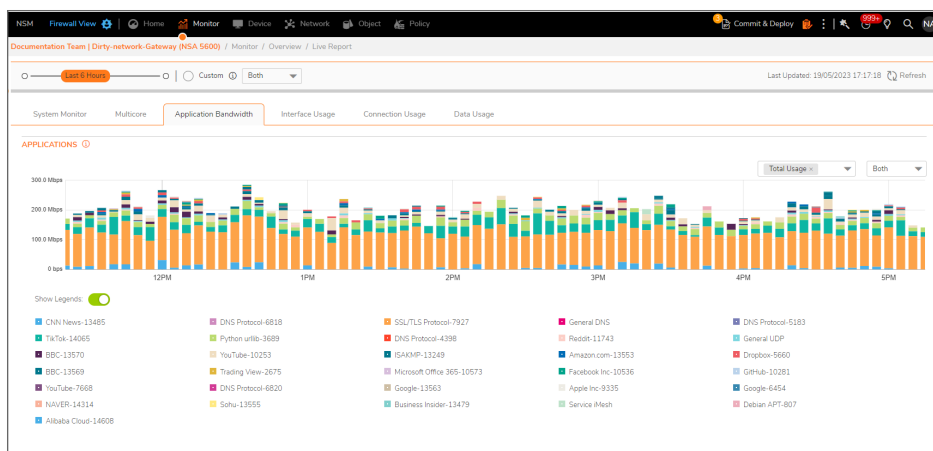
System



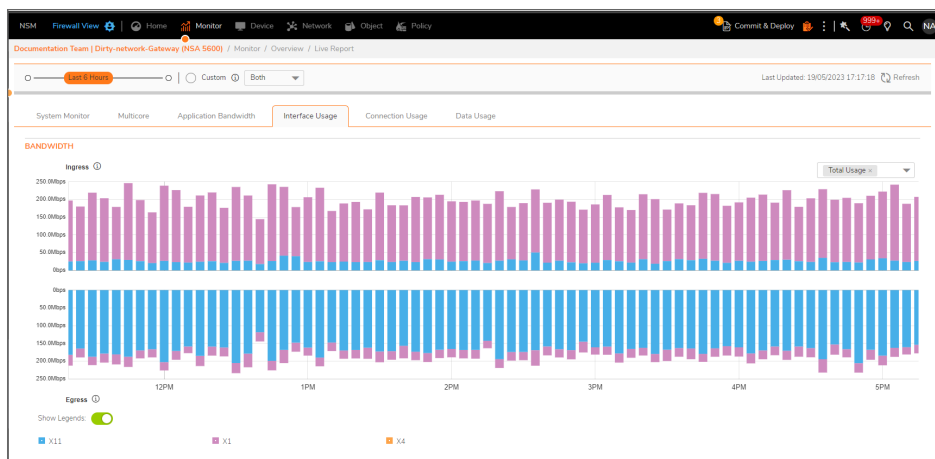
Multi-Core



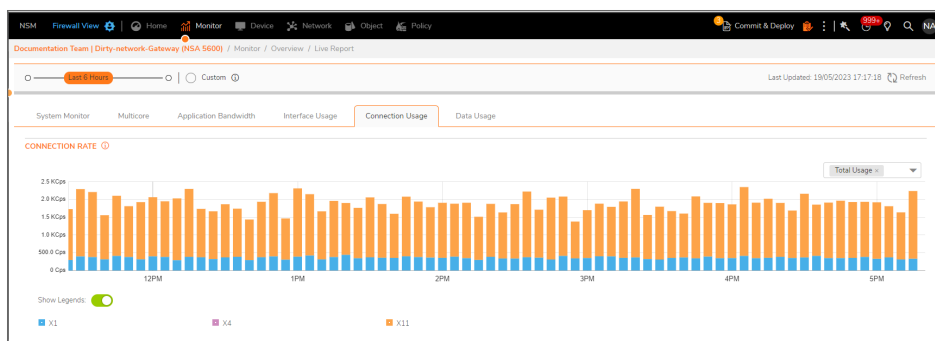
Application Bandwidth



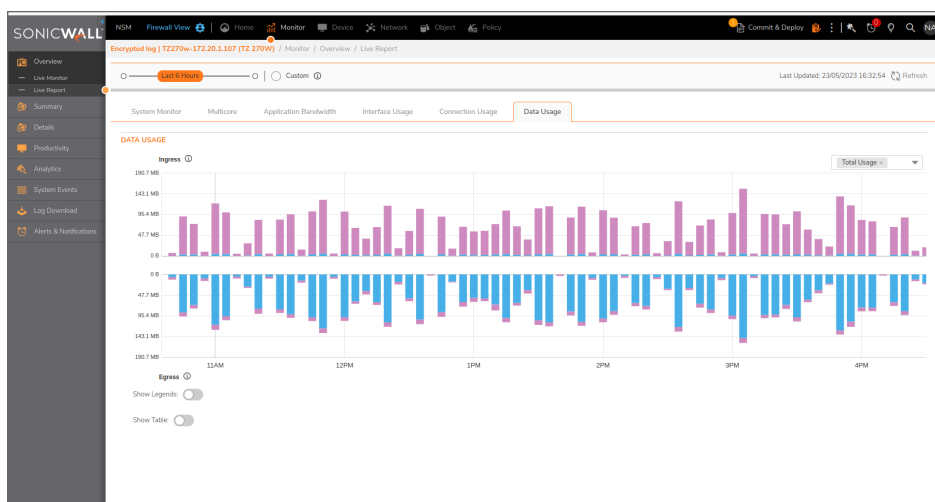
Interface Usage



Connection Usage



Data Usage



① **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.

❶ | **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.

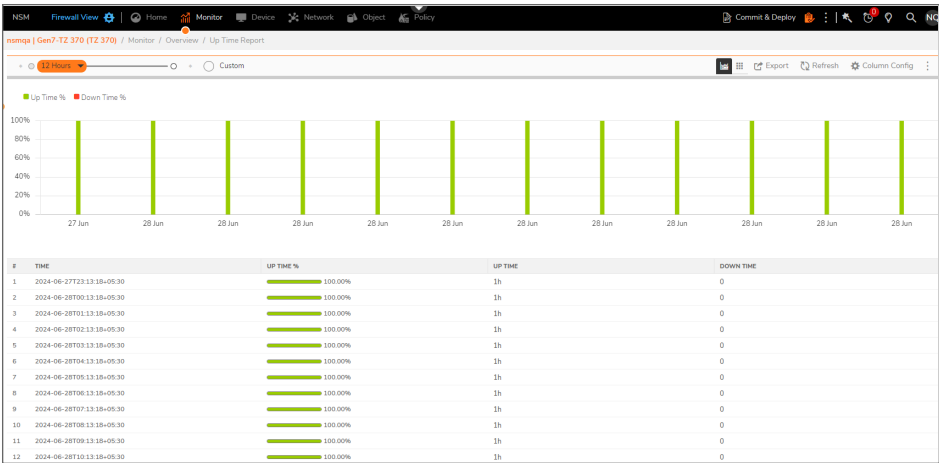
You can use the **Time Slider** to adjust the time duration and the **Custom** button to customize the dates. The slider allows you to view the report from a duration of 12 hours to 30 days. If you select a time range of 12 or 24 hours, then the report will be shown in the interval of 1 hour. If you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

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

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

❶ | **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
--------	-------------

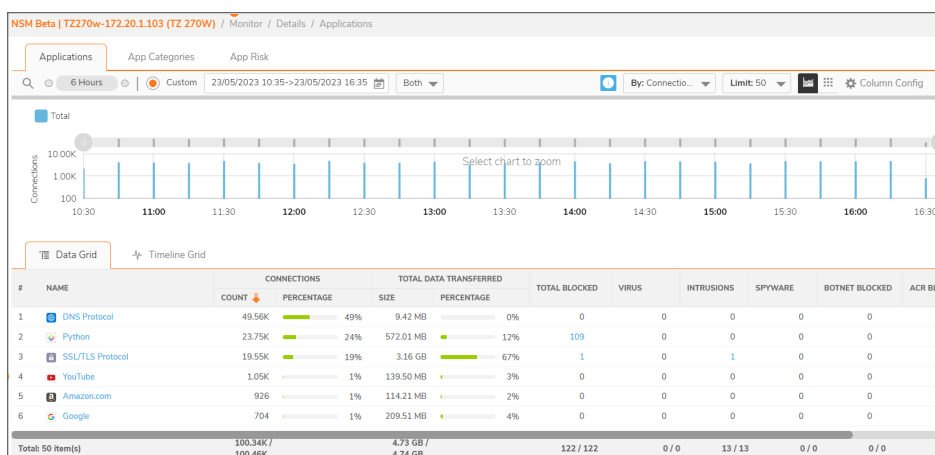
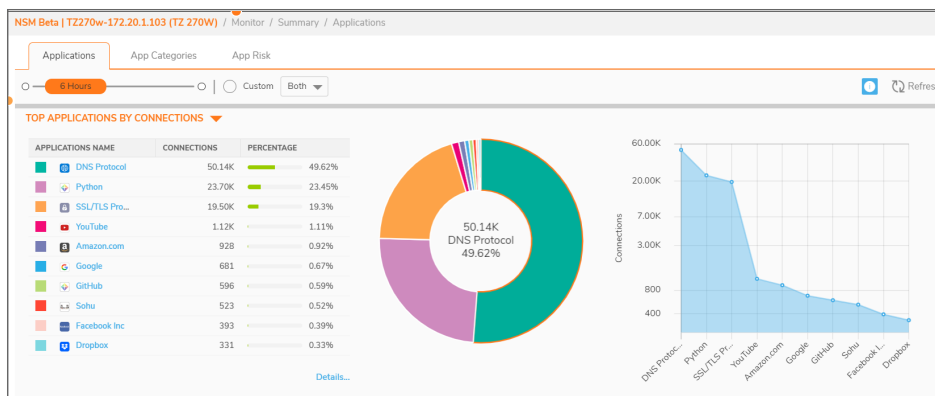
Sliding bar	Slide left or right to select a predefined period for the reports to cover. The range is 1 hour to 365 days.
Custom option	Define a custom period for the reports to cover. Select starting and ending dates and times for the custom period.
By	Filter data by any one of the parameters.
Limit	Number of connections.
Export	Provides three options: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 .

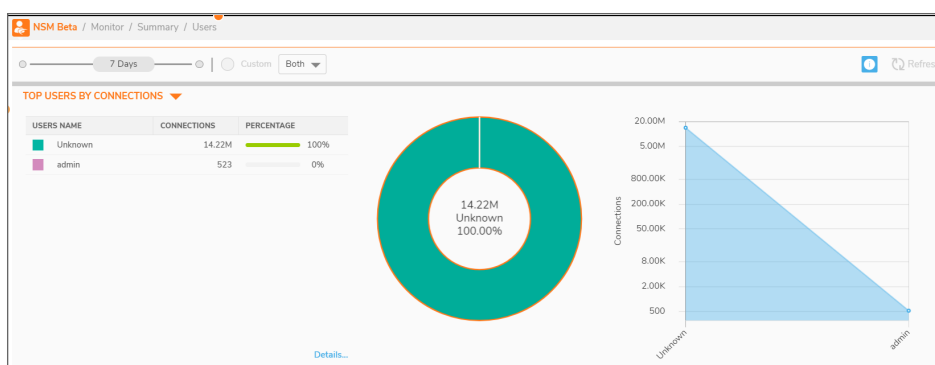
Applications

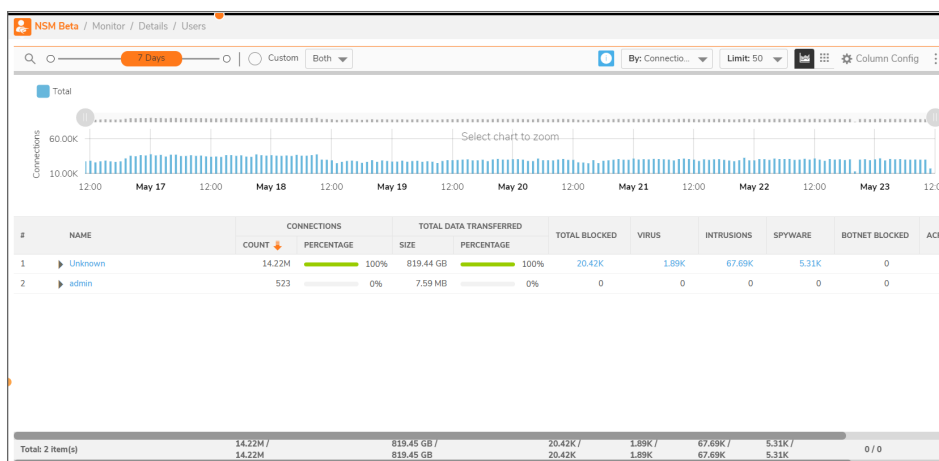
The Applications summary page has three types of reports displayed by default: Applications, App Categories, and App Risks.



Users

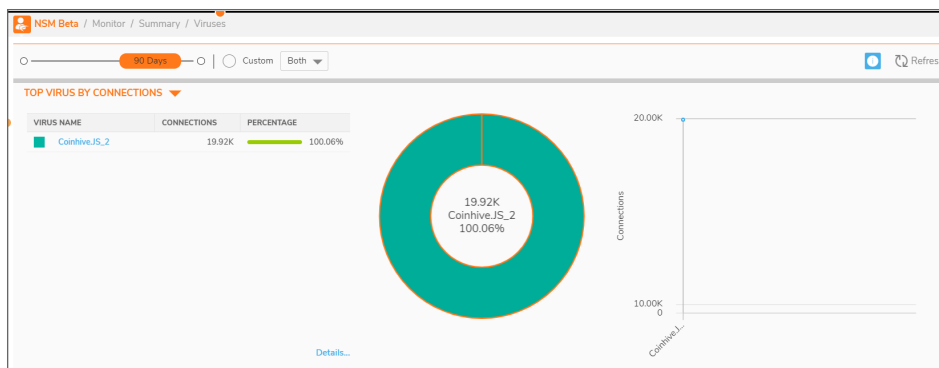
This report provides data that relates to the users connected to the system. You can track user level transactions and activities by filtering on different drill-down options.

