

SOPHOS

Security made simple.



Sophos XG Firewall Reports Guide v16.5

For Sophos Customers

Document Date: December 2016

Copyright Notice

Copyright 2015-2016 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Contents

Reports.....	4
Basics.....	4
Reports Navigation.....	6
Dashboards.....	8
Traffic Dashboard.....	9
Security Dashboard.....	26
Executive Report.....	46
User Threat Quotient (UTQ).....	70
Applications & Web.....	75
User App Risks & Usage.....	75
Blocked User Apps.....	95
Web Risks & Usage.....	106
Blocked Web Attempts.....	126
Search Engine.....	143
Web Server Usage.....	146
Web Server Protection.....	150
User Data Transfer Report.....	155
FTP Usage.....	159
FTP Protection.....	168
Network & Threats.....	175
Intrusion Attacks.....	175
Advanced Threat Protection.....	190
Wireless.....	201
Security Heartbeat.....	205
Sandstorm.....	214
VPN.....	220
VPN.....	220
SSL VPN.....	231
Clientless Access.....	233
Email.....	236
Email Usage.....	237
Email Protection.....	248
Compliance.....	271
HIPAA.....	272
GLBA.....	287
SOX.....	302
FISMA.....	302
PCI.....	314
NERC CIP v3.....	326
CIPA.....	327
Events.....	327
Bookmarks.....	331
Custom.....	331
Custom Web Report.....	331
Custom Mail Report.....	335
Custom FTP Report.....	337
Custom User Report.....	338
Custom Web Server Report.....	351
Settings.....	353

Custom View.....	353
Report Scheduling.....	354
Data Management.....	357
Manual Purge.....	360
Bookmark Management.....	361
Integration with ConnectWise.....	362
Custom Logo.....	363

Reports

Reports provide organizations with visibility into their networks for high levels of security, data confidentiality while meeting the requirements of regulatory compliance.



Note: This feature is not available in models: CR10iNG, CR10wiNG, CR15i, CR15wi, CR15iNG, CR15wiNG, CR15iNG-LE, CR15iNG-4P, CR15wiNG-4P nor in XG85, and XG85w.

Reports offer a single view of the entire network activity. This allows organizations not just to view information across hundreds of users, applications and protocols; it also helps them correlate the information, giving them a comprehensive view of network activity.

Moreover, organizations receive logs and reports related to intrusions, attacks, spam and blocked attempts, both internal and external, enabling them to take rapid action throughout their network.

Given below are some of the salient features of Reports:

- At-a-glance flow graphs show usage trends and web activity.
- The daily summary Executive Report keeps you informed.
- Report anonymization can hide user identities, where needed.
- Built-in Syslog support and automated log backup options.


Basics

This section provides basic instructions on how to view Reports, in addition to information on configuration settings related to Reports.

Given below are common screen components used to generate and view reports:

- [Date Selection](#)
- [Records per chart](#)
- [Page Controls](#)
- [Reports Navigation](#)
- [Search Reports](#)
- [Filter Reports](#)
- [Export to PDF](#)
- [Export to HTML](#)
- [Export to MS Excel](#)
- [Bookmark](#)
- [Schedule](#)

Date Selection

1. Use  icon to select the time interval for which you want to view the reports. By default, the report for the current date is displayed.
2. Click Generate to generate reports for the selected time interval.

Records per chart

Select the number of records (rows) of the report to be displayed per page from Records per chart. A page can have a minimum of 5 and a maximum of 200 rows.







Note: The exported PDF and HTML contains graphs when a report is having 5 or 10 records. For more than 10 records, the report is displayed in tabular format along with the in-line graphs.


Page Controls

Every report displays the first page of the report along with total number of pages available for the report.

Use the following controls to navigate through pages:

- : Navigate to the next page
- : Navigate to the previous page
- : Navigate to the first page
- : Navigate to the last page

Search Reports

Click  icon to perform a search in a given report based on the following search criterion:

- is
- is not
- contains
- does not contain

For example, if you want to perform a search for a user with User Name Joseph in **Users** report under **User Data Transfer Report**, given below are sample results using each search criterion:

- is - Displays details of the user Joseph
- is not - Displays details of all the users other than Joseph
- contains - Displays details of all the users whose User Name or Name contains Joseph
- does not contain - Displays details of all the users whose User Name or Name does not contain Joseph


Filter Reports

A report can be further filtered or drilled-down using a specific filtering criteria.

For example, clicking the User Name hyperlink from the **Users** report under **User Data Transfer Report** will display all the reports specific to the selected user. You can further filter this report by adding another filtering criteria, e.g - Client Type.

The filter criteria is displayed as:



This means the **Users** report is filtered to display data only for the user Joseph when logged in through the Web Client. Click  icon to remove any of the filter(s).

Export to PDF

Click PDF hyperlink given at the top right of a report to export the report in PDF format.

Export to HTML

Click HTML hyperlink given at the top right of a report to export the report in HTML format.

Export to MS Excel

Click EXCEL hyperlink given at the top right of a report to export the report in MS Excel format.

Bookmark

Use this to create a bookmark of a report page at any level of filtering. Click Bookmark hyperlink given at the top right of a report to create a bookmark of the report page. The created bookmark(s) can be viewed from **Reports > Settings > Bookmark Management**.

Schedule

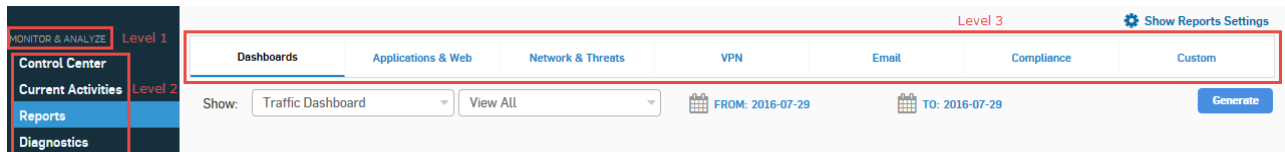
Use this to create a report schedule. Once configured, the Device sends report schedule(s) to specified Email Addresses as per the configured frequency.

Reports Navigation

Navigation bar on the leftmost side provides access to the modules like Monitor & Analyze, Protect, Configure and System.

Reports Navigation

Refer the Monitor & Analyze module to view Reports and configure related settings. Reports module consists of Level 3 report headings.

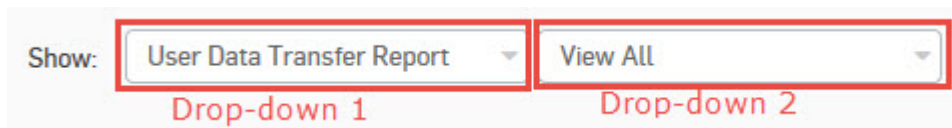


The Reports module includes following Level 3 report headings:

- [Dashboards](#)
- [Applications & Web](#)
- [Network & Threats](#)
- [VPN](#)
- [Email](#)
- [Compliance](#)
- [Bookmarks](#)
- [Custom](#)
- [Settings](#)

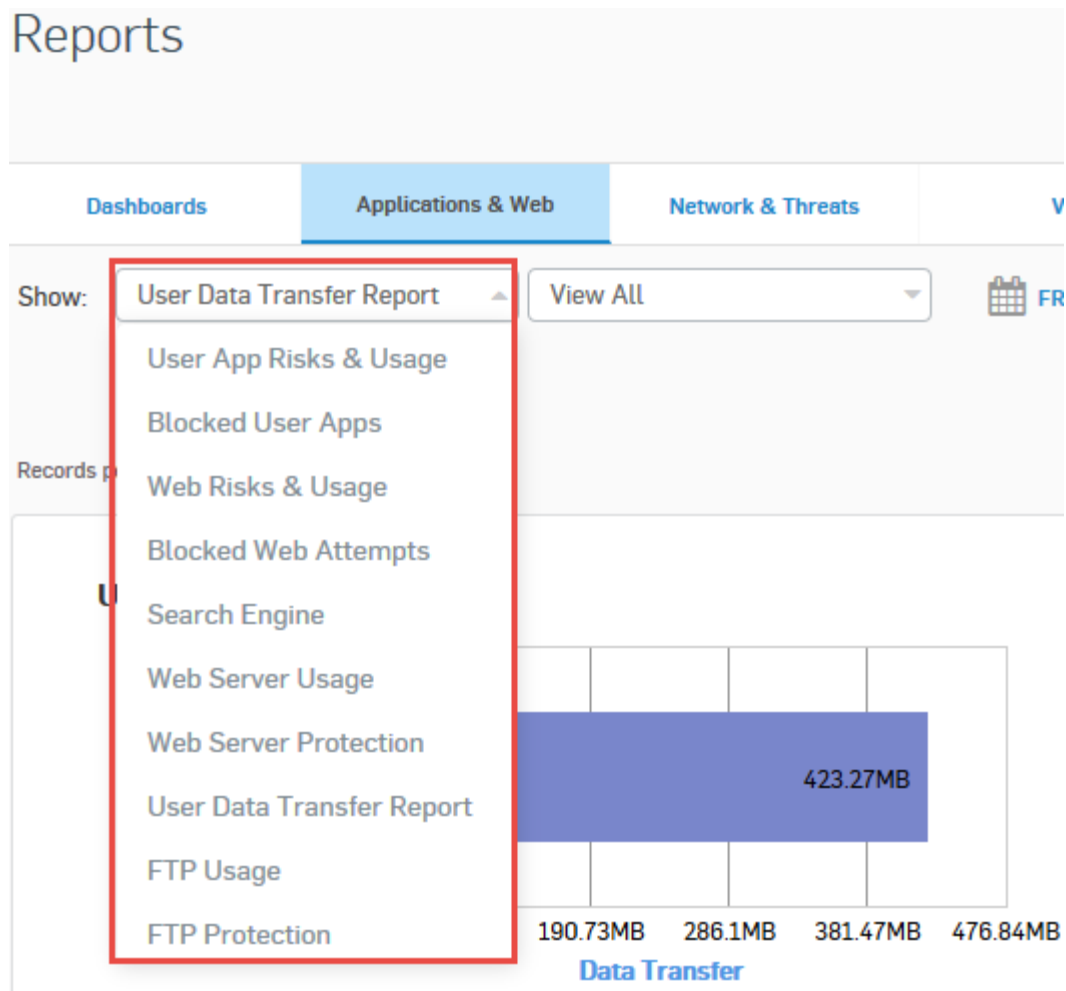
Click a level 2 menu item to view level 3 report headings. Level 3 report headings, display reports dashboard and the underlying reports in widget format.