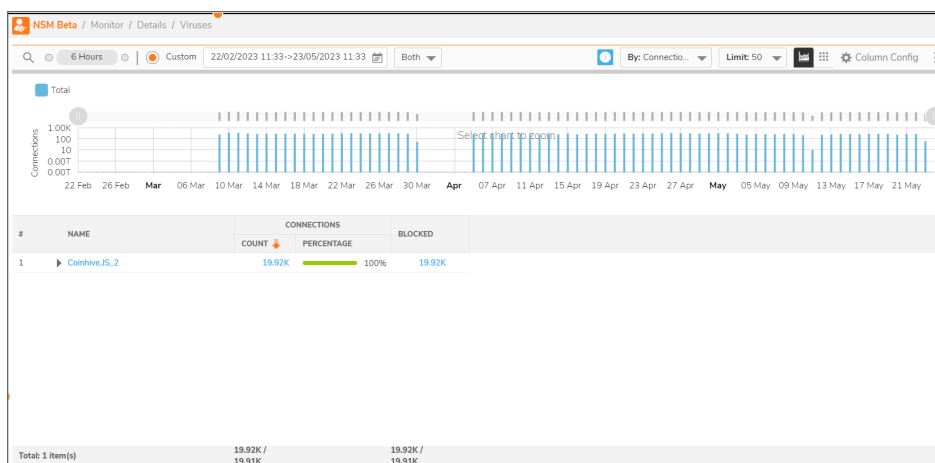




Viruses

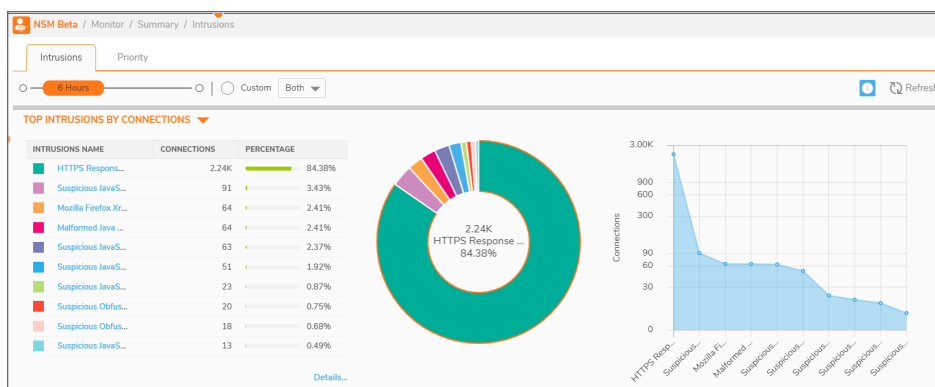
This report tracks the viruses that have been detected. You can filter on connections they occurred on or by which viruses were blocked. Details are provided in the table. Click on **HOME > Summary > OBSERVED THREATS** to see the reports on virus, botnet, spyware, and intrusion.

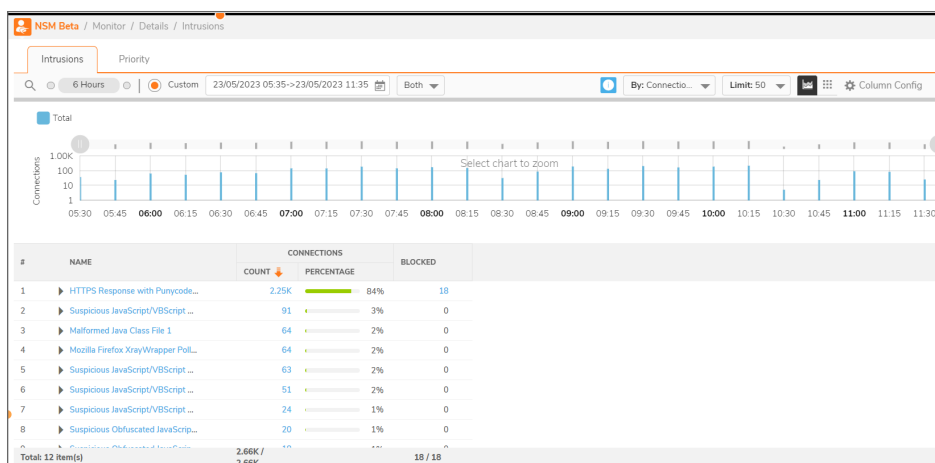




Intrusions

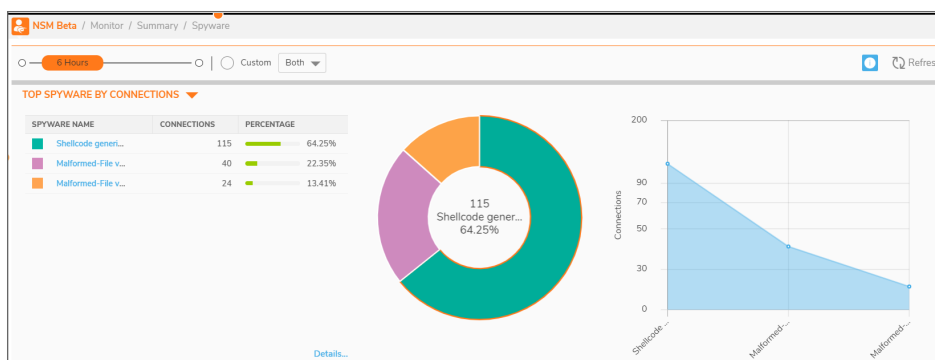
The Intrusions summary has two types of reports (represented by the different tabs): **Intrusions** and **Priority**. The Intrusions report tracks the disturbances that have been detected. You can filter on connections that occurred on or by which intrusions were blocked. Details are provided in the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

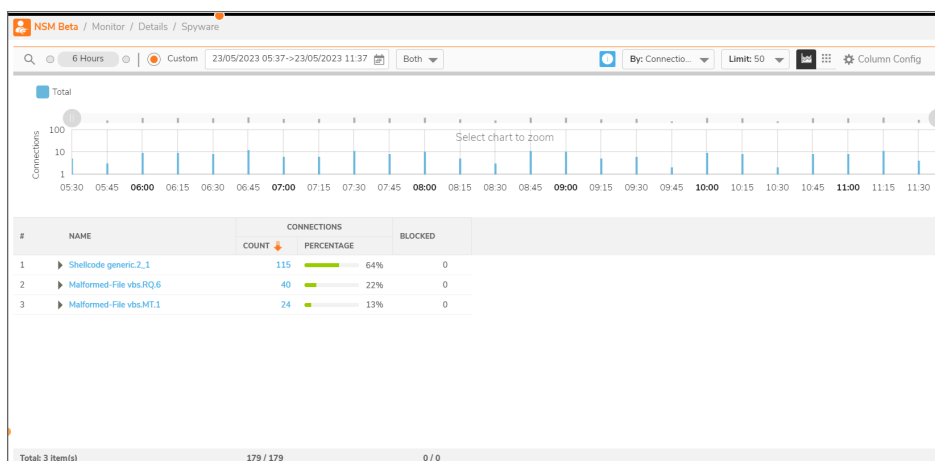




Spyware

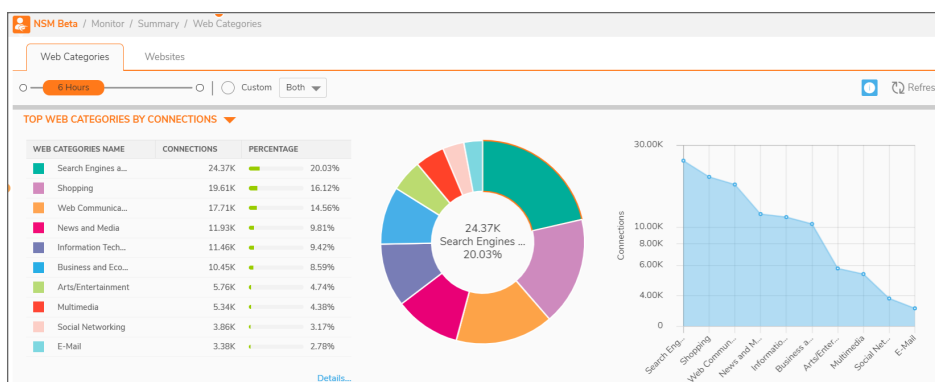
This report tracks the spyware that has been detected. You can filter on connections they occurred on or by which spyware was blocked. Two summary reports are available and displayed by default: Spyware by Connections and Spyware by Blocked.

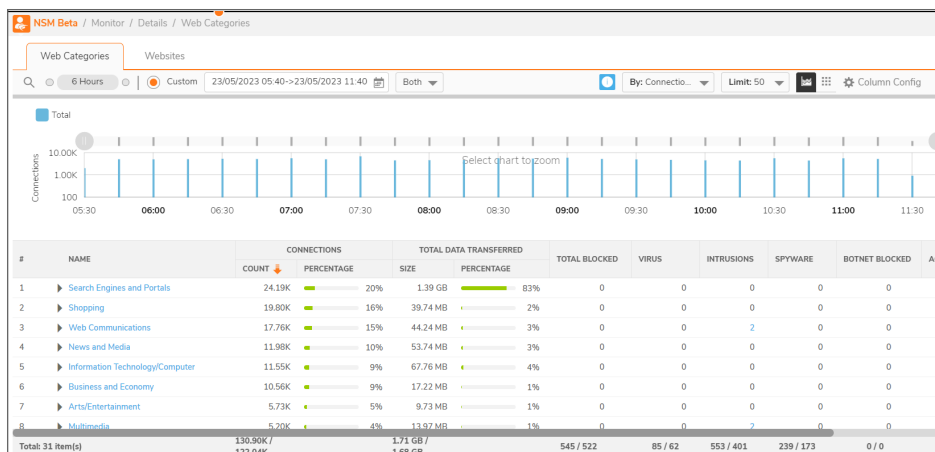




Web Categories

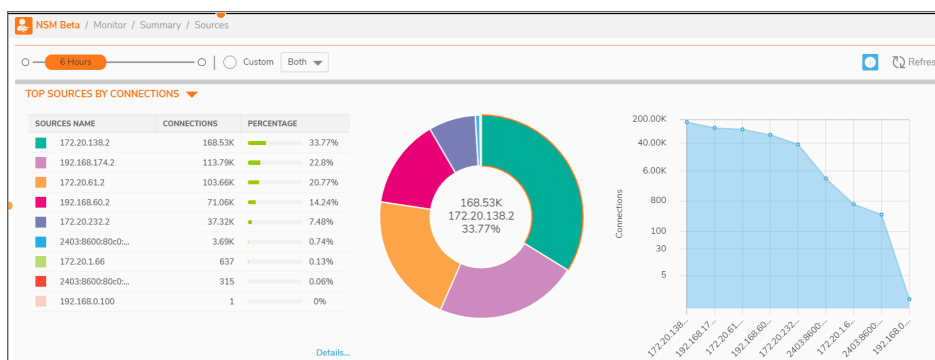
On the NSM system, the Web Categories summary has two types of reports. **Web Categories** and **Websites**. This report displays the number of connections based on web categories. You can filter on the categories in the View drop-down list. Details are provided in the table. Click on **HOME > Network > 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

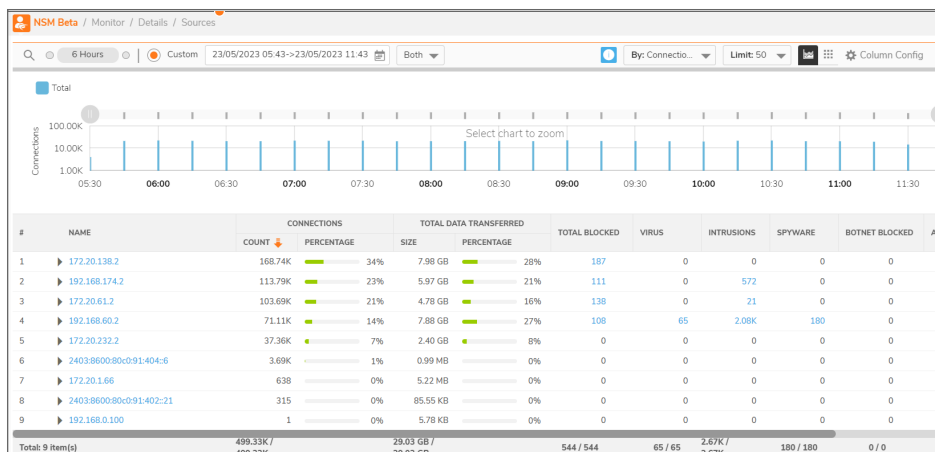


Click on **Details**, below each report, to go to the details page of the Source report. You can also view the page by navigating to **Details > Sources**. The top of the **Details** page shows a graphical representation of the selected **By Metric** data over a time period.

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.

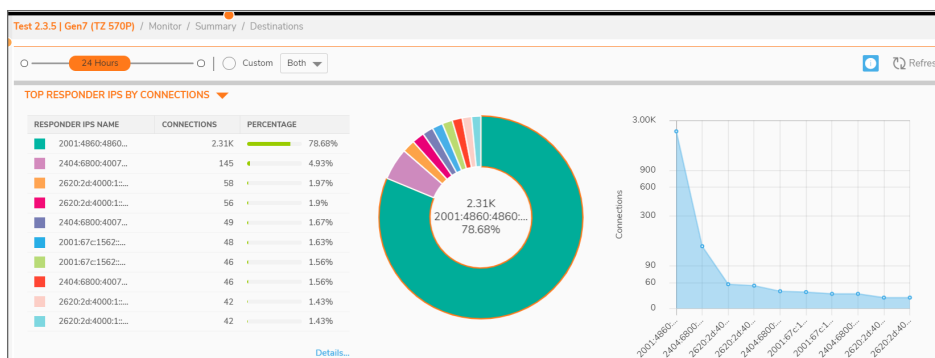
You can filter the information according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

The **Search** button at the top of the page allows you to search multiple IP addresses 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

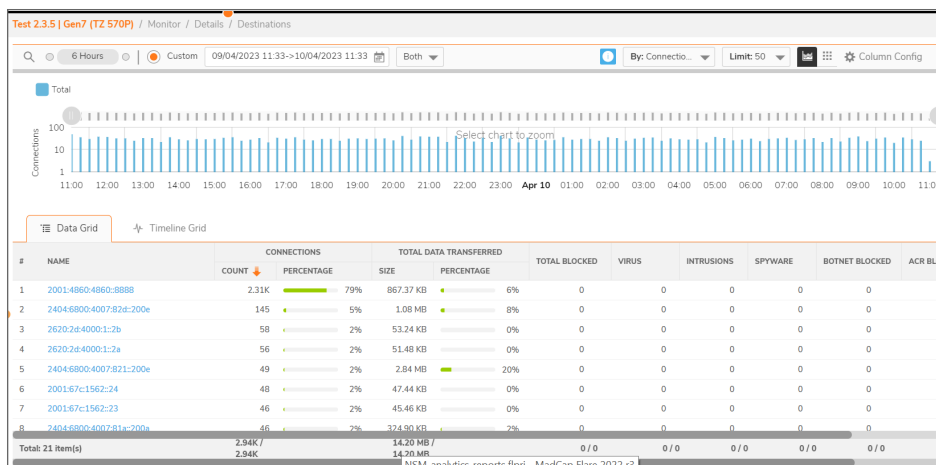


Click on **Details**, below each report, to go to the details page of the Destination report. You can also view the page by navigating to **Details > Destinations**. The top of the **Details** page shows a graphical representation of the selected **By Metric** data over a time period.

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.

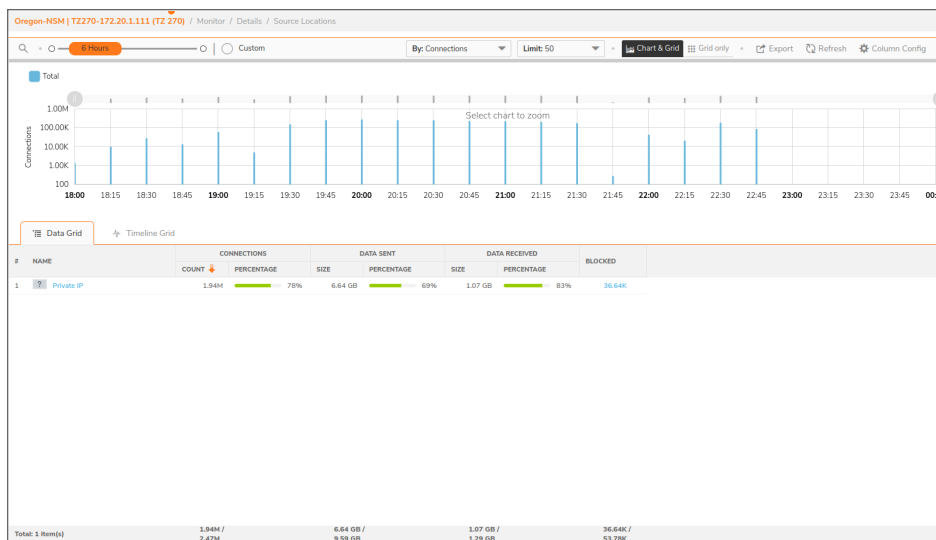
You can filter the information according to the IP version by selecting from **IPv4**, **IPv6** or **Both**.