Each report dashboard shows two drop-downs i.e. drop-down 1 and drop-down 2, as shown in the image below:

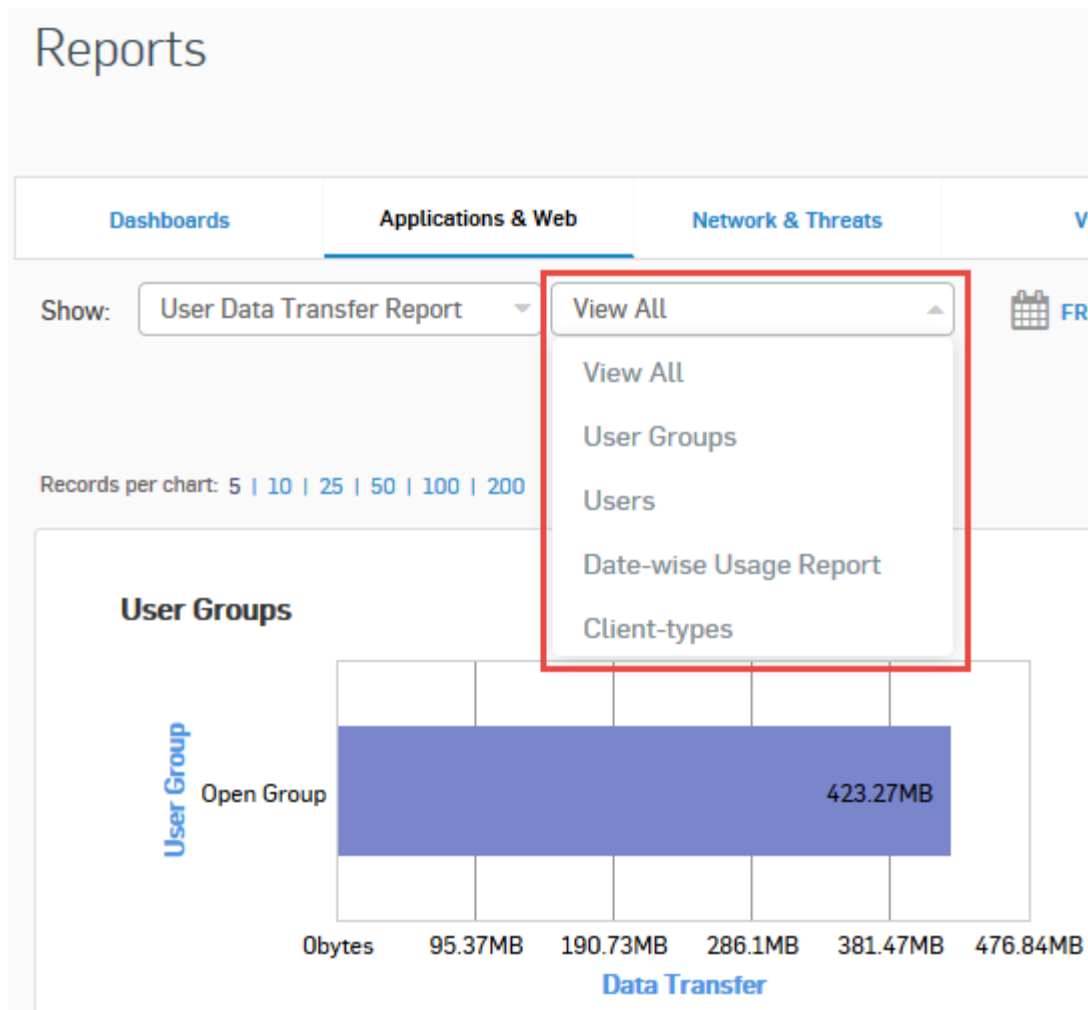


The drop-down 1 includes fellow sub-report items, while drop-down 2 includes fellow reports of sub-reports, displayed as widgets on the reports dashboard. For example, in the image above, we've selected User Data Transfer Report as a sub-report. Use the:

- drop-down 1 to view fellow Level 3 sub-report items, as shown in the image below:

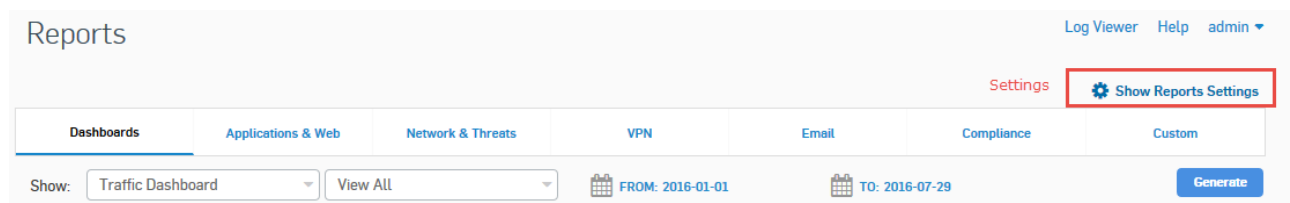


- drop-down 2 to view fellow reports of sub-reports, as shown in the image below:



Settings

To view Settings page, click Show Reports Settings as shown in the below image. To return to the main menu click Close Reports Settings.



Dashboards

Dashboards provide a comprehensive summary of network traffic passing through the Device as well as security threats associated with the processed network traffic.



Note: The Dashboards sub menu items can be accessed from the drop-down 1 given at the upper left corner of the page.

The Reports consists of following Dashboards:

- [Traffic Dashboard](#)

- [Security Dashboard](#)
- [Executive Report](#)
- [User Threat Quotient \(UTQ\)](#)

Traffic Dashboard

The Traffic Dashboard is a collection of widgets displaying comprehensive summary of the network traffic in terms of applications, web categories, users, hosts, source and destination countries, mail traffic and FTP activities.

View the Traffic dashboard from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard**.

The Traffic Dashboard consists of following reports in the form of widgets: These Reports can be accessed by selecting the submenu items from the drop-down 2 level.

- [Applications](#)
- [Applications Categories](#)
- [Application Users](#)
- [Hosts](#)
- [Source Countries](#)
- [Destination Countries](#)
- [Allowed Policies](#)
- [Web Categories](#)
- [Web Users](#)
- [Web Domains](#)
- [Web Servers by Data Transfer](#)
- [Files Uploaded via Web](#)
- [Files Uploaded via FTP](#)
- [Files Downloaded via FTP](#)
- [FTP Servers](#)
- [Mail Traffic Summary](#)
- [Mail Senders](#)
- [Mail Recipients](#)

Applications

This Report displays the list of top applications along with application wise distribution of total data transfer and relative percentage distribution amongst those applications.

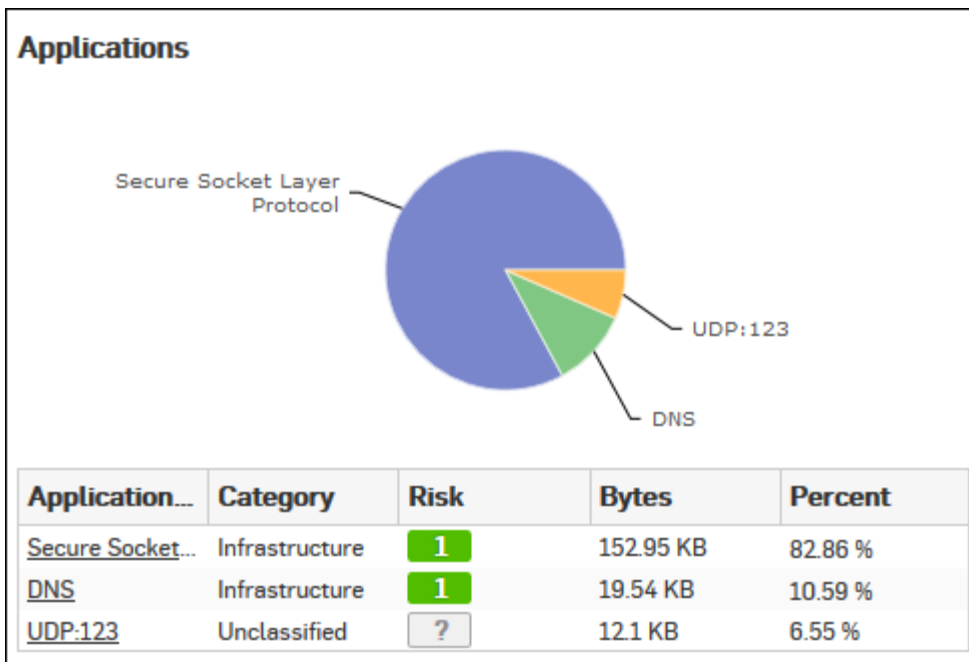
View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Applications & Web**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the report date from the inline calender button provided on top of the page.

The pie chart displays percentage distribution of data transfer per application, while the tabular report contains the following information:

- **Application/Proto:Port:** Name of the application. If the application is not defined in the Device, then this field displays the application identifier as a combination of protocol and port number.
- **Category:** Name of application category as defined in the Device.
- **Risk:** Risk level associated with the application. This is a numeric value. Higher value represents higher risk.
- **Bytes:** The amount of data transferred per application.
- **Percent:** The amount of data transfer per application, in percentage.



Click Application hyperlink in the table or the pie chart to view the [Filtered User App Risks & Usage Reports](#).

Application Categories

This Report displays the list of top application categories along with category wise distribution of the total data transfer and relative percentage distribution among those categories.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Application Categories**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per application category, while the tabular report contains following information:

- Category: Name of the Application category as defined in the Device.
- Bytes: Amount of data transferred.
- Percent: Amount of data transfer in percentage.

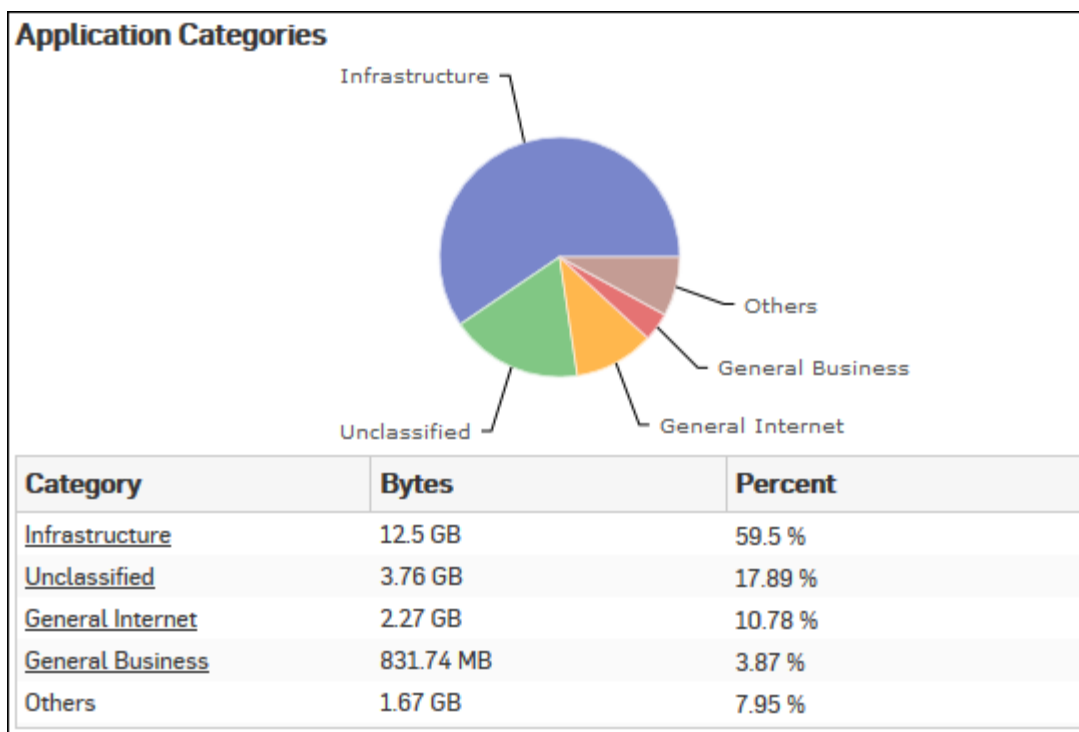


Figure 1: Application Categories

Click the Category hyperlink in the table or the pie chart to view the [Filtered User App Risks & Usage Reports](#).

Application Users

This Report displays list of top users along with the amount of traffic generated for various applications, hosts, destinations, domains and categories.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Application Users**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per user, while the tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined, then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Bytes: Amount of data transferred.
- Percent: Amount of data transfer in percentage.

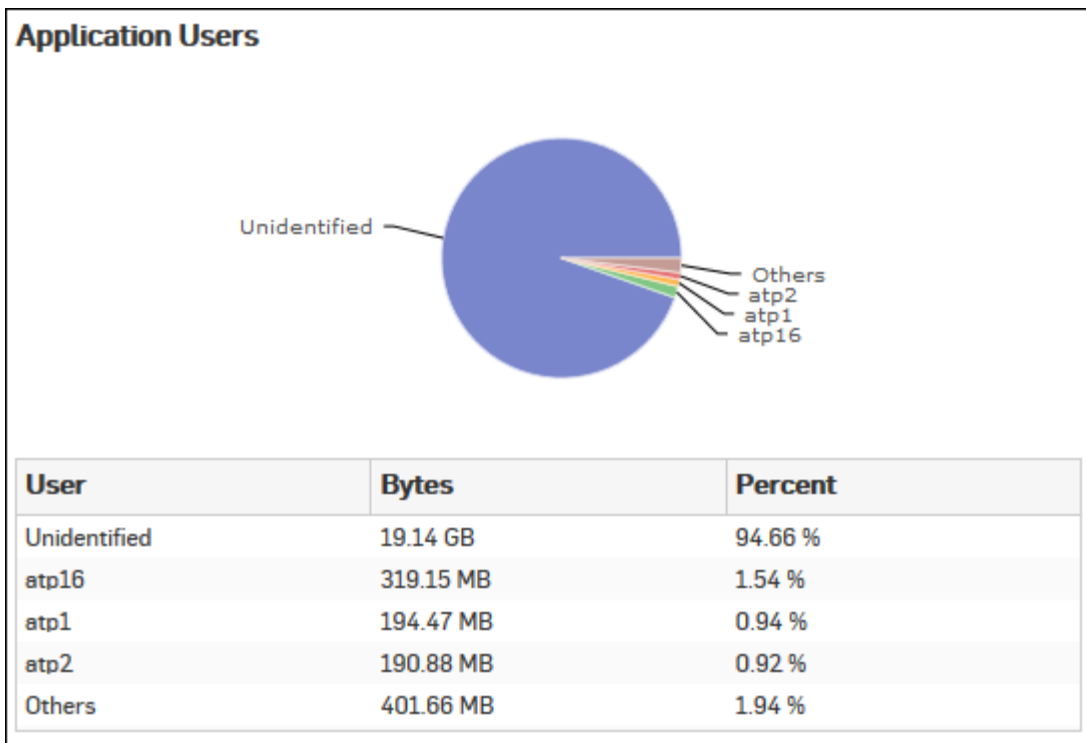


Figure 2: Application Users

Click the User hyperlink in the table or the pie chart to view the [Filtered User App Risks & Usage Reports](#).

Hosts

This Report displays the list of top hosts along with host wise distribution of total data transfer and relative percentage distribution amongst those hosts.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Hosts**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per host, while the tabular report contains following information:

- Host: IP Address of the host.
- Bytes: Amount of data transferred.
- Percent: Amount of data transfer in percentage.

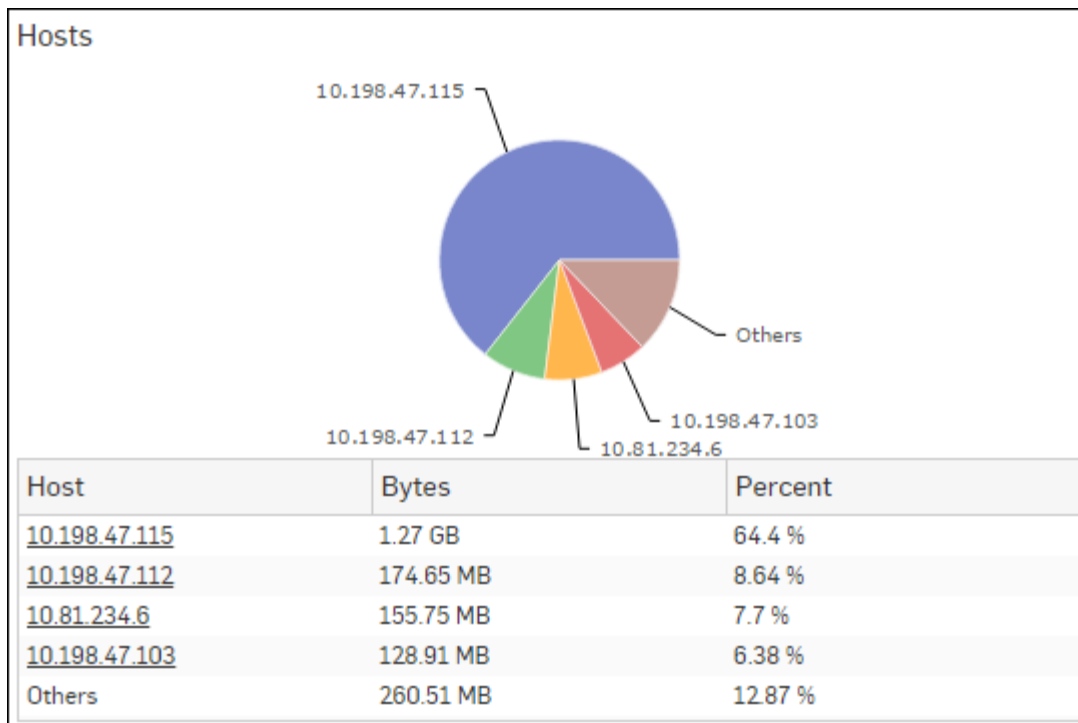


Figure 3: Hosts

Click the Host hyperlink in table or the pie chart to view the [Filtered User App Risks & Usage Reports](#).