The **Search** button at the top of the page allows you to search multiple IP addresses 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.



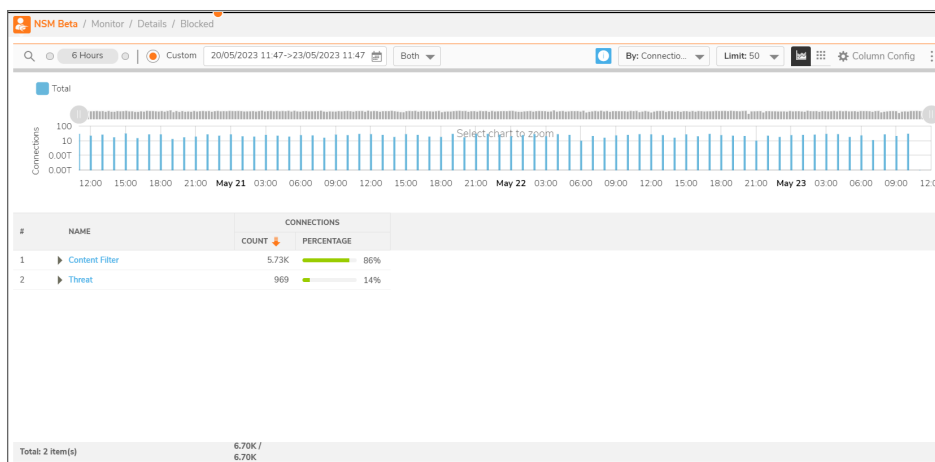
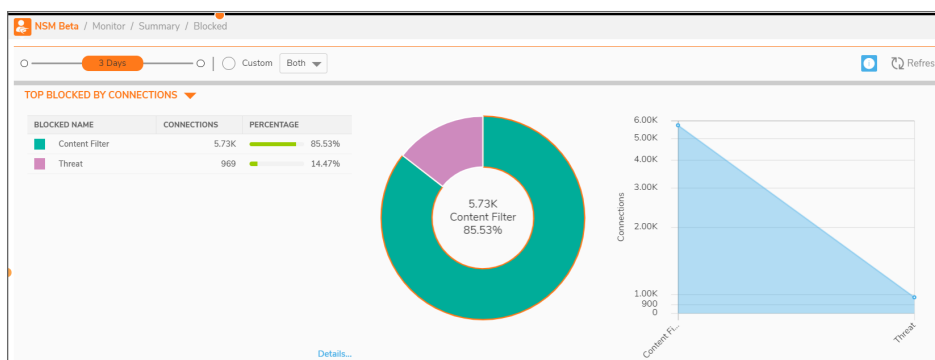
Locations

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.



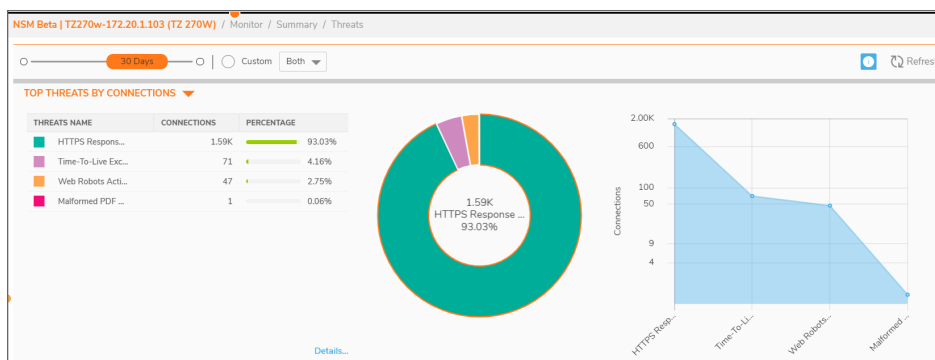
Blocked

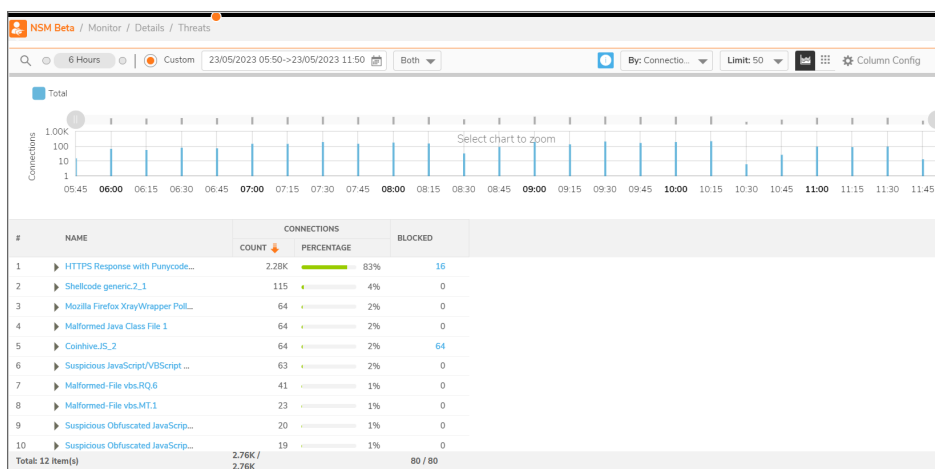
This report tracks the number of blocked connections. The report shows, the number of connections blocked and percentage of them based on Firewall rule, Threat, and Botnet Filter.



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

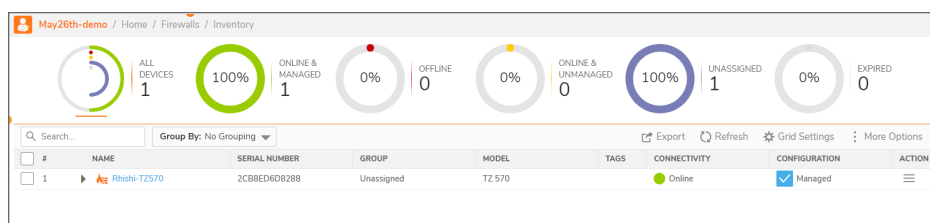
VPN Report tracks the traffic flowing through a pair of firewalls to which you have established a VPN tunnel. For example, if you are working on a local system that is protected by a firewall and you want to access information from a system that is remotely located and is protected by another firewall, 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.

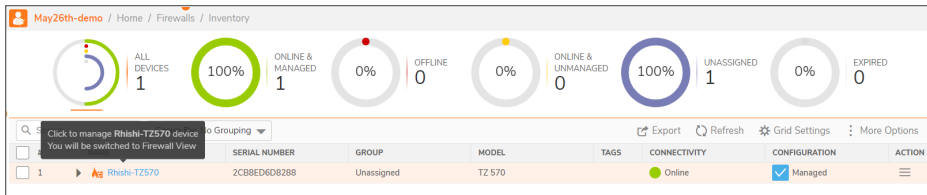
Navigating the VPN Reports

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

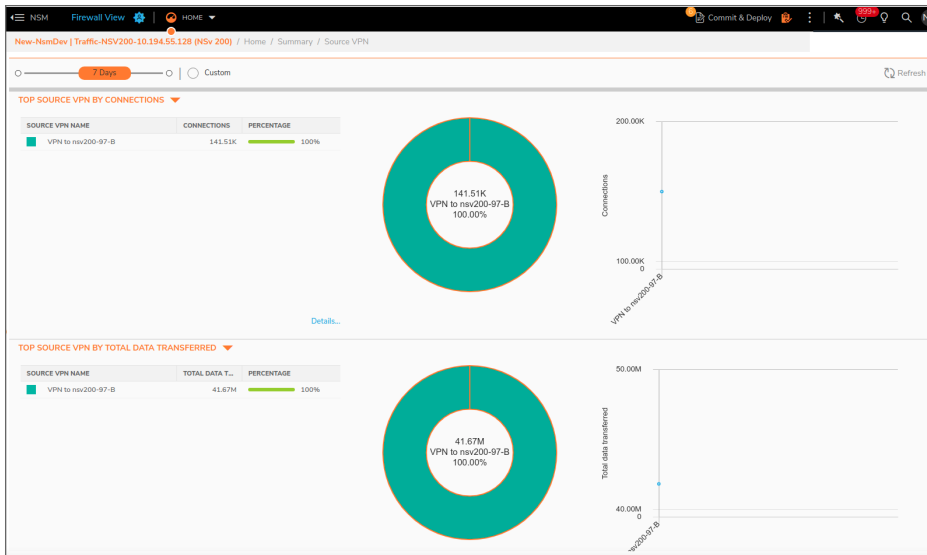
1. Go to **Firewalls > Inventory** to view a list of all the firewall devices.



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.

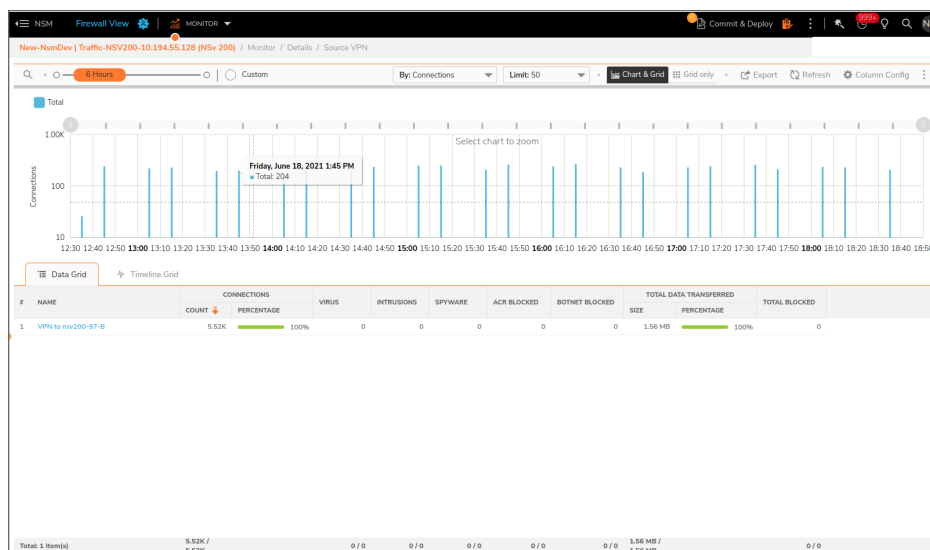


This reports page shows information such as source vpn name, connections and percentage. You can also find the data in the form of a Pie Chart as well as a Graph. The **Time Range** option lets you customize the time duration of the report to show data from the last hour to the last 365 days. You can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



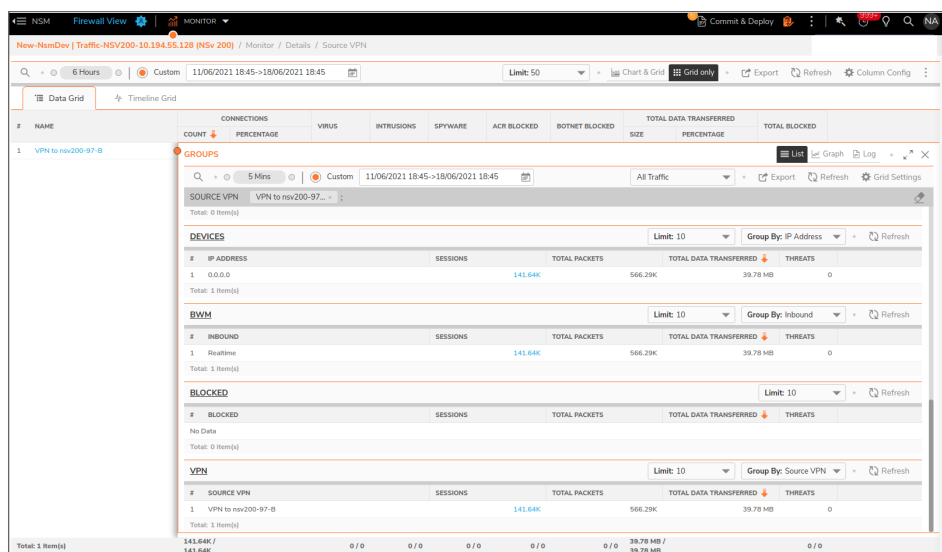
The top of the **Details** page shows a graphical representation of the selected **By Metric** data over a time period. You can change the information on the graph according to the above mentioned **By Metric** list by using the drop down button, at the top of the page. You can also hover above the graph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

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.

① | **NOTE:** You need to have NSM advance license to view and manage the Analytics.

- [About Analytics](#)
- [Navigating to the Analytics Page](#)
- [Custom Filters](#)

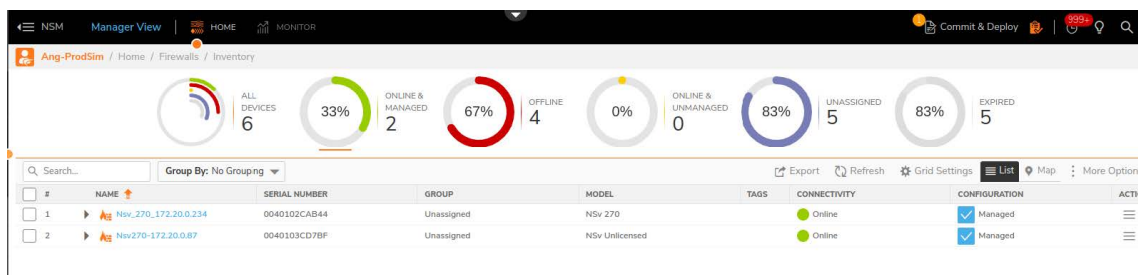
About Analytics

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.