Source Countries

This Report displays the list of source countries from where the Internet traffic is originated along with the country wise distribution of total data transfer and relative percentage distribution amongst those countries.

The report is helpful to identify the country of web visitors. To cite a use-case scenario - you might have an e-commerce website, and would like to know the country to which your potential customers belong.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Source Countries**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per source country, while the tabular report contains following information:

- Source Country: Name of the country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Bytes: Amount of data transferred.
- Percent: Amount of data transfer in percentage.

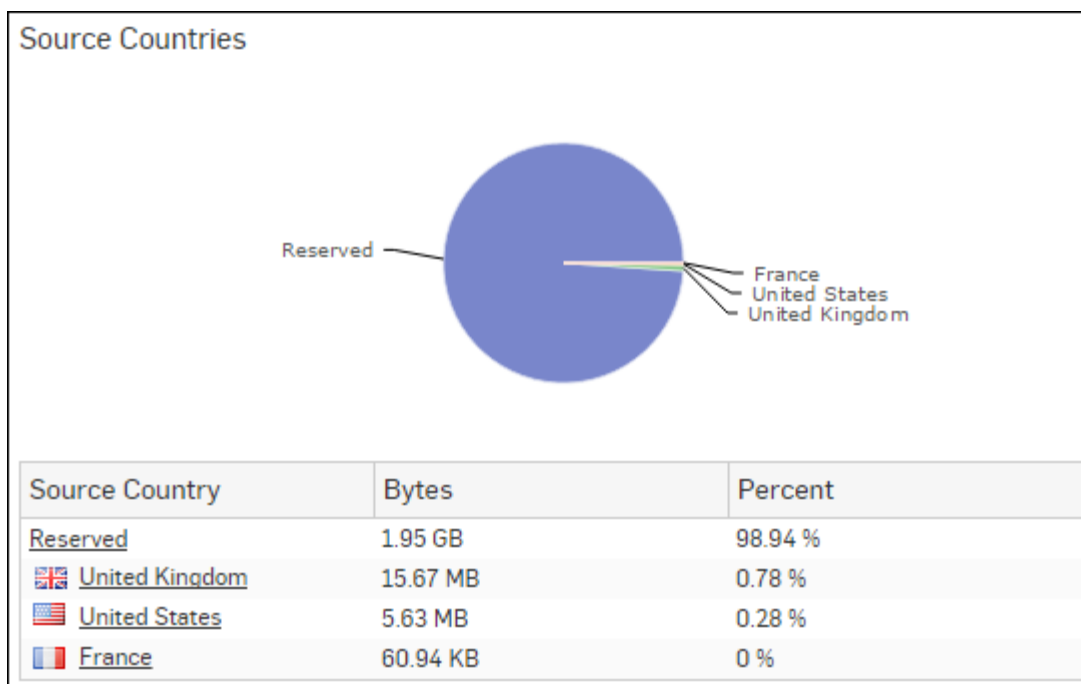


Figure 4: Souce Countries

Click the Source Country hyperlink in table or the pie chart to view the [Filtered User App Risks & Usage Reports](#).

Destination Countries

This Report displays the list of destination countries where the web traffic is directed along with country wise distribution of the total data transfer and relative percentage distribution amongst those countries.

The report is helpful when you need to identify where your web visitors are going to.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Destination Countries**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per destination country, while the tabular report contains following information:

- Destination Country: Name of the country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Bytes: Amount of data transferred.
- Percent: Amount of data transfer in percentage.

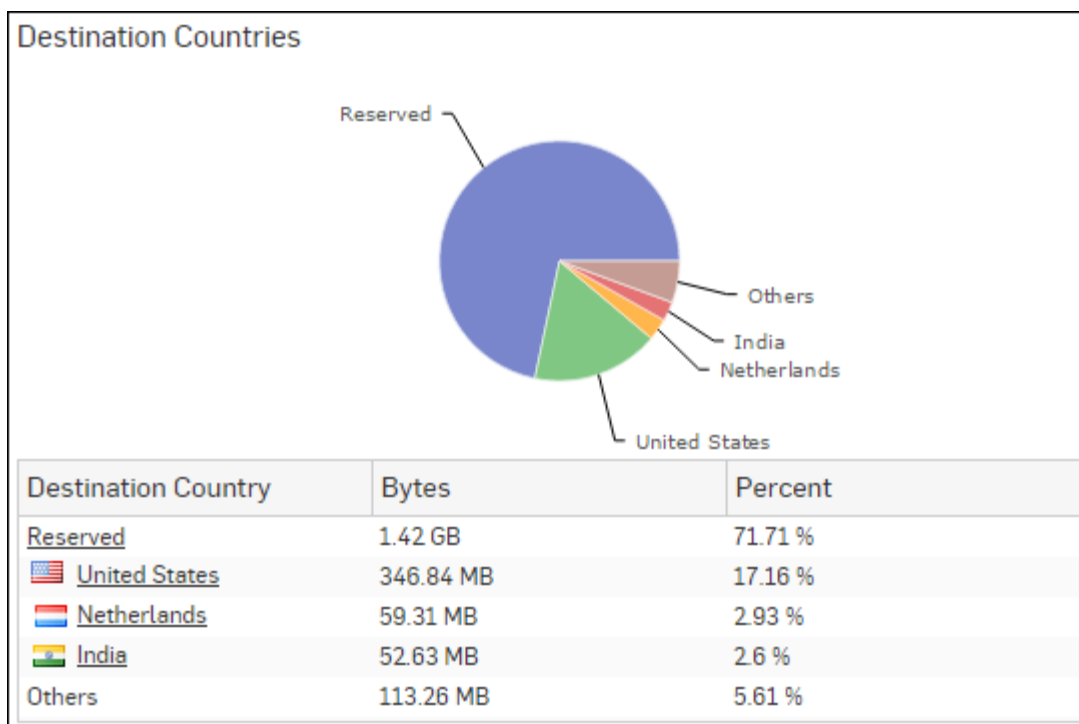


Figure 5: Destination Countries

Click the Destination Country hyperlink in table or the pie chart to view the [Filtered User App Risks & Usage Reports](#).

Allowed Policies

This Report displays the list of rules along with rule wise distribution of the total data transfer and relative percentage distribution amongst those rules.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Allowed Policies**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per Firewall Rule ID, while the tabular report contains following information:

- Rule ID: Firewall Rule ID.
- Bytes: Amount of data transferred.
- Percent: Amount of data transfer in percentage.

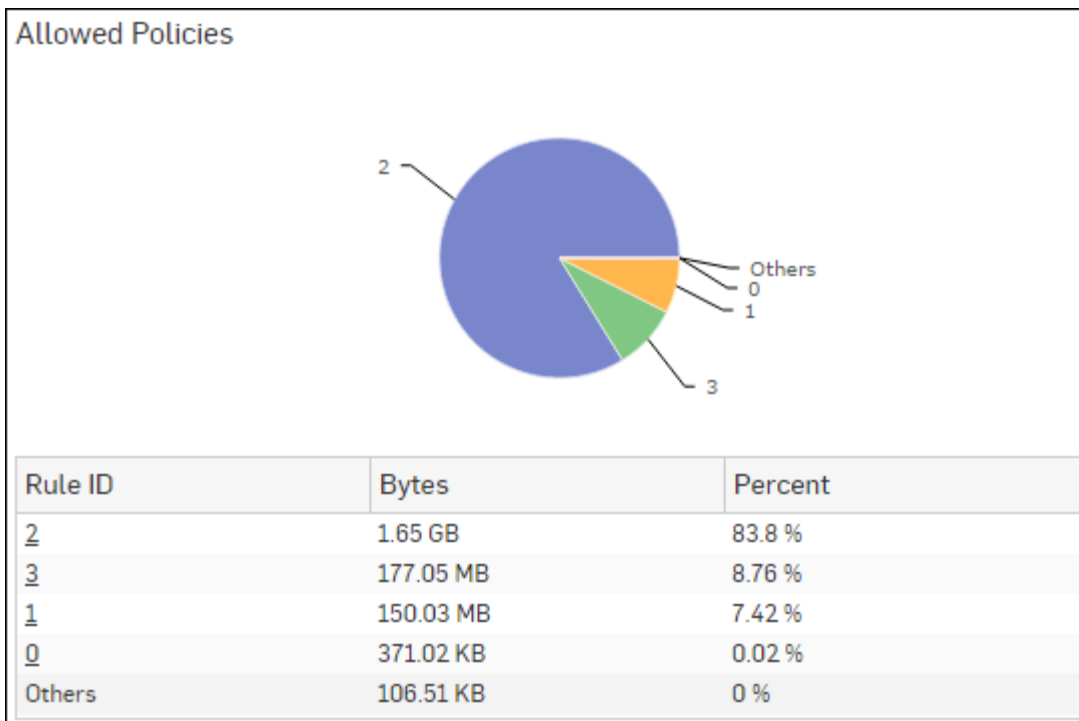


Figure 6: Allowed Policies

Click the Rule ID hyperlink in table or the pie chart to view the [Filtered User App Risks & Usage Reports](#).

Web Categories

This Report displays the list of top web categories along with category wise distribution of total data transfer and relative percentage distribution amongst those categories.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Web Categories**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per web category, while tabular report contains following information:

- Category: Name of the Web category, as defined in the Device.
- Hits: Number of Hits to the Web category.
- Percent: Amount of data transfer in percentage.

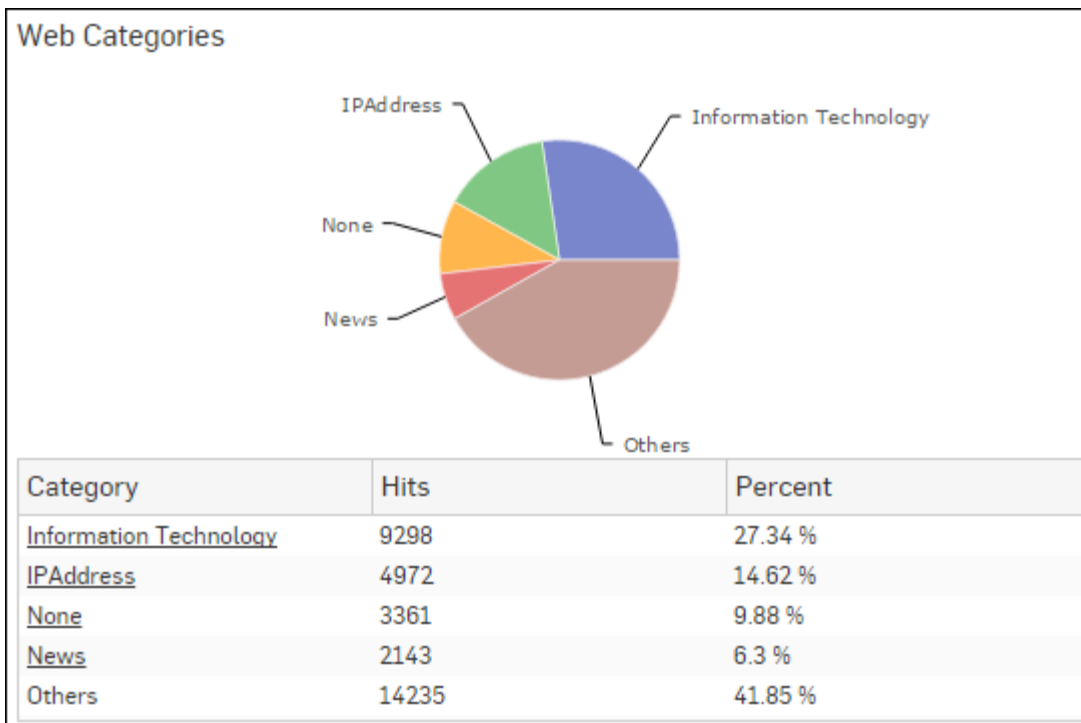


Figure 7: Web Categories

Click the Category hyperlink in the table or the pie chart to view the [Filtered Web Risks & Usage Reports](#).

Web Users

This Report displays the list of Web users along with user wise distribution of total data transfer and relative percentage distribution amongst those Web users.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Web Users**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per user, while the tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Bytes: Amount of data transferred.
- Percent: Amount of data transfer in percentage.

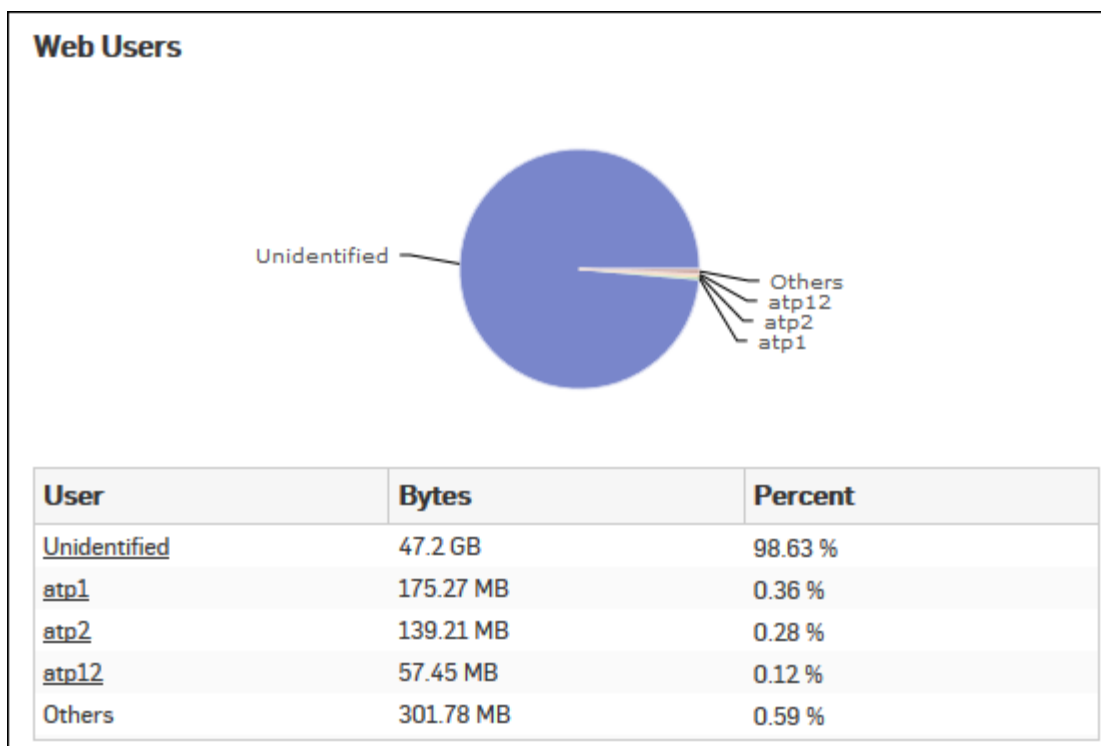


Figure 8: Web Users

Click the User hyperlink in the table or the pie chart to view the [Filtered Web Risks & Usage Reports](#).

Web Domains

This Report displays the list of domains along with domain wise distribution of the total data transfer and the relative percent distribution amongst those domains.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Web Domains**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per domain, while the tabular report contains following information:

- Domain: Displays the name of the domain.
- Bytes: Amount the of data transfer.
- Percent: Displays the amount of data transfer in percentage.

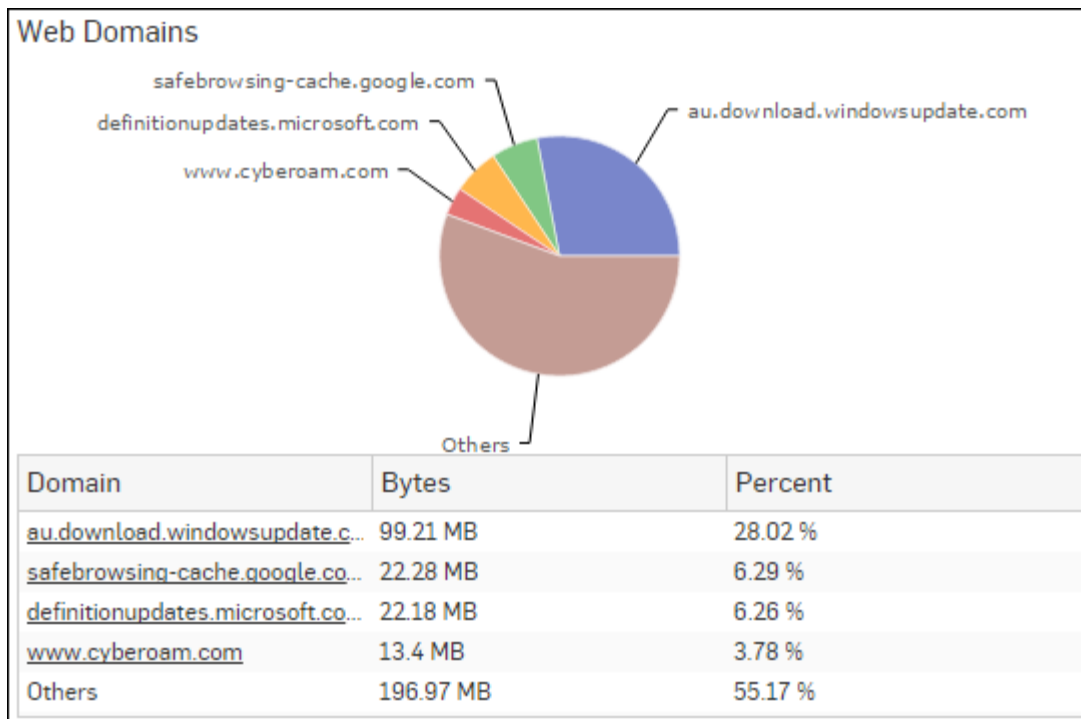


Figure 9: Web Domains

Click the Domain hyperlink in the table or the pie chart to view the [Filtered Web Risks & Usage Reports](#).

Web Server Domains

This Report displays a list of frequently accessed web server domains according to the utilization of bandwidth, along with the number of requests per web server.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Web Server Domains** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of web servers along with the number of bytes while the tabular report contains the following information:

- Web Server Domain: Displays name of the web server domain.
- Bytes: Bandwidth used per web server domain.
- Requests: Number of requests per web server domain.