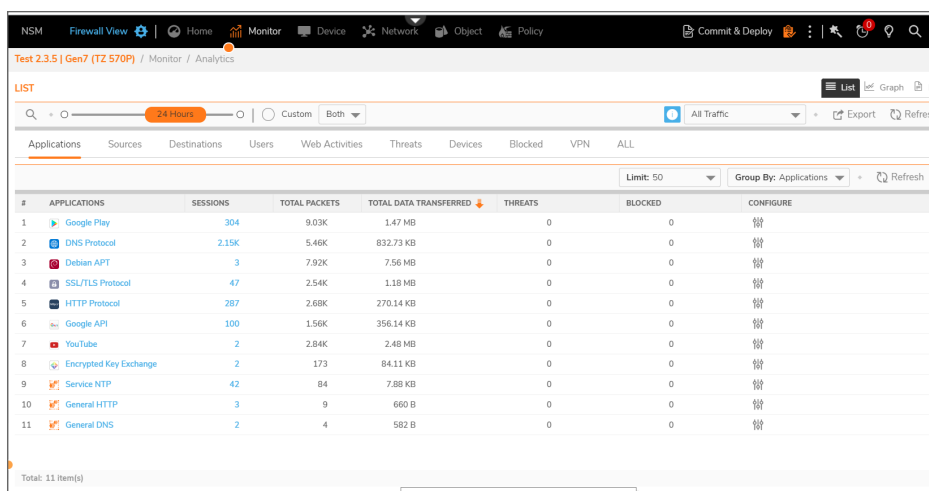
Analytics gives detailed insight of user information such as network events, user activities, threats, operational and performance issues, security efficacy, risks and security gaps, compliance readiness, and auditing. You can perform flexible drill-down and gain insight into your network, user access,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

#	APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL DATA TRANSFERRED	THREATS	BLOCKED	CONFIGURE
1	Google Play	304	9.03K	1.47 MB	0	0	
2	DNS Protocol	2.15K	5.46K	832.73 KB	0	0	
3	Debian APT	3	7.92K	7.56 MB	0	0	
4	SSL/TLS Protocol	47	2.54K	1.18 MB	0	0	
5	HTTP Protocol	287	2.68K	270.14 KB	0	0	
6	Google API	100	1.56K	356.14 KB	0	0	
7	YouTube	2	2.84K	2.48 MB	0	0	
8	Encrypted Key Exchange	2	173	84.11 KB	0	0	
9	Service NTP	42	84	7.88 KB	0	0	
10	General HTTP	3	9	660 B	0	0	
11	General DNS	2	4	582 B	0	0	

#	APPLICATIONS	SESSIONS	TOTAL PACKETS	TOTAL DATA TRANSFERRED	THREATS	BLOCKED	CONFIGURE
1	SSL/TLS Protocol	61	8.30K	7.01 MB	0	0	
2	CNN News	3	4.03K	4.15 MB	0	0	
3	YouTube	10	2.83K	2.71 MB	0	0	
4	Dropbox	4	2.68K	2.58 MB	0	0	
5	Python	85	3.04K	1.85 MB	0	1	
6	Redis	2	1.11K	966.45 KB	0	0	
7	Alibaba Cloud	2	710	676.71 KB	0	0	
8	Google	2	684	646.08 KB	0	0	
9	Amazon.com	3	808	615.91 KB	0	0	
10	DNS Protocol	106	212	21.51 KB	0	0	

#	SOURCES	SESSIONS	TOTAL PACKETS	TOTAL DATA TRANSFERRED	THREATS	BLOCKED	CONFIGURE
1	IP ADDRESS 172.20.138.2	282	24.57K	21.17 MB	0	1	

#	DESTINATIONS	SESSIONS	TOTAL PACKETS	TOTAL DATA TRANSFERRED	THREATS	BLOCKED	CONFIGURE
1	IP ADDRESS 162.125.81.18	9	2.74K	2.58 MB	0	0	

Graph View

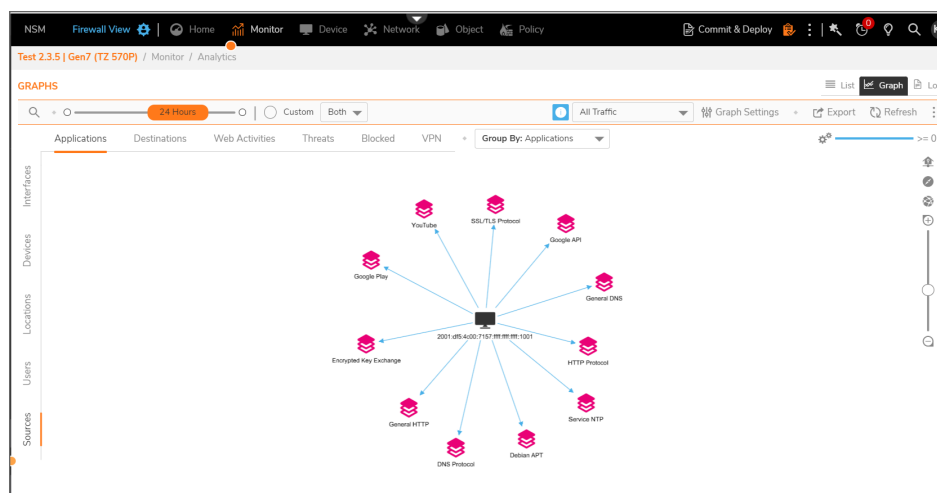
This view allows you to see the relationship between any two metrics available on X and Y, in a graphical format. You can change the individual metric by clicking on the different options on the X and Y axis. For example, if you

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.

#	TIME	USERS	ACTION	APPLICATION	CATEGORY	RISK	SIGNATURE	IP ADDRESS	LOCATION
	OPEN TIME							INITIATOR	RESPONDER
1	2023-04-10 11:4...	Unkno...	Allow...	Google Play	INFRASTRU...	Guard...	Google Play -- H...	2001:df5:4c...	2404:6800...
2	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
3	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
4	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
5	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
6	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
7	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
8	2023-04-10 11:4...	Unkno...	Allow...	HTTP Protocol	PROTOCOLS	Low	HTTP Protocol -- ...	2001:df5:4c...	2620:2d40...
9	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
10	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
11	2023-04-10 11:4...	Unkno...	Allow...	Google Play	INFRASTRU...	Guard...	Google Play -- D...	2001:df5:4c...	2001:4860...
12	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
13	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
14	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...
15	2023-04-10 11:4...	Unkno...	Allow...	DNS Protocol	PROTOCOLS	Low	DNS Protocol -- ...	2001:df5:4c...	2001:4860...

You can use the **Search** button to search for a particular information. The **Search** button also allows you to search multiple IP addresses 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.

SESSION LOGS														
PORT		STATISTICS		THREAT			POLICIES							
INITIATOR	RESPON...	INITIATO...	RESPON...	THREAT TYPE	THREAT NAME	BOTNET	APP RULE ID	SECURITY P...	NAT POLICY ...	ROUTE POLL...	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	
10370	53	145 B	150 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

-

NAT Rule Details

NAT RULE DETAILS

TRANSLATED

Name

Default NAT Policy_30

ID

30

UUID

df9323d5-bfff-ft76-0800-2cb8eda63008

IP Version

IPv4

Comment

Auto-added W0 outbound NAT Policy for X1 WAN

ADVANCED

Source Address

X1 IP

Destination Address

Original

Service

Original

ORIGINAL

Ingress Interface

W0

Egress Interface

X1

Source Address

Any

Destination Address

Any

Service

Any

TICKET

Tag 1

Tag 2

Tag 3

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.

SESSION LOGS

Q

5 Mins

Custom

All Traffic

Limit: 50

Export

Refresh

Grid Settings

Custom Filters

app-wget

#	TIME	USERS	ACTION	APPLICATION	CATEGORY	RISK	SIGNATURE	IP ADDRESS	LOCATION	PORT	STATISTICS			
	OPEN TIME							INITIATOR	RESPONDER	INITIATOR	RESPONDER	INITIATOR...	RESPO	
1	2021-08-09 16:31:12	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	208.94.116.21	Private IP	United States	45316	80	429 B 5.9
2	2021-08-09 16:31:11	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	208.94.116.21	Private IP	United States	45314	80	446 B 4.5
3	2021-08-09 16:31:09	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	208.94.116.21	Private IP	United States	45312	80	495 B 5.9
4	2021-08-09 16:31:08	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	208.94.116.21	Private IP	United States	45310	80	500 B 13.9
5	2021-08-09 16:31:03	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	208.94.116.21	Private IP	United States	45298	80	441 B 6.3
6	2021-08-09 16:31:01	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	208.94.116.21	Private IP	United States	45286	80	437 B 6
7	2021-08-09 16:31:00	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	208.94.116.21	Private IP	United States	45282	80	499 B 1.7
8	2021-08-09 16:30:08	user11	Allowed	Wiget	DOWNLOAD-APPS	Low	Wiget - Client Activity	192.168.150.2	138.113.144.148	Private IP	United States	45276	80	377 B 13.2

Total: 8 items

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-**

Network Security Manager Reporting and Analytics Administration Guide
Analytics

50

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.

① | **NOTE:** You can add multiple filters to the table.

SESSION LOGS

Custom Filters: Net

APP CATEGORIES: Networking

#	OPEN TIME	USERS	ACTION	APPLICATION	CATEGORY	RISK	SIGNATURE	INITIATOR	RESPONDER	LOCATION	RESPONDER	INITIATOR	RESPON.	INITIATOR...	RESPON...	THRU
1	2021-08-11 11:04:04	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.131.185.136	Private IP	United States	47444	80	360 B	46 B	No
2	2021-08-11 11:05:22	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	34.122.121.32	Private IP	United States	46622	80	300 B	46 B	No
3	2021-08-11 11:05:01	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.130.32.2	Private IP	United States	47676	80	360 B	46 B	No
4	2021-08-11 11:01:52	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.126.230.92	Private IP	United States	40150	80	318 B	3.53 KB	No
5	2021-08-11 11:01:49	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	1.1210.16	Private IP	Thailand	49936	80	318 B	3.53 KB	No
6	2021-08-11 11:00:33	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.236.67	Private IP	United States	55336	80	318 B	3.53 KB	No
7	2021-08-11 10:58:32	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.178.131	Private IP	United States	42586	80	360 B	46 B	No
8	2021-08-11 10:57:29	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.131.185.136	Private IP	United States	46998	80	360 B	46 B	No
9	2021-08-11 10:56:27	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.131.172.1	Private IP	United States	46744	80	360 B	46 B	No
10	2021-08-11 10:55:26	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.130.32.2	Private IP	United States	47374	80	360 B	46 B	No
11	2021-08-11 10:55:22	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	113.50.65.8	Private IP	China	56494	80	360 B	46 B	No
12	2021-08-11 10:53:54	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.236.68	Private IP	United States	37140	80	318 B	3.53 KB	No
13	2021-08-11 10:53:51	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.236.67	Private IP	United States	54888	80	180 B	3.53 KB	No
14	2021-08-11 10:52:50	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.178.131	Private IP	United States	42154	80	360 B	46 B	No

- 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.

SESSION LOGS

Custom Filters: Net

APP CATEGORIES: Networking

Save Filter

Delete Filter

+ Create Custom Report Rule

#	OPEN TIME	USERS	ACTION	APPLICATION	CATEGORY	RISK	SIGNATURE	INITIATOR	RESPONDER	LOCATION	RESPONDER	INITIATOR	RESPON.	INITIATOR...	RESPON...	THRU
1	2021-08-11 11:04:04	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.131.185.136	Private IP	United States	47444	80	360 B	46 B	No
2	2021-08-11 11:05:22	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	34.122.121.32	Private IP	United States	46622	80	300 B	46 B	No
3	2021-08-11 11:05:01	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.130.32.2	Private IP	United States	47676	80	360 B	46 B	No
4	2021-08-11 11:01:52	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.126.230.92	Private IP	United States	40150	80	318 B	3.53 KB	No
5	2021-08-11 11:01:49	user4	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	1.1210.16	Private IP	Thailand	49936	80	318 B	3.53 KB	No
6	2021-08-11 11:00:33	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.236.67	Private IP	United States	55336	80	318 B	3.53 KB	No
7	2021-08-11 10:58:32	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.178.131	Private IP	United States	42586	80	360 B	46 B	No
8	2021-08-11 10:57:29	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.131.185.136	Private IP	United States	46998	80	360 B	46 B	No
9	2021-08-11 10:56:27	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.131.172.1	Private IP	United States	46744	80	360 B	46 B	No
10	2021-08-11 10:55:26	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.130.32.2	Private IP	United States	47374	80	360 B	46 B	No
11	2021-08-11 10:55:22	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	113.50.65.8	Private IP	China	56494	80	360 B	46 B	No
12	2021-08-11 10:53:54	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.236.68	Private IP	United States	37140	80	318 B	3.53 KB	No
13	2021-08-11 10:53:51	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.236.67	Private IP	United States	54888	80	180 B	3.53 KB	No
14	2021-08-11 10:52:50	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.156.178.131	Private IP	United States	42154	80	360 B	46 B	No
15	2021-08-11 10:51:49	user3	Allowed	General HTTP	Networking	Low	General HTTP -- 49175	192.168.209.2	98.131.229.2	Private IP	United States	40744	80	360 B	46 B	No

- 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.

Save Custom Filter As

Filter name * social-media

Filters * APP CATEGORIES SOCIAL-NETWORK...

Cancel Save Save & Create Report Rule

Editing and Deleting Custom Filters

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

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.

SESSION LOGS

12 hours

Custom

All Traffic

Limit: 50

Export

Refresh

Grid Settings

Custom Filters

Net

Networking

Relaxed

SIGNATURES		APP CATEGORIES		Networking		Relaxed								
#	TIME	USERS	ACTION	APPLICATION	CATEGORY	RISK	SIGNATURE	INITIATOR	RESPONDER	INITIATOR	LOCATION	INITIATOR	PORT	RESULTS
1	2021-08-11 11:04:04	user4	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.131.195.136	Private ip	United States	47444	80	
2	2021-08-11 11:03:22	user4	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	34.122.121.32	Private ip	United States	46622	80	
3	2021-08-11 11:02:01	user4	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.130.122.2	Private ip	United States	40786	80	360 0 46 0 N
4	2021-08-11 11:01:52	user4	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	192.168.230.92	Private ip	United States	41015	80	318 0 353 0 N
5	2021-08-11 11:01:49	user4	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	1.210.16	Private ip	Thailand	49936	80	318 0 353 0 N
6	2021-08-11 11:00:31	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.158.230.67	Private ip	United States	50536	80	318 0 353 0 N
7	2021-08-11 10:59:52	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.158.178.31	Private ip	United States	42996	80	360 0 46 0 N
8	2021-08-11 10:47:20	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.131.195.136	Private ip	United States	40988	80	360 0 46 0 N
9	2021-08-11 10:46:27	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.131.172.1	Private ip	United States	46744	80	360 0 46 0 N
10	2021-08-11 10:50:26	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.130.122.2	Private ip	United States	47574	80	360 0 46 0 N
11	2021-08-11 10:50:22	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	113.50.65.8	Private ip	United States	50894	80	360 0 46 0 N
12	2021-08-11 10:53:54	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.158.230.67	Private ip	United States	37440	80	318 0 353 0 N
13	2021-08-11 10:53:51	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.158.230.67	Private ip	United States	54880	80	318 0 353 0 N
14	2021-08-11 10:52:50	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.158.178.31	Private ip	United States	42154	80	360 0 46 0 N
15	2021-08-11 10:52:49	user3	Allowed	General HTTP	Networking	Low	General HTTP - 40176	192.168.209.2	90.131.229.2	Private ip	United States	40744	80	360 0 46 0 N

Save Filter

Delete Filter

Create Custom Filter Rule

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**.

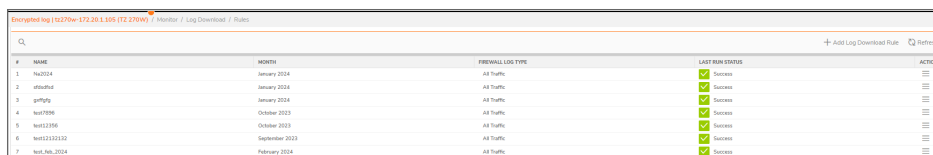
① | **NOTE:** You need to have NSM advance license to view and manage the Log Download.

① | **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.



NAME	MONTH	FIREWALL LOG TYPE	LAST RUN STATUS	ACTION
Test1234	January 2024	All Traffic	Success	
Test1234	January 2024	All Traffic	Success	
Test1234	January 2024	All Traffic	Success	
Test1234	October 2023	All Traffic	Success	
Test1234	October 2023	All Traffic	Success	
Test1234	September 2023	All Traffic	Success	
Test1234	February 2024	All Traffic	Success	

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 calendar 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 filter 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.

① | **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

Custom Filter ☐ There are no custom filters to select

IP Version

Firewall Log Type

Previous Next

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

Custom Filter ☐ There are no custom filters to select

IP Version

Firewall Log Type

Previous Next

Add Log Download Rule

1

2

GENERALSUMMARY

Please note you can run log download rule for a given month only 3 times.

GENERAL

Name

Month

Custom Filter ☐ There are no custom filters to select

IP Version

Firewall Log Type

RULE RUN HISTORY FOR MONTH

This device has no previously run rules for this month.

Add Log Download Rule

1

2

GENERALSUMMARY

Please note you can run log download rule for a given month only 3 times.

GENERAL

Name

Month

Custom Filter ☐ There are no custom filters to select

IP Version

Firewall Log Type

✓ IPv4 & IPv6

IPv4

IPv6

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

Custom Filter ☐ There are no custom filters to select

IP Version

Firewall Log Type

- ✓ All Traffic
- Web Activities
- Threats
- Blocked

- 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.

Add Log Download Rule

1 GENERAL 2 SUMMARY

SUMMARY

Name Test1

Month January 2024

Use Custom Filter No

IP Version IPv4 & IPv6

Firewall Log Type All Traffic

Approximate number of records 15,308,108

Previous Apply

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

Add Log Download Rule

✓

✓

GENERALSUMMARY

✓ Success

Log file generation is in progress

SUMMARY

Name

Test1

Month

January 2024

Use Custom Filter

No

IP Version

IPv4 & IPv6

Firewall Log Type

All Traffic

Approximate number of records

15,308,108

Close

- 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.

#	NAME	MONTH	FIREWALL LOG TYPE	LAST RUN STATUS	ACTION
1	Test1	January 2024	All Traffic	Success	
2	Test2	January 2024	All Traffic	Success	
3	Test3	January 2024	All Traffic	Success	
4	Test4	October 2023	All Traffic	Success	
5	Test5	October 2023	All Traffic	Success	
6	Test6	September 2023	All Traffic	Success	
7	Test7	February 2024	All Traffic	Success	
8	Test8	January 2024	All Traffic	Success	

① | **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 ILog 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.

- 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.

#	NAME	MONTH	NO. OF FILES GENERATED	EXPIRY	ACTION
1	Na0001a_JC000004037A0L_1_2024_1709027100	January 2024	17	Expires on 2024-01-29 15:15	
2	Na0001a_JC000004037A0L_1_2024_1709050100	January 2024	16	Expires on 2024-01-29 15:15	
3	Na0001a_JC000004037A0L_1_2024_1706041007	January 2024	17	Expires on 2024-01-29 15:15	
4	Na0001a_JC000004037A0L_1_2023_1706032005	October 2023	16	Expires on 2024-01-29 15:15	
5	Na0001a_JC000004037A0L_1_2023_1706080728	October 2023	16	Expires on 2024-01-29 15:15	
6	Na0001a_JC000004037A0L_1_2023_1706092139	September 2023	16	Expires on 2024-01-29 15:15	
7	Na0001a_JC000004037A0L_1_2024_1709050605	January 2024	1	Expires on 2024-01-29 15:15	
8	Na0001a_JC000004037A0L_1_2024_1709091002	January 2024	17	Expires on 2024-01-29 15:15	

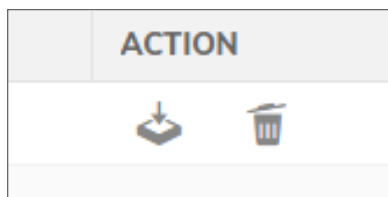
① | **NOTE:** Each log download rule will be available for a month for download. You can see the date and time at which it will get expired under the **Expiry** column.

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.

#	NAME	MONTH	NO. OF FILES GENERATED	EXPIRY	ACTION
1	Na0001a_JC000004037A0L_1_2024_1709027100	January 2024	17	Expires on 2024-01-29 15:15	

#	NAME	ACTION
1	Na0001a_JC000004037A0L_1_2024_1709027100_Na0001a.csv	
2	Na0001a_JC000004037A0L_1_2024_1709027100_Part_1.koorge	
3	Na0001a_JC000004037A0L_1_2024_1709027100_Part_2.koorge	
4	Na0001a_JC000004037A0L_1_2024_1709027100_Part_3.koorge	
5	Na0001a_JC000004037A0L_1_2024_1709027100_Part_4.koorge	
6	Na0001a_JC000004037A0L_1_2024_1709027100_Part_5.koorge	
7	Na0001a_JC000004037A0L_1_2024_1709027100_Part_6.koorge	
8	Na0001a_JC000004037A0L_1_2024_1709027100_Part_7.koorge	
9	Na0001a_JC000004037A0L_1_2024_1709027100_Part_8.koorge	
10	Na0001a_JC000004037A0L_1_2024_1709027100_Part_9.koorge	

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.

① | **NOTE:** There is no restriction on the number of times you can download a generated log

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.

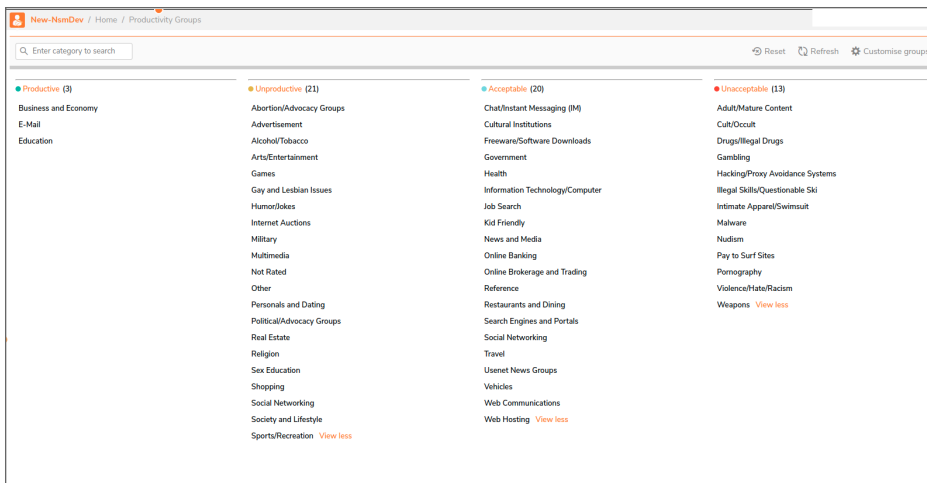
- ① | **NOTE:** You need to have NSM Advance License to view and manage the Productivity Reports.
- ① | **NOTE:** The Productivity Report is available at **tenant, group and firewall level**.
- ① | **NOTE:** Tenant and Group level productivity report is available from NSM SaaS **2.3.5** onwards.

Productivity Groups

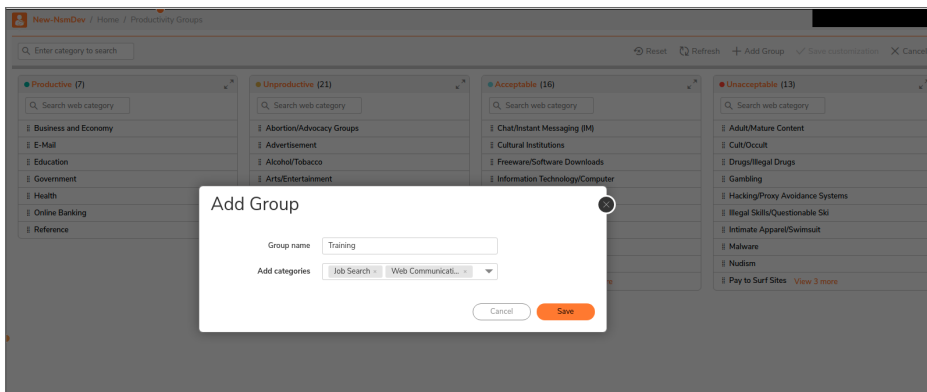
Productivity groups section allows grouping of **Content Filter Service(CFS)** categories. URLs accessed by users is matched first to the CFS and then to the respective productivity groups. There are two types of CFS groups under NSM Productivity Reports i.e. CFS 4.0 and CFS 5.0. Firewalls with SonicOS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

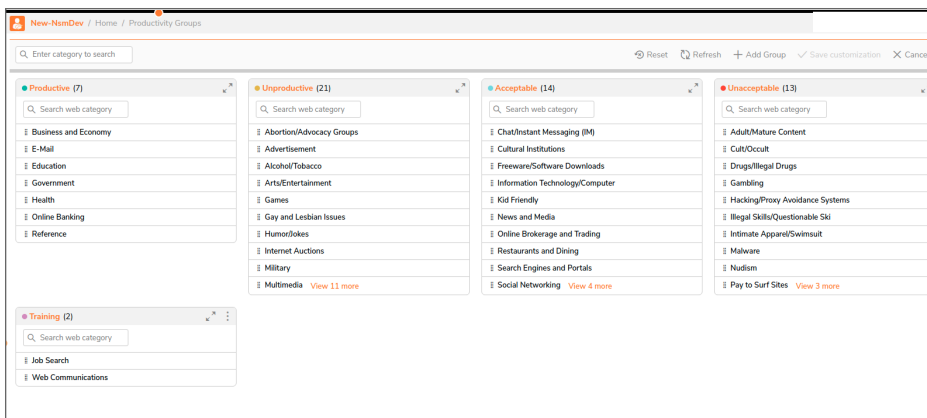
1. Click on **Productivity Groups** tab on the **Manager View** to see the Default group configuration. This list consists of Productive, Unproductive, Acceptable and Unacceptable groups. If you do not see the default groups then you can click on **Reset** button to reset it to default. You can also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



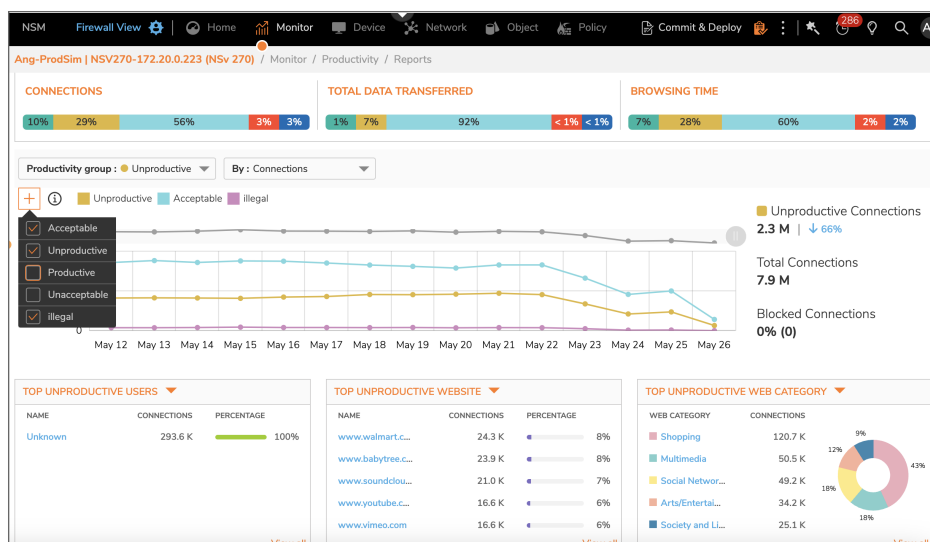
4. Click **Save** to add the new group to the list of existing Productivity groups.



- 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

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



① | **NOTE:** You can access Productivity Reports at the Group and Firewall level as well.

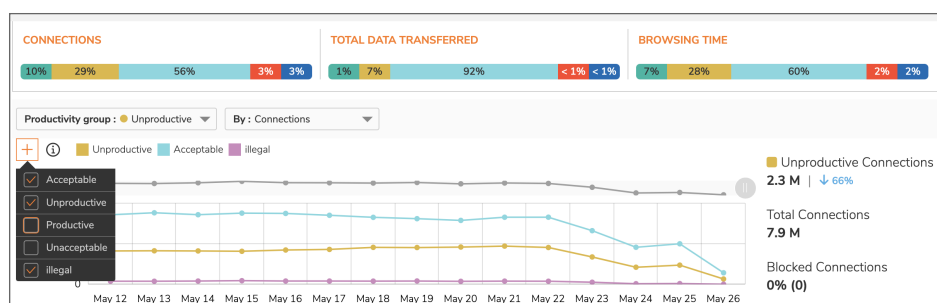
① | **NOTE:** You can do a comparative analysis of various Productivity Group trends by selecting two or more Productivity Groups.

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:

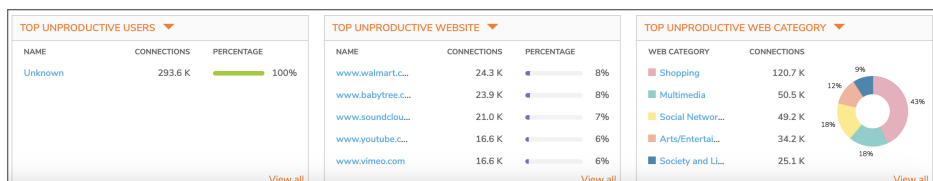
- **Trend Graph** - This graph displays trend of selected productivity category by selected metric. For example if user has selected productive category and metric as data transfer, then this graph displays trend of data transfer in productive category. You can click on the **+** button to add data for 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.

#	USER NAME	TOTAL CONNECTIONS	BLOCKED CONNECTIONS	TOTAL BROWSING TIME	DATA TRANSFERRED	ACTIONS
1	Unknown	2.0 K 20.23%	15	2 hrs 37 mins	37.5 MB	...
2	user8	1.7 K 12.55%	11	1 hr 32 mins	42.8 MB	...
3	user11	1.4 K 10.06%	4	1 hr 17 mins	3.4 MB	...
4	user14	1.3 K 9.05%	6	59 mins	12.1 MB	...
5	user9	1.0 K 7.48%	7	49 mins 55 secs	16.3 MB	...
6	user5	1.0 K 7.35%	6	50 mins 25 secs	3.0 MB	...
7	user2	995 6.89%	0	49 mins 46 secs	21.3 MB	...
8	user0	716 5.16%	7	35 mins 48 secs	8.5 MB	...
9	user10	710 5.12%	3	35 mins 42 secs	12.9 MB	...
10	user1	586 4.22%	1	29 mins 36 secs	7.0 MB	...
11	user7	584 4.21%	0	29 mins 31 secs	8.8 MB	...
12	user4	551 3.97%	5	26 mins 16 secs	10.2 MB	...
13	user13	512 3.69%	2	24 mins 40 secs	6.3 MB	...

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.

#	USER NAME	TOTAL CONNECTIONS	BLOCKED CONNECTIONS	TOTAL BROWSING TIME	DATA TRANSFERRED	ACTIONS
1	Unknown	6.4 K 87.92%	520	2 hrs 36 mins	68.4 MB	...
2	user2	217 2.96%	7	5 mins 52 secs	1.0 MB	...
PRODUCTIVITY GROUP						
	Acceptable	74 34.1%	6	59 secs	147.4 KB	
	Unproductive	54 24.88%	0	3 mins 22 secs	159.4 KB	
	Productive	47 21.66%	0	17 secs	530.4 KB	
	Unacceptable	31 14.29%	1	1 min 4 secs	199.0 KB	
	Training	11 5.07%	0	10 secs	11.0 KB	
3	user10	178 2.43%	9	4 mins 31 secs	1.2 MB	...
4	user1	174 2.37%	12	5 mins 3 secs	5.4 MB	...
5	user9	141 1.92%	9	4 mins 31 secs	5.4 MB	...
6	user6	133 1.81%	0	3 mins 2 secs	521.7 KB	...
7	user3	43 0.59%	2	41 secs	437.0 KB	...