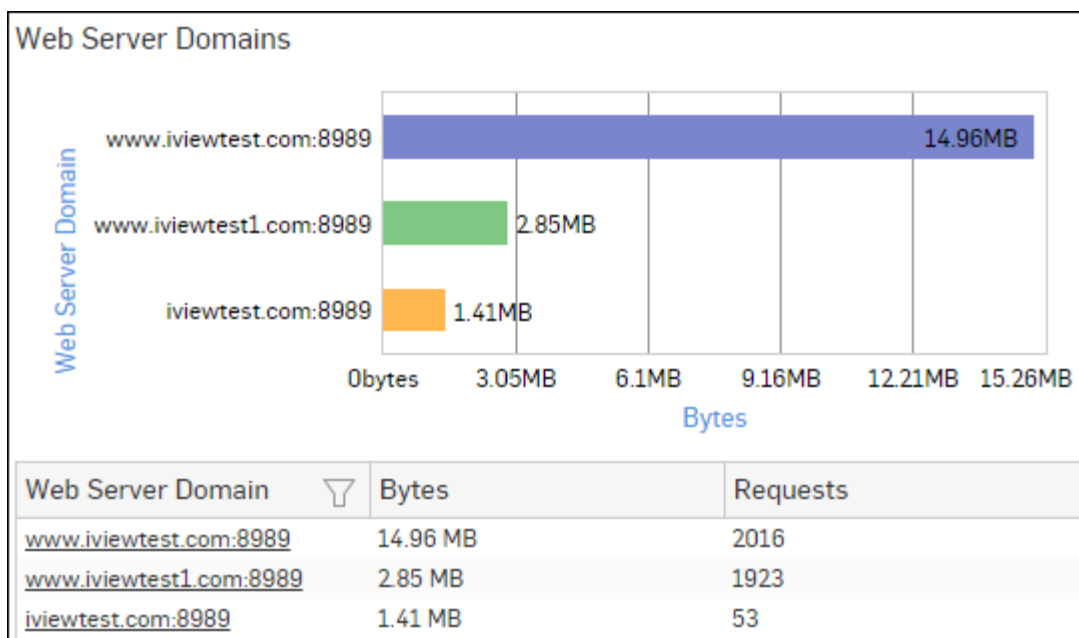


Figure 10: Web Server Domains

Click the Web Server Domain hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

File Uploaded via Web

This Report displays the list of Files Uploaded via web along with date, user, domain name, size and source from which it was uploaded.

View the report from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > File Uploaded via Web**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > File Uploaded via Webs** as well.

The report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Tabular report contains the following information:

- Date: Date of file upload.
- Users: Name of the user.
- Source IP: IP Address of the source.
- Domain: Name of the domain where file has been uploaded.
- File name: Name of the file.
- Size: Size of the file.

File Uploaded via Web					
Date	Users	Source IP	Domain	File Name	Size
2015-10-31 1...	unidentified	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	unidentified	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	unidentified	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	new1	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	new1	10.198.47.103	update.cyber...	update.cyber...	1002 B

Figure 11: File Uploaded via Web

Files Uploaded via FTP

This Report displays the list of the files uploaded via FTP with file wise distribution of the total data transfer and the relative percentage distribution amongst those files.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Files Uploaded via FTP**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per uploaded file, while the tabular report contains the following information:

- File: Name of the top files uploaded via FTP.
- Bytes: Size of the top uploaded files.
- Percent: Relative percent distribution among the top files uploaded via FTP.

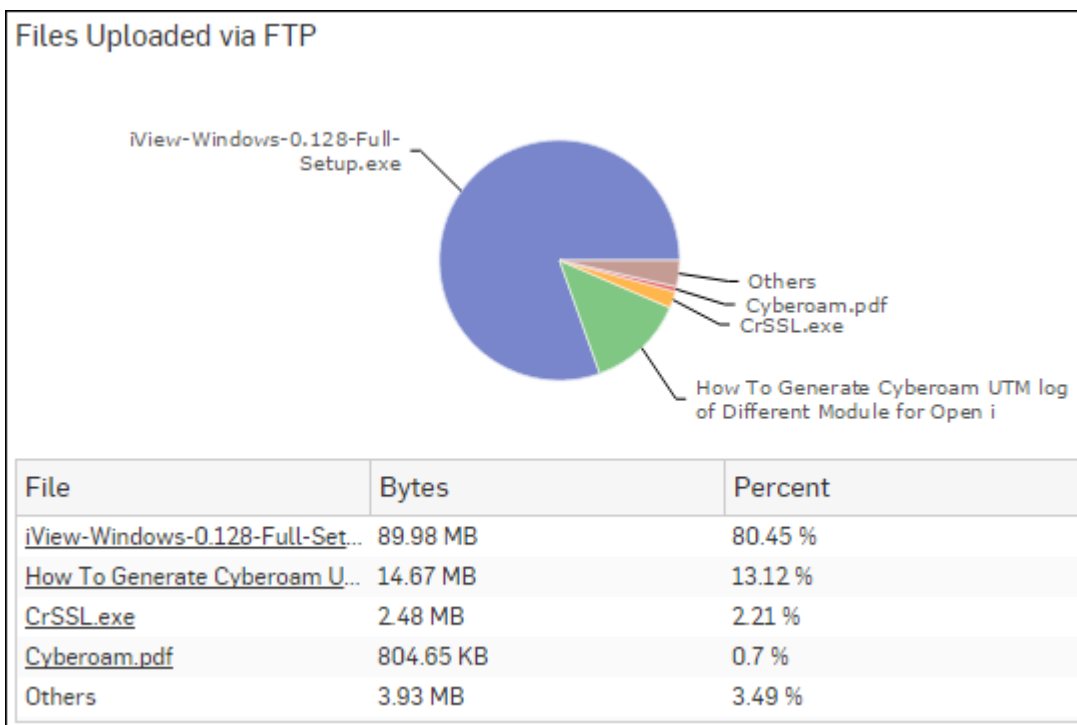


Figure 12: Files Uploaded via FTP

Click the File hyperlink in the table or the pie chart to view the [Filtered FTP Usage Reports](#).

Files Downloaded via FTP

This Report displays list of the files downloaded via FTP along with file wise distribution of the total data transfer and relative percent distribution among those files.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Files Downloaded via FTP**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per downloaded file, while the tabular report contains the following information:

- File: Name of the top files downloaded via FTP.
- Bytes: Size of the top downloaded files.
- Percent: Relative percent distribution among the top files downloaded via FTP.

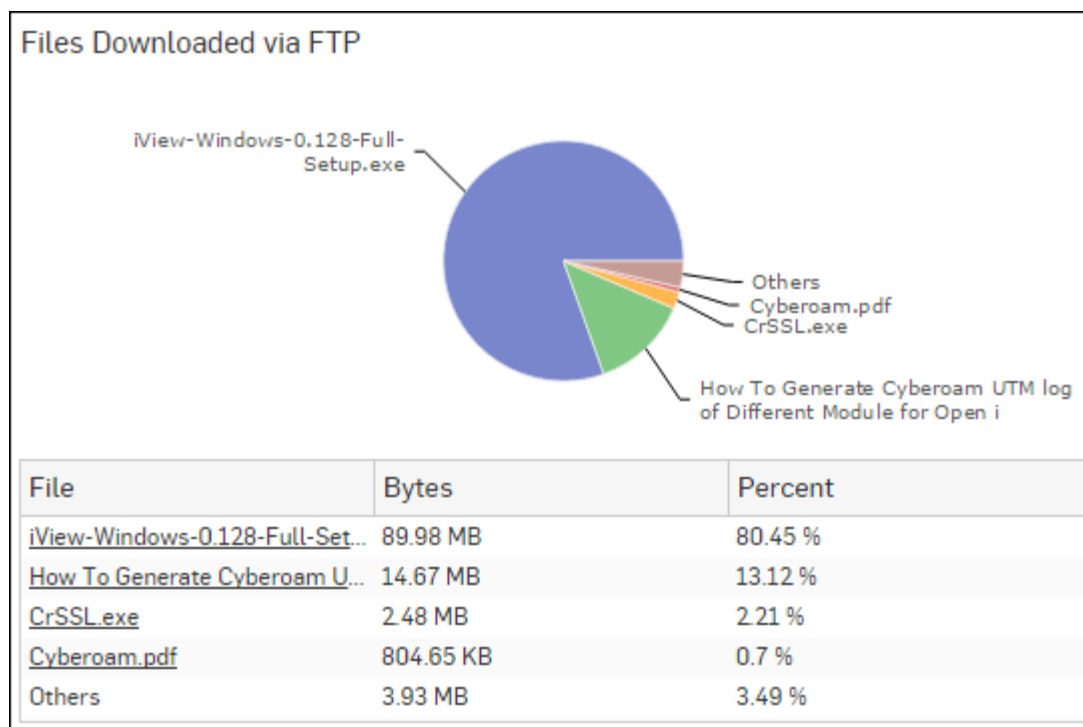


Figure 13: Files Downloaded via FTP

Click the File hyperlink in the table or the pie chart to view the [Filtered FTP Usage Reports](#).

FTP Servers

This Report displays a list of FTP servers along with data transfer per server along with relative percent distribution among the FTP servers.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > FTP Servers**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays percentage distribution of data transfer per server, while the tabular report contains following information:

- Server: Name of the FTP server.

- Bytes: Total data transfer via FTP server.
- Percent: Relative percent distribution among the FTP servers.

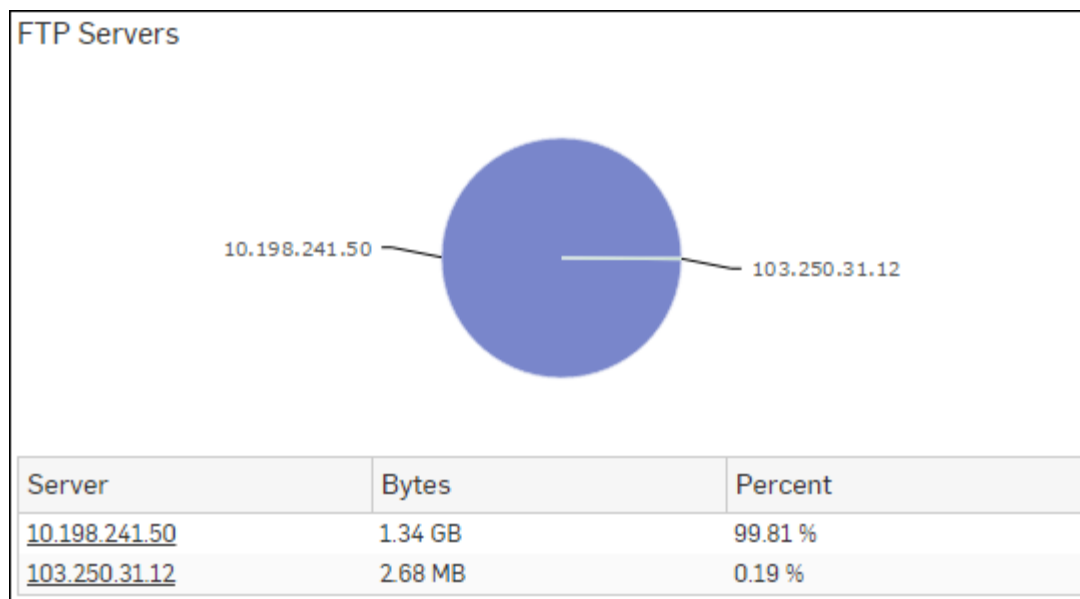


Figure 14: FTP Servers

Click the Server hyperlink in the table or the pie chart to view the [Filtered FTP Usage Reports](#).

Mail Traffic Summary

This Report displays type of Email traffic along with number of emails and percentage distribution among the traffic type.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Mail Traffic Summary**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays relative percentage distribution of traffic types, while the tabular report contains the following information:

- Traffic: The type of Email traffic. Possible types are :
 - Clean Mail
 - Spam
 - Probable Spam
 - Virus
- Mail Count: Number of emails per traffic type.
- Percent: Relative percentage distribution among the traffic types.

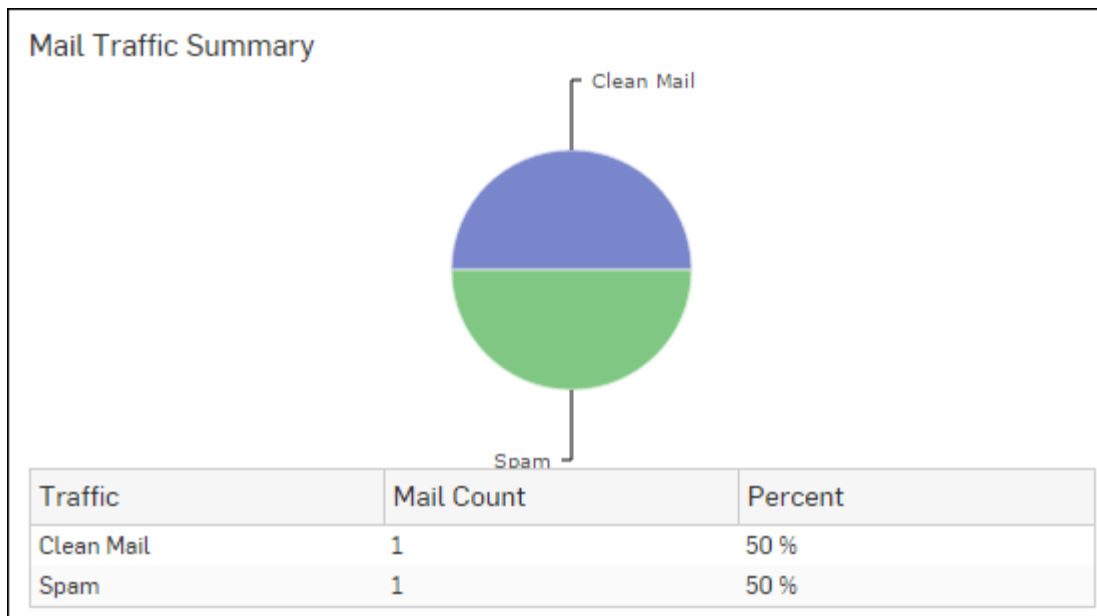


Figure 15: Mail Traffic Summary

Click the Traffic hyperlink in the table or the pie chart to view the [Filtered Email Usage Reports](#).

Mail Senders

This Report displays the list of top Email senders along with the number of hits that generated the most traffic for various users, destinations, hosts and applications.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Mail Senders**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Bar graph displays the relative percentage distribution of data transferred by each sender while the tabular report contains following information:

- Sender: Email ID of the sender.
- Bytes: Amount of data transferred.
- Percent: The amount of data transferred per sender, in percentage.

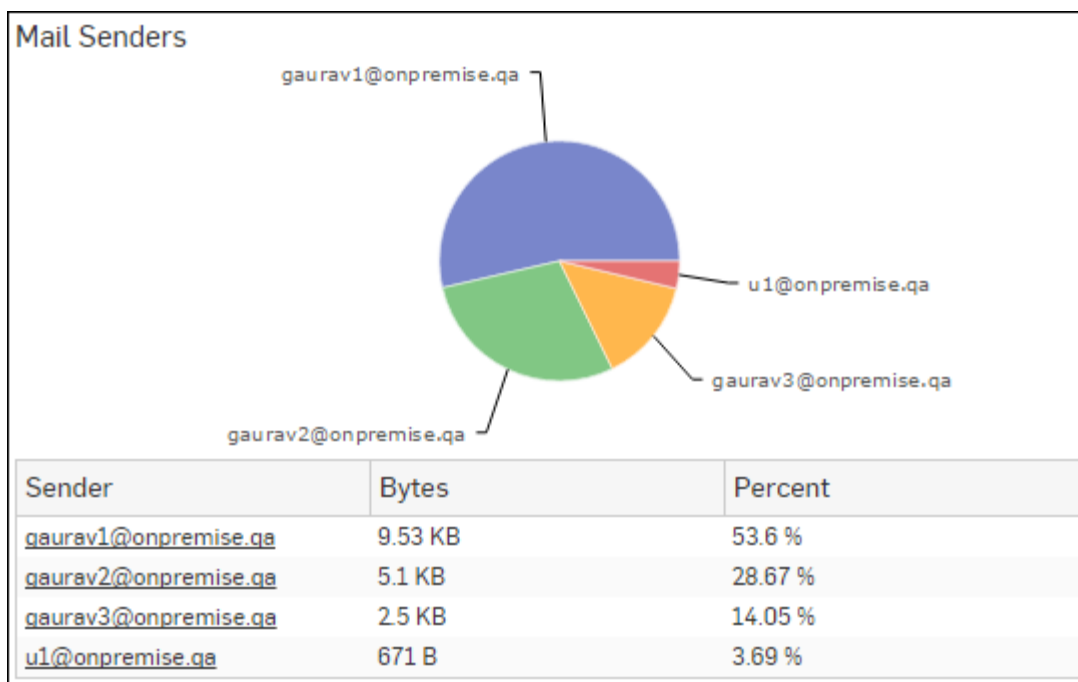


Figure 16: Mail Senders

Click the Sender hyperlink in the table or the pie chart to view the [Filtered Email Usage Reports](#).

Mail Recipients

This Report displays list of top Email recipients along with the number of hits that generated the most traffic for various users, destinations, hosts and applications.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Mail Recipients**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Bar graph displays the relative percentage distribution of data transferred by each recipient while the tabular report contains following information:

- Recipient: Email ID of the recipient.
- Bytes: Amount of data transferred.
- Percent: The amount of data transferred per recipient, in percentage.