Total : 7 Items

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.

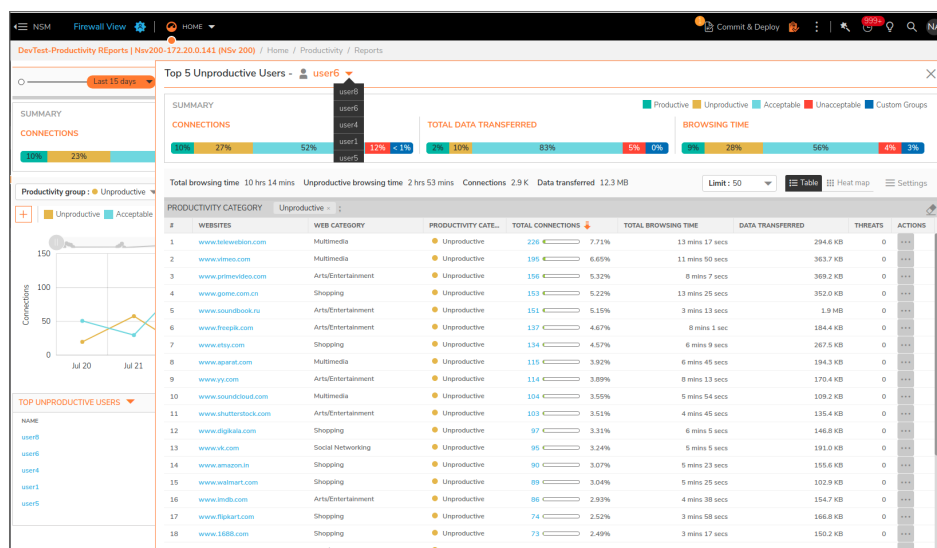
This page also provides you the option to filter the table according to individual web category or productivity category. You can click on the **Filter** symbol besides any of the category and click Reload.

- **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.

① **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.

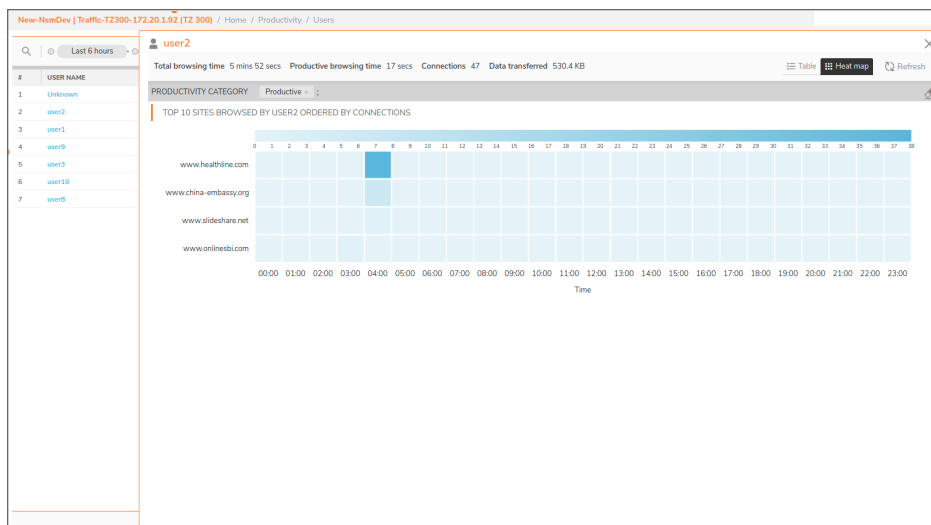


The **Heat Map** is color coded chart that shows the hourly distribution of the top websites that the user has browsed. For example, you can find out browsing pattern of websites during office and non-office hours. The different shades of the heat map represents different amount of data. The darker the 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.

① **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.

① **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.

① **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.

① **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.facebook...	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.1mail.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	920	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.wikipedia...	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.

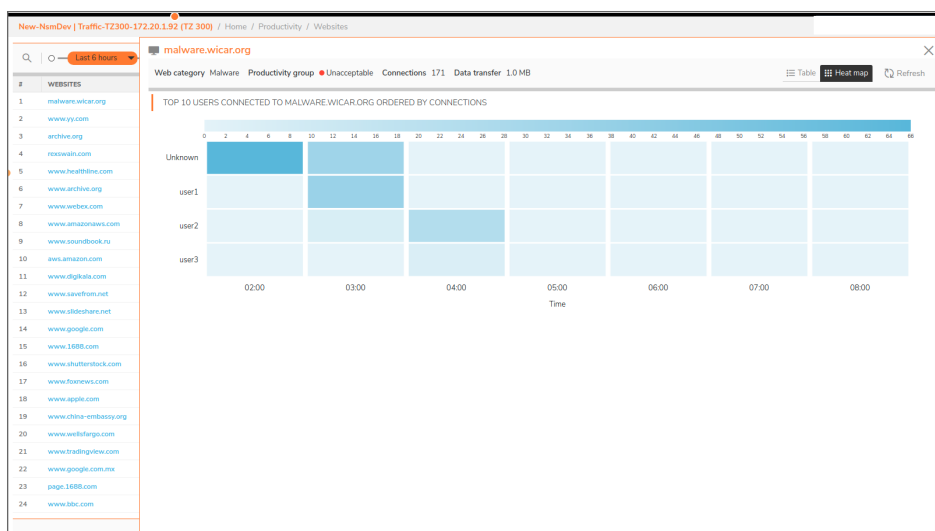
At the top of the table you can find website information such as web category, productivity group, connections and data transfer. You can use the **Limit** drop down button to set the limit of the number of users. You can also use the **Settings** button to refresh the page, edit the columns and export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

① **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 group	Connections	Data transfer	Limit	Table	Heat map	Settings
1	malware.wicar.org	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
1	malware.wicar.org	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
2	www.vy.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
3	archive.org	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
4	renewal.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
5	www.healthline.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
6	www.archive.org	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
7	www.webex.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
8	www.amazon.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
9	www.soundbook.ru	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
10	aws.amazon.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
11	www.digikala.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
12	www.savefrom.net	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
13	www.slideshare.net	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
14	www.google.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
15	www.1688.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
16	www.shutterstock.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
17	www.foxfocus.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
18	www.apple.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
19	www.china-embassy.org	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
20	www.wellfargo.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
21	www.tradingview.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
22	www.google.com.mx	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
23	page.1688.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings
24	www.bbc.com	Malware	Unacceptable	171	1.0 MB	50	Table	Heat map	Settings

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.

① **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.

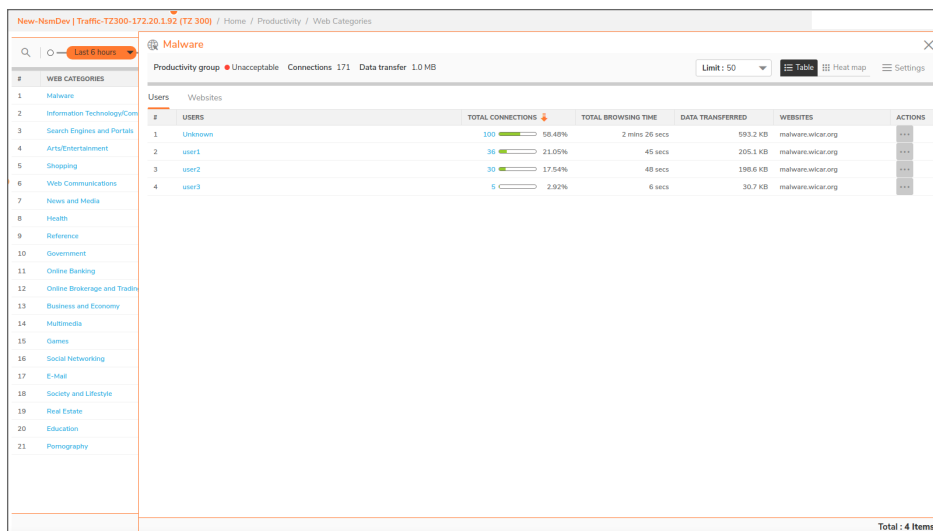
The User table shows the following information:

- **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.

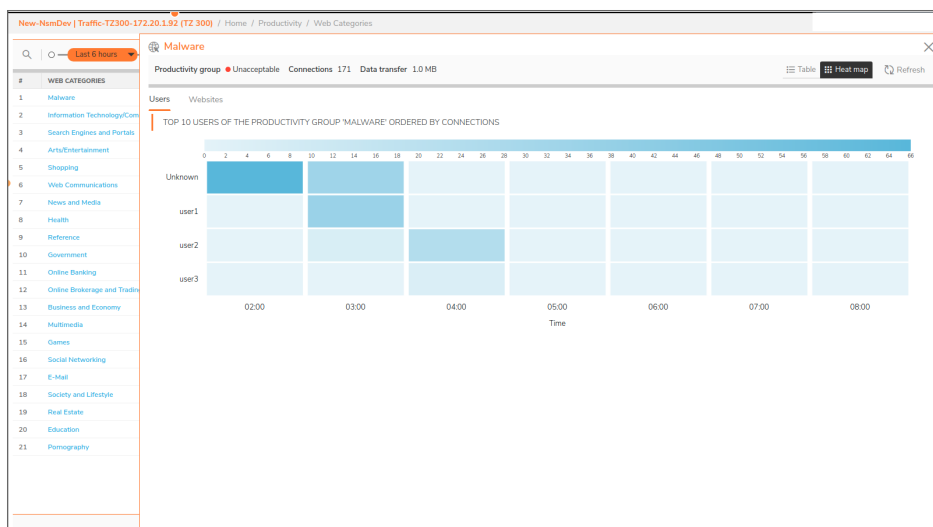
The Websites table shows the following information:

- **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.

① **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.



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.

① | **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.

Documentation Team | Nsv200-172.20.0.209 (Nsv 200) / Home / Reports / Rules

Summary: ALL RULES 2, SUCCESS 2 (100%), FAILED 0 (0%), IN PROGRESS 0 (0%)

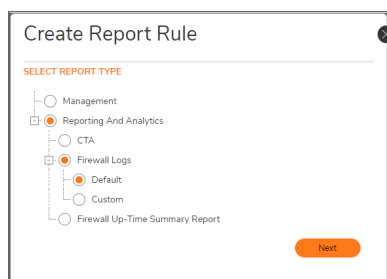
Search: [] + Add Delete Refresh Column Selection

#	NAME	INTERVAL TYPE	REPORT TYPE	DELIVERY TYPE	RUN TYPE	LAST RUN TIME	NEXT RUN TIME	LAST RUN STATUS	ACTION
1	abc	Weekly	Flow	Saved Report	Scheduled	2021-08-12 12:54	2021-08-15 05:30	Success	...
2	ABC	Daily	Custom	Saved Report	Scheduled	2021-08-12 12:53	2021-08-13 05:30	Success	...

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.**

Create Report Rule

Reporting And Analytics / CTA

1 2 3 4
REPORT CONFIGURATION DEVICE SELECTION DELIVERY CONFIGURATION REVIEW

REPORT CONFIG

Report Name

Report Description

Cover Title

IP version

REPORTS

☒ Select All

☒ 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.

Create Report Rule

✓

✓

3

4

REPORT CONFIGURATION

DEVICE SELECTION

DELIVERY CONFIGURATION

REVIEW

Run Type

☒ Scheduled
 ☐ On-Demand

Delivery Interval

☐ Daily
 ☒ Weekly
 ☐ Monthly

Schedule Time

05:30 AM - 06:30 AM ▼

Day

Sunday ▼

Delivery Type

☒ Save Report
 ☐ Email

Password Protect

☐

Previous

Next

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

Create Report Rule

Reporting And Analytics / CTA

✓

✓

3

REPORT CONFIGURATION

DELIVERY CONFIGURATION

REVIEW

Name

CTA

Report Interval

Weekly

Report Type

Reporting And Analytics/CTA

Report Delivery

Save Report

Report Configuration

CTA Reports

Previous

Save

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.

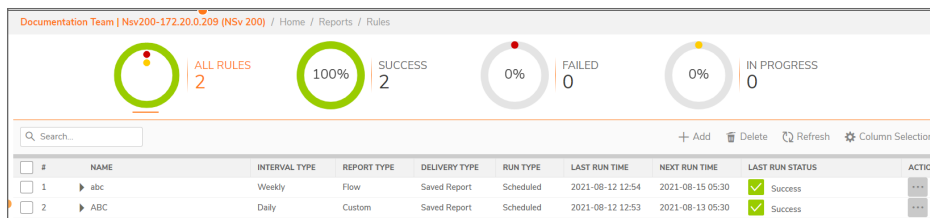
① | **NOTE:** The **Default Report Rules** feature is the same for both NSM on-prem and SaaS versions.

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.



The screenshot shows the 'Default Report Rules' page. At the top, there are four circular progress indicators: 'ALL RULES' (2), 'SUCCESS' (100%), 'FAILED' (0%), and 'IN PROGRESS' (0%). Below these is a search bar and a table of reports. The table has columns: #, NAME, INTERVAL TYPE, REPORT TYPE, DELIVERY TYPE, RUN TYPE, LAST RUN TIME, NEXT RUN TIME, LAST RUN STATUS, and ACTION. There are two rows of reports listed.

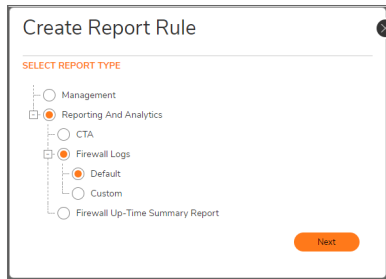
#	NAME	INTERVAL TYPE	REPORT TYPE	DELIVERY TYPE	RUN TYPE	LAST RUN TIME	NEXT RUN TIME	LAST RUN STATUS	ACTION
1	abc	Weekly	Flow	Saved Report	Scheduled	2021-08-12 12:54	2021-08-15 05:30	Success	...
2	ABC	Daily	Custom	Saved Report	Scheduled	2021-08-12 12:53	2021-08-13 05:30	Success	...

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.

① | **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.

Create Report Rule

✓

✓

3

4

REPORT CONFIGURATION

DEVICE SELECTION

DELIVERY CONFIGURATION

REVIEW

Run Type

☒ Scheduled ☐ On-Demand

Delivery Interval

☐ Daily ☒ Weekly ☐ Monthly

Schedule Time

05:30 AM - 06:30 AM ▼

Day

Sunday ▼

Delivery Type

☒ Save Report ☐ Email

Password Protect

☐

Use Custom Logo

☐

Previous

Next

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

Create Report Rule

REPORT CONFIGURATION DEVICE SELECTION DELIVERY CONFIGURATION **4 REVIEW**

Name Intrusion Report

Report Interval Weekly

Report Type Reporting And Analytics/Flow Logs/Default

Report Delivery Save Report

Report Configuration

- RealTime Reports
- Dashboard Reports
- Details Reports

Device Selection

- Tenant

Previous **Save**

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

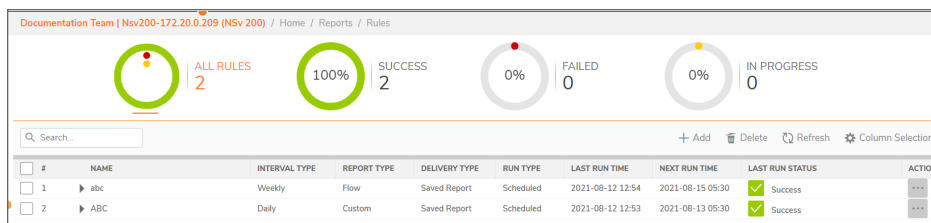
Firewall Up-Time Summary Report Rules

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.

① **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

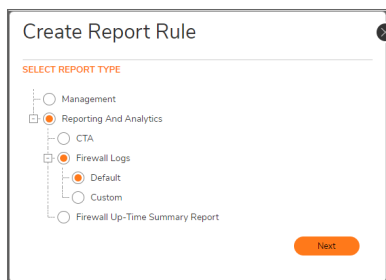
Go to **Reports > Rules** to view a list of all the reports that have been defined. The details of each report are shown in the table.



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**.

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

- 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.

① | **NOTE:** You need to have NSM advance license to view and manage the Custom Reports.

① | **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.

#	NAME	INTERVAL TYPE	REPORT TYPE	DELIVERY TYPE	RUN TYPE	LAST RUN TIME	NEXT RUN TIME	LAST RUN STATUS	ACTION
1	abc	Weekly	Flow	Saved Report	Scheduled	2021-08-12 12:54	2021-08-15 05:30	Success	...
2	ABC	Daily	Custom	Saved Report	Scheduled	2021-08-12 12:53	2021-08-13 05:30	Success	...

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.

CREATE REPORT RULE

SELECT REPORT TYPE

- Management
- ☒ Reporting And Analytics
 - CTA
 - Firewall Logs
 - ☒ Default
 - Custom
 - Firewall Up-Time Summary Report

Next

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.

The screenshot shows the 'Create Report Rule' interface with a progress bar at the top indicating four steps: 1. BASIC INFO (active), 2. SETUP CONTENT, 3. REPRESENTATION, and 4. REVIEW. The form fields are as follows:

- Logo:** A box containing the 'SONICWALL' logo with a pencil icon for editing. Below it, text reads: 'This will be used for report customization ⓘ'.
- Report Title:** A text input field containing 'social-media-analysis'.
- Run Type:** Two radio buttons: 'On-Demand' (selected) and 'Scheduled'.
- Time Period:** A slider control set to '7 Days'.
- Description:** A text area containing 'My organisation social media data analysis.'
- Delivery Type:** Two checkboxes: 'Save Report' (checked) and 'Email'.
- Password Protected:** A toggle switch currently turned off.

At the bottom of the form are two buttons: 'Previous' and 'Next'.

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.
- ① **NOTE:** The scope selector option is only available on custom reports for the Manager View and not the Firewall View.

Create Report Rule

Reporting And Analytics / Flow Logs / Custom

1 BASIC INFO 2 SETUP CONTENT 3 REPRESENTATION 4 REVIEW

SECTION / TEST

Section Title: Test

Scope: TZ300-172.20.1.60

Filters: Custom Predefined

Representation Type: Time Series Chart

Time Series Data: Number of Distinct...

Show Representation: ☐

SCOPE SELECTOR

- DevTest-Productivity RReports
 - Root Group
 - sample
 - 10116-9
 - kl
 - Nsv200-172.20.0.141
 - Nsv200-172.20.0.90
 - TZ300-172.20.1.60
 - TZ300-172.20.1.85
 - Dirty-NSV270-172.20.0.193
 - TZ300p-172.20.1.78
 - NSV200-172.20.0.189
 - NSV200-172.20.0.228
 - NSV-172.20.0.245

+ Add Section

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

Filters			
Custom Predefined			
Q			
FILTER NAME	FILTER CONTENT	CREATED BY	CREATED ON
social-media	App Categories : SOCIAL-NETWORKING	NSM Administrator	2021-08-02 23:34
networking	App Categories : Networking	NSM Administrator	2021-07-30 21:08
mysocialactivity	App Categories : SOCIAL-NETWORKING	NSM Administrator	2021-07-30 16:44
low	App Risk : Low	NSM Administrator	2021-07-30 13:55

Filters

Custom

Predefined

FILTER NAME

Applications

Users

Sources

- **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.

Create Report Rule

Reporting And Analytics / Flow Logs / Custom

1

2

3

4

BASIC INFO

SETUP CONTENT

REPRESENTATION

REVIEW

SECTION / SOCIAL-MEDIA-TRENDS

Delete Edit Saved

Section Title

social-media-trends

Filters

Custom

Predefined

FILTER NAME	FILTER CONTENT	CREATED BY	CREATED ON
social-media	App Categories : SOCIAL-NETWORKING	NSM Administrator	2021-08-02 23:34
networking	App Categories : Networking	NSM Administrator	2021-07-30 21:08
mysocialactivity	App Categories : SOCIAL-NETWORKING	NSM Administrator	2021-07-30 16:44
low	App Risk : Low	NSM Administrator	2021-07-30 13:55
...

Representation Type

☒ Time Series Chart
 ☐ Data Table

Time Series Data

Number of Distinct...

Number of Distinct...

Show Representation

☐

Previous

Next

+ Add Section



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.

Create Report Rule

Reporting And Analytics / Flow Logs / Custom

1 BASIC INFO 2 **SETUP CONTENT** 3 REPRESENTATION 4 REVIEW

SECTION / SOCIAL-MEDIA-AGGREGATION [Delete] [Edit] [Saved]

Section Title: social-media-aggregation

Filters: Custom | Predefined

FILTER NAME	FILTER CONTENT	CREATED BY	CREATED ON
python	Application : Python Default URL Library	NSM Administrator	2021-07-27 21:13
omdep	App Risk : Low Initiators : 192.168.78.2	NSM Administrator	2021-07-27 15:23
om	Application : Wget	NSM Administrator	2021-07-26 23:46
appCat	App Categories : MISC-APPS App Risk : Low	NSM Administrator	2021-07-25 21:11

Representation Type: ☐ Time Series Chart ☒ Data Table

Number of rows: 20

Grouping Criterion: Users x Responders x Threat Type x

Aggregation Criterion: Number of connec... x Total Data Transfe... x

[Previous] [Next]

- **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 you 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.

Create Report Rule

Reporting And Analytics / Flow Logs / Custom

BASIC INFO SETUP CONTENT REPRESENTATION REVIEW

Report Type Reporting And Analytics / Flow Logs / Custom

Report Name social-media-analysis

Schedule Type On-Demand

Time Period 7 Days

Description My organisation social media data analysis.

Report Content

SOCIAL-MEDIA-TRENDS

social-media

App Categories: SOCIAL-NETWORKING

SOCIAL-MEDIA-AGGREGATION

social-media

App Categories: SOCIAL-NETWORKING

Previous Finish

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.

#	NAME	INTERVAL TYPE	REPORT TYPE	DELIVERY TYPE	RUN TYPE	LAST RUN TIME	NEXT RUN TIME	LAST RUN STATUS	ACTION
1	social-media-analysis		Custom	Saved Report	On-Demand	2023-08-02 23:46		Success	...

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

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.

NSM20-DEMO-NEW / 2020-02-24 14:14:14 / Monitor / Alerts & Notifications / Rules										
<div> <input type="text" value="Search..."/> + Add Rule 🗑 Delete 📄 Export 🔄 Refresh ⚙ Column Selection </div>										
<input type="checkbox"/>	#	NAME	TYPE	SUB TYPE	DETAILS	REDUNDANCY	PRIORITY	ACTION	ENABLE/DISABLE	CONFIGURE
<input type="checkbox"/>	▶ 1	AppBW_test	Network Usage	App Bandwidth	50 Mbps	2 min	Medium	📢 📧	<input checked="" type="checkbox"/>	✎ 🗑
<input type="checkbox"/>	▶ 2	InterfaceBW_test	Network Usage	Interface Bandwidth	10 Mbps	2 min	Medium	📢 📧	<input checked="" type="checkbox"/>	✎ 🗑

Creating an alert rule:

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

Add Rule

1

2

3

DETAILS ACTION REVIEW

BASIC DETAILS

Rule Name

Enter the name for the rule.

Priority Level

Medium

Set Redundancy Filter

☐ 2 min
 ☐ ⑦

Alert Type

Network Usage

Sub-Type

App Bandwidth

App Bandwidth (Mbps) >

3.95

3

2

1

0

App Bandwidth (Mbps)

Trend (Last 24 Hours from Mo

Cancel

Next

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.

Add Rule

1 2 3
DETAILS ACTION REVIEW

BASIC DETAILS

Rule Name

Rule Priority Level

Set Redundancy Filter

Alert Type

Sub-Type

VPN Tunnel Name

VPN Tunnel Status

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.

NSM20-DEMO-NEW 2020-06-19 09:00:00 / Monitor / Alerts & Notifications / History									
<div><input type="text" value="Search..."/></div> <div>Limit: 50 Entries</div> <div>Export</div> <div>Refresh</div> <div>Column Selection</div>									
#	TIME	DETAILS	INFO	SERIAL	TYPE	SUB TYPE	PRIORITY	ALERT NAME	<input checked="" type="checkbox"/> Time
▶ 1	2020-06-18 10:21	10 Mbps	info = Interface Bandwidth :: 16 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Details
▶ 2	2020-06-18 10:45	10 Mbps	info = Interface Bandwidth :: 18 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Info
▶ 3	2020-06-18 14:12	10 Mbps	info = Interface Bandwidth :: 10 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Serial
▶ 4	2020-06-18 15:33	10 Mbps	info = Interface Bandwidth :: 10 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Type
▶ 5	2020-06-18 17:35	10 Mbps	info = Interface Bandwidth :: 18 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Sub Type
▶ 6	2020-06-18 17:45	10 Mbps	info = Interface Bandwidth :: 54 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Priority
▶ 7	2020-06-19 08:48	10 Mbps	info = Interface Bandwidth :: 10 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Alert Name
▶ 8	2020-06-19 09:00	10 Mbps	info = Interface Bandwidth :: 11 Mbps	2CB8ED3AF4A0	Network Usage	Interface Bandwidth	Medium	InterfaceBW_test	<input checked="" type="checkbox"/> Action

To export historic alerts:

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

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.

① | **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.

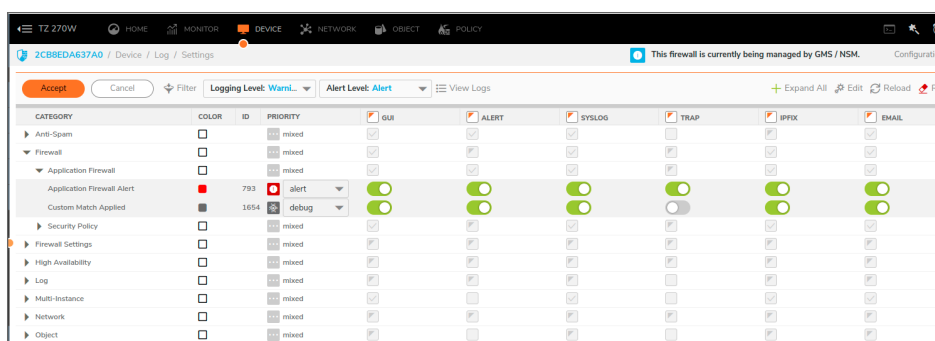
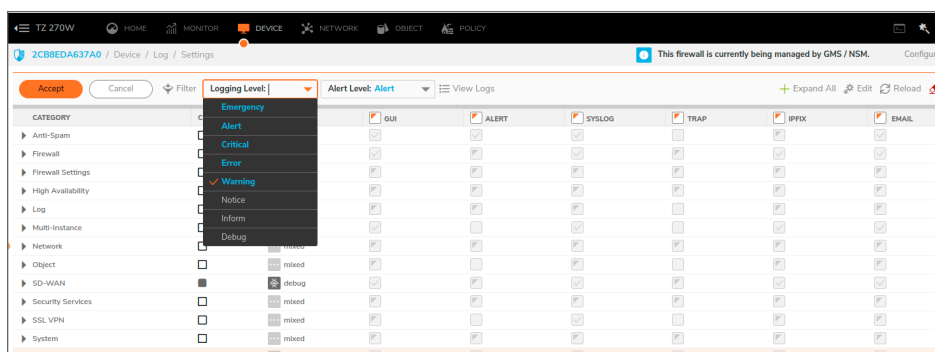
#	TIME	ID	CATEGORY	PRIORITY	MESSAGE	SOURCE IP	SOURCE	SOURCE	DESTINATION IP	DESTINA	DESTINA
1	12:15:20 Oct 22	998	Users	Warning	GUI administration session ended	192.168.11.134	-	X1	10.5.158.187	443	X1
2	12:15:20 Oct 22	262	Users	Warning	Administrator logged out - inactivity timer expired	192.168.11.134	-	X1	10.5.158.187	443	X1
3	12:00:36 Oct 22	995	Users	Warning	Configuration mode administration session ended	127.0.0.1	-	X1	-	-	X1
4	12:00:35 Oct 22	994	Users	Warning	Configuration mode administration session started	127.0.0.1	-	X1	-	-	X1
5	12:00:27 Oct 22	995	Users	Warning	Configuration mode administration session ended	127.0.0.1	-	X1	-	-	X1
6	12:00:26 Oct 22	994	Users	Warning	Configuration mode administration session started	127.0.0.1	-	X1	-	-	X1
7	12:00:16 Oct 22	995	Users	Warning	Configuration mode administration session ended	127.0.0.1	-	X1	-	-	X1
8	12:00:15 Oct 22	994	Users	Warning	Configuration mode administration session started	127.0.0.1	-	X1	-	-	X1
9	12:00:06 Oct 22	995	Users	Warning	Configuration mode administration session ended	127.0.0.1	-	X1	-	-	X1
10	12:00:05 Oct 22	994	Users	Warning	Configuration mode administration session started	127.0.0.1	-	X1	-	-	X1
11	12:00:05 Oct 22	995	Users	Warning	Configuration mode administration session ended	192.168.11.134	-	X1	10.5.158.187	443	X1
12	12:00:05 Oct 22	997	Users	Warning	Non-config mode GUI administration session started	192.168.11.134	-	X1	10.5.158.187	443	X1
13	12:00:04 Oct 22	994	Users	Warning	Configuration mode administration session started	192.168.11.134	-	X1	10.5.158.187	443	X1
14	12:00:00 Oct 22	997	Users	Warning	Non-config mode GUI administration session started	192.168.11.134	-	X1	10.5.158.187	443	X1
15	12:00:00 Oct 22	236	Users	Warning	WAN zone administrator login allowed	192.168.11.134	-	X1	10.5.158.187	443	X1

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.

#	TIME	ID	CATEGORY	PRIORITY	MESSAGE	SOURCE IP	SOURCE	SOURCE	DESTINATION IP	DESTINA	DESTINA
1	12:15:20 Oct 22	998	Users	Warning	GUI administration session ended	192.168.11.134	-	X1	10.5.158.187	443	X1

General	Protocol	NAT	Policy	Traffic	Others	All
Time	12:15:20 Oct 22					
ID	998					
Category	Users					
Group	Authentication Access					
Event	GUI Administration Session End					
Message Type	Standard Note String					
Priority	Warning					
Message	GUI administration session ended					
Source Name	-					
Destination Name	-					
Notes	User: admin					
Source IP	192.168.11.134					
Source Port	-					
Source Interface	X1					
Destination IP	10.5.158.187					
Destination Port	443					
Destination Interface	X1					
Source MAC	-					
Source Zone	-					
Destination MAC	-					
Destination Vendor	XEROX CORPORATION					
Destination Zone	-					
IP Protocol	Tcp					
ICMP Type	-					
ICMP Code	-					
Source NAT IP	-					
Source NAT Port	-					
Destination NAT IP	-					
Destination NAT Port	-					
NAT Policy	-					
Incoming SPI	-					
Outgoing SPI	-					
Access Rule	-					
VPN Policy	-					
IDP Rule	-					
IDP Priority	-					
Transmit Bytes	-					
Receive Bytes	-					
HTTP OP	-					
URL	-					
HTTP Result	-					
Block Category	-					

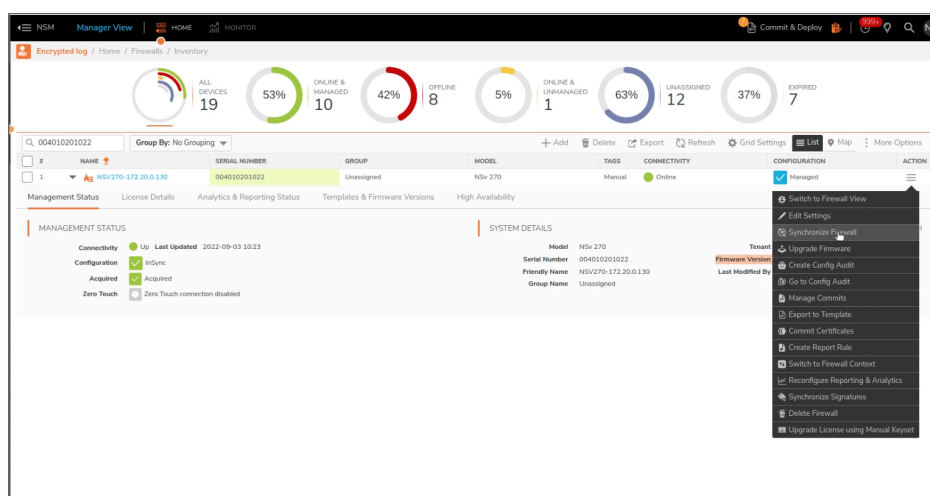
Only the following **Priority** levels for System Logs are supported for egressing to NSM SaaS - Alerts, Critical, Error, and Warning. For a log priority to show up in NSM SaaS, its IPFIX setting has to be enabled on the **Log>Settings** page of the **Device View**.



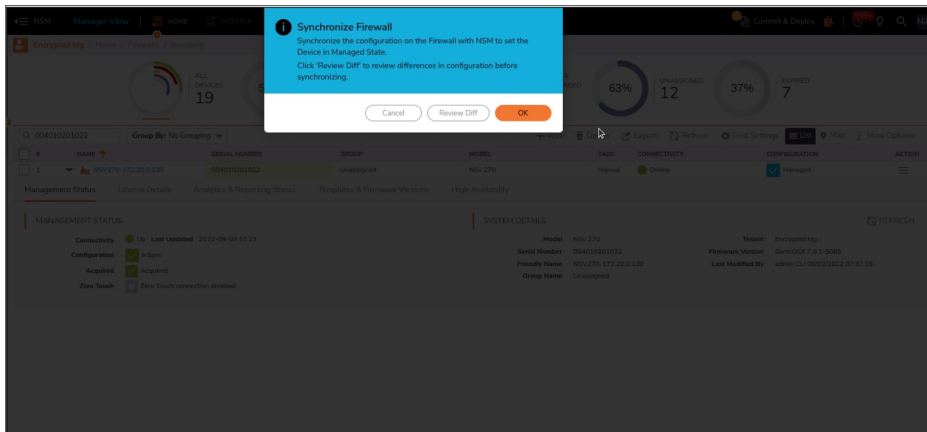
Enabling System Logs for Existing Firewalls

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:

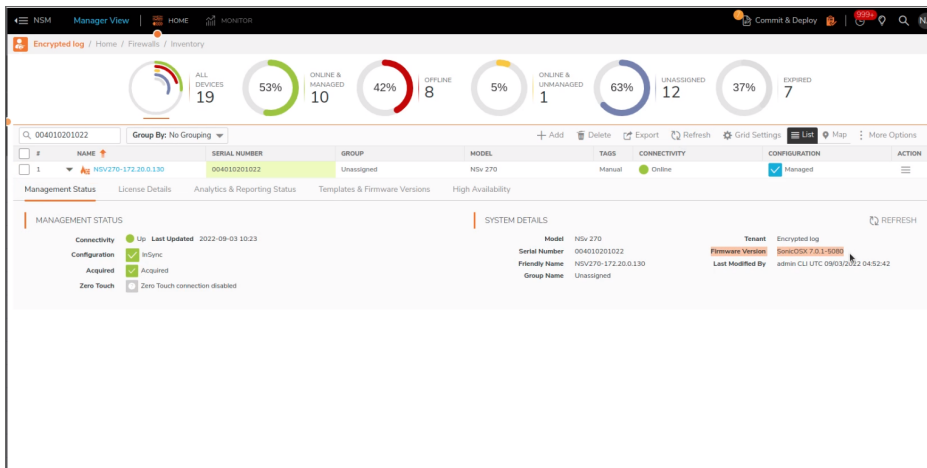
1. Click on **Synchronize Firewall** option under **Actions** on the **Firewall > Inventory** page.



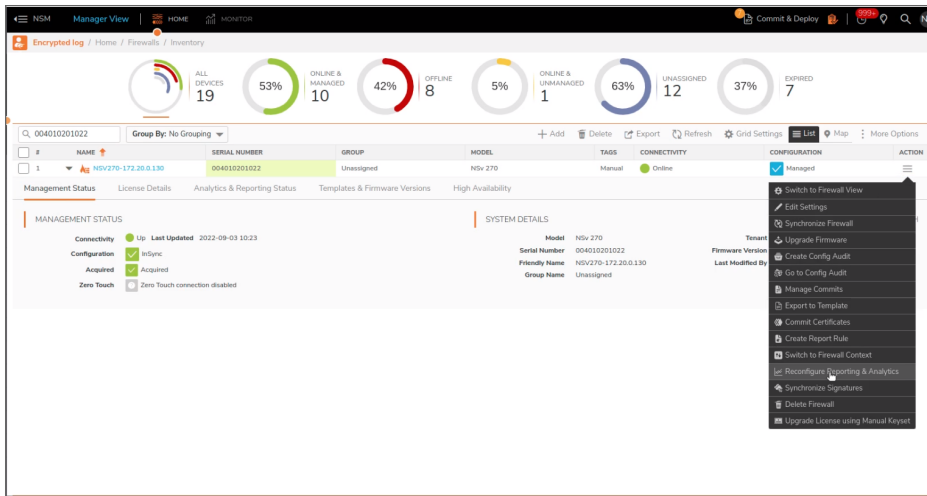
2. Click on **OK** to complete the synchronization.



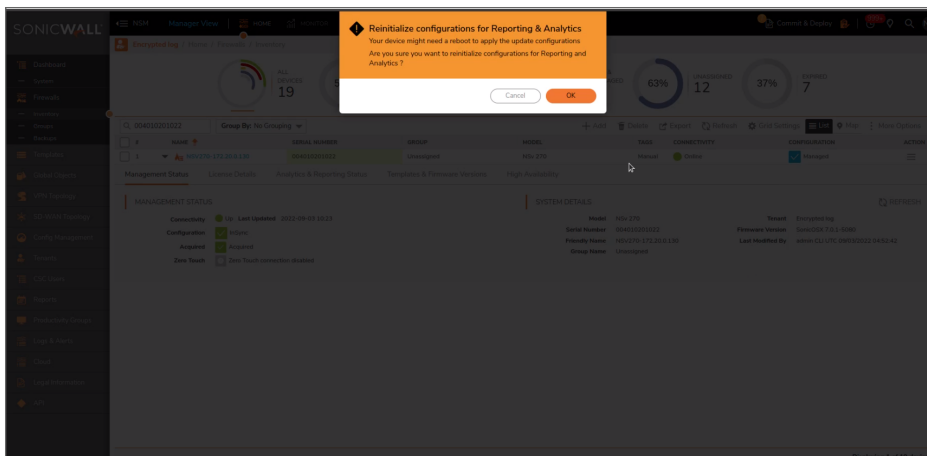
3. You can view the **Firmware Version** under the firewall to confirm if the updated version is appearing on the firewall.



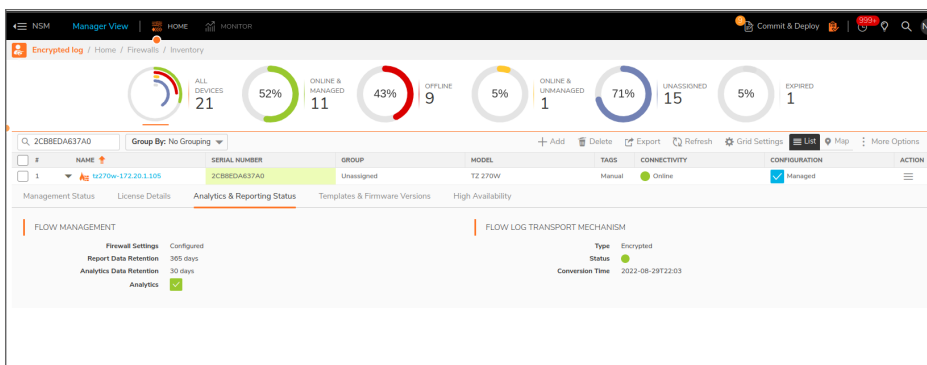
4. Next, click on **Reconfigure Reporting and Analytics** option under **Actions** on the **Firewall > Inventory** page.



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



- 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.

① | **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.

① | **NOTE:** You need to have **NSM Advance License** to view and manage Authentication Logs.

① | **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:

NSM

Firewall View

Home

Monitor

Device

Network

Object

Policy

Commit & Deploy

NA

Encrypted log | 172.20.1.105 (TZ 270V)

Monitor / System Events / Authentication Logs

Admin Login

User Login

Failed Login

7 Days

Custom

Limit: 50

Export

Refresh

Column Selection

#	TIME	INITIATOR IP	USER	INITIATOR INTL...	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 12:26:02	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

Total: 23 item(s)

User Login:

NSM

Firewall View

Home

Monitor

Device

Network

Object

Policy

Commit & Deploy

Encrypted log | 172.20.1.105 (TZ 270W)

/ Monitor / System Events / Authentication Logs

Admin Login

User Login

Failed Login

30 Days

Limit: 50

Export

Refresh

Column Selection

#	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	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	gcouser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
14	2023-04-26 15:18:38	172.20.2.222	gcouser1	X1	X1	0 sec	N/A	User VPN Login	VPN zone remote user login allowed
15	2023-04-26 15:18:38	172.20.2.222	gcouser1	N/A	N/A	0 sec	N/A	XAUTH Success	XAUTH Succeeded with VPN client

Total: 15 item(s)

Failed Login:

NSM Firewall View Home Monitor Device Network Object Policy Commit & Deploy									
Encrypted log (127.0.0.172.20.1.105 (TZ 270W)) Monitor / System Events / Authentication Logs									
Admin Login User Login Failed Login 30 Days									
Limit: 50 Export Refresh Column Selection									
#	TIME	INITIATOR IP	USER	INITIATOR INTE...	DESTINATION IN...	SESSION TIME	SERVICE	EVENT NAME	MESSAGE
1	2023-05-23 11:39:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
2	2023-05-23 11:09:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
3	2023-05-23 10:27:50	172.20.0.8	admin	X1	X1	1 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
4	2023-05-23 10:25:32	172.20.0.8	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
5	2023-05-23 09:39:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
6	2023-05-23 09:32:21	34.215.123.214	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
7	2023-05-23 09:31:21	34.215.123.214	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
8	2023-05-23 09:15:56	3.140.21.189	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
9	2023-05-23 09:13:59	172.20.0.8	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
10	2023-05-23 09:09:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
11	2023-05-23 08:43:11	172.20.0.8	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
12	2023-05-23 08:41:36	172.20.0.8	admin	X1	X1	1 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
13	2023-05-23 08:39:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
14	2023-05-23 07:39:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
15	2023-05-23 06:39:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
16	2023-05-23 05:39:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
17	2023-05-23 05:09:04	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
18	2023-05-23 02:42:44	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
19	2023-05-23 02:26:25	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
20	2023-05-23 01:56:25	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
21	2023-05-23 01:16:25	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
22	2023-05-22 23:56:25	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
23	2023-05-22 23:26:25	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
24	2023-05-22 20:56:25	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
25	2023-05-22 20:26:25	4.78.245.210	admin	X1	X1	0 sec	Web Browser	Wrong Admin Password	Administrator login denied due to bad credentials
Total: 50 item(s)									

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.

n 10.5.158.187 (TZ 80) / Monitor / Logs / Auditing Logs											
Q Search... ✔ 📧 Email Audit Records 📄 Supplemental 📤 Export 🔄 Refresh ⚙️ Grid											
BASIC											
#	AUDIT ID	TRANSACTION ID	TIME	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION S...	USER	FAILURE
▶ 1	168	140	00:17:34 Oct 21 2024			End Configuration Mode			Succeeded	admin	
▶ 2	167	139	00:17:33 Oct 21 2024			Added 'Upgrade Keyset'		encrypted	Succeeded	admin	
▶ 3	166	138	00:17:32 Oct 21 2024			Begin Configuration Mode			Succeeded	admin	
▶ 4	165	137	03:28:54 Oct 17 2024	Allow 'Any' from 'Any' to 'Any'	Firewall Access Rules	'TCP Connection Inactivity Timeout (minutes)'		15	Succeeded	admin	
▶ 5	164	137	03:28:54 Oct 17 2024	Allow 'Any' from 'Any' to 'Any'	Firewall Access Rules	'Enable Logging'		enabled	Succeeded	admin	
▶ 6	163	137	03:28:54 Oct 17 2024	Allow 'Any' from 'Any' to 'Any'	Firewall Access Rules	'Policy Name'		acc	Succeeded	admin	
▶ 7	162	137	03:28:54 Oct 17 2024	Allow 'Any' from 'Any' to 'Any'	Firewall Access Rules	Added 'Policy Action'		Allow 'Any' from 'Any' to 'Any'	Succeeded	admin	
▶ 8	161	136	03:28:50 Oct 17 2024			'Email password'	*****	*****	Succeeded	admin	
▶ 9	160	135	03:28:50 Oct 17 2024			'Log email authentication password'	*****	*****	Succeeded	admin	
▶ 10	159	134	03:28:49 Oct 17 2024			'Visualization server password'	*****	*****	Succeeded	admin	
▶ 11	158	133	03:28:48 Oct 17 2024	WLAN GroupVPN	VPN SA	'Encryption Key'	*****	*****	Succeeded	admin	
▶ 12	157	132	03:28:48 Oct 17 2024	WAN GroupVPN	VPN SA	'Encryption Key'	*****	*****	Succeeded	admin	
03:28:38 Oct 17 2024 NSMv3 Engine											

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
NETWORK USAGE
THREATS
WEB ACTIVITIES

4K
3K
0
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

Commit & Deploy
999+
C1

NOTIFICATION CENTER

THREATS
WEB ACTIVITIES
GEO LOCATION
SYSTEM EVENTS

0
607
0
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.

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