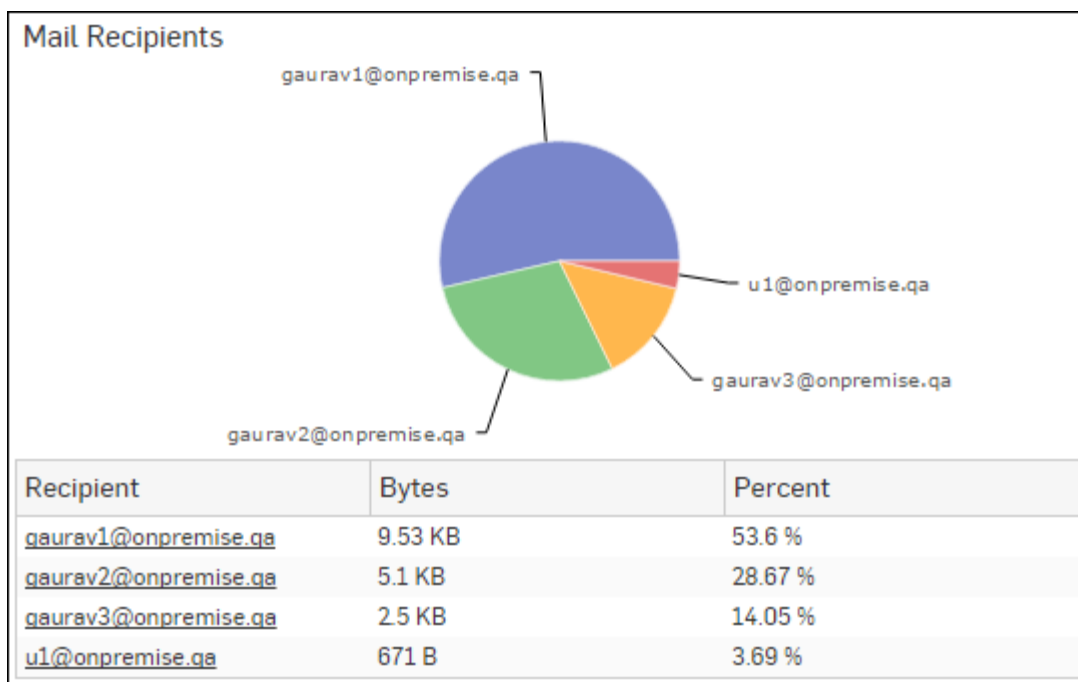


Figure 17: Mail Recipients

Click the Recipient hyperlink in the table or the pie chart to view the [Filtered Email Usage Reports](#).

Security Dashboard

The Security dashboard is a collection of widgets displaying information regarding the denied network activities and traffic. It also gives an overview of malware, spam as well as top source and destination countries.

View the Security dashboard from **Monitor & Analyze > Reports > Dashboards > Security Dashboard**.

The Security Dashboard consists of following reports in widget form:

- [High Risk Applications](#)
- [High Risk Application Users](#)
- [Blocked Applications](#)
- [Blocked Application Users](#)
- [Objectionable Web Categories](#)
- [Objectionable Web Domains](#)
- [Blocked Web Categories](#)
- [Blocked Web Domains](#)
- [Objectionable Web Users](#)
- [Blocked Web Users](#)
- [Hosts - ATP](#)
- [Users - ATP](#)
- [Advanced Threats](#)
- [Security Heartbeat - ATP](#)
- [Intrusion Attacks](#)
- [Intrusion Source](#)
- [Virus Summary](#)
- [Spam Senders](#)
- [Spam Recipients](#)
- [Detailed View - Client Health](#)
- [Attacked Web Server Domains](#)

- [Blocked Web Server Requests](#)

High Risk Applications

This Report displays a list of Applications with Risk Level greater than equal to 4, along with number of hits and total amount of data transfer per application.

View the report from User App Risks & Usage reports dashboard or **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > High Risk Applications**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > High Risk Applications** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. The date can be changed from the top most row of the page.

The bar graph displays the list of high risk applications along with amount of data transfer per application, while the tabular report contains the following information:

- Application/Proto: Port: Name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of the protocol and port number.
- Risk: Level of risk associated with the application.
- Hits: Number of hits per application.
- Bytes: Amount of data transfer through the application, in bytes.

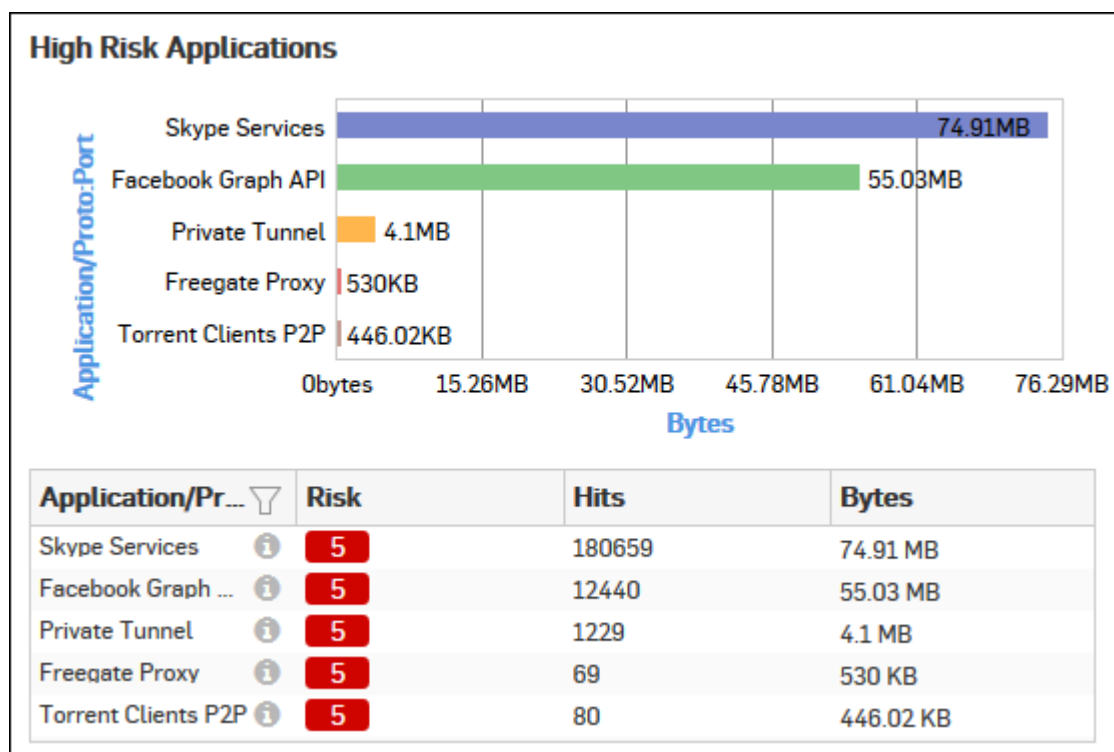


Figure 18: High Risk Applications

Click the Application hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

High Risk Application Users

This Report displays a list of Users accessing high risk applications (Risk Level greater than or equal to 4), along with application count, total number of hits to the applications and total amount of data transfer by each user.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > High Risk Application Users**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > High Risk Application Users** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with number of hits while the tabular report contains the following information:

- Username: Username of the user as defined in the monitored device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Application Count: Number of applications accessed per user.
- Hits: Number of hits to the high risk applications accessed by the user.
- Bytes: User-wise amount of data transfer through the high risk applications, in bytes.

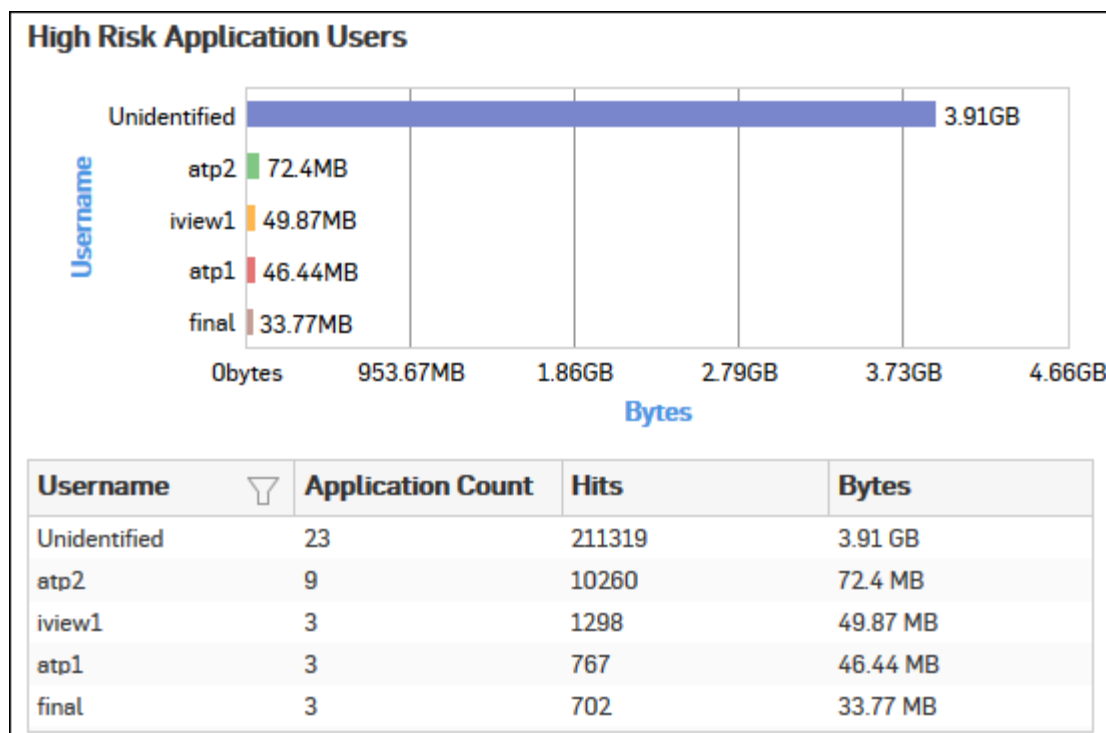


Figure 19: High Risk Application Users

Click the Username hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Blocked Applications

This Report displays a list of blocked applications which have the maximum number of access attempts.

View the report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Applications**.

The Report is displayed using a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays the percentage distribution of number of hits amongst the denied applications while the tabular report contains the following information:

- Application/Protocol: Displays the name of the application as defined in the Device. If application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Category: Name of the application category as defined in the Device.

- Risk: Risk level associated with the application. The risk level is a numeric value. A higher value represents higher risk.
- Hits: Number of attempts to access the application.
- Percent: Relative percentage distribution amongst denied applications.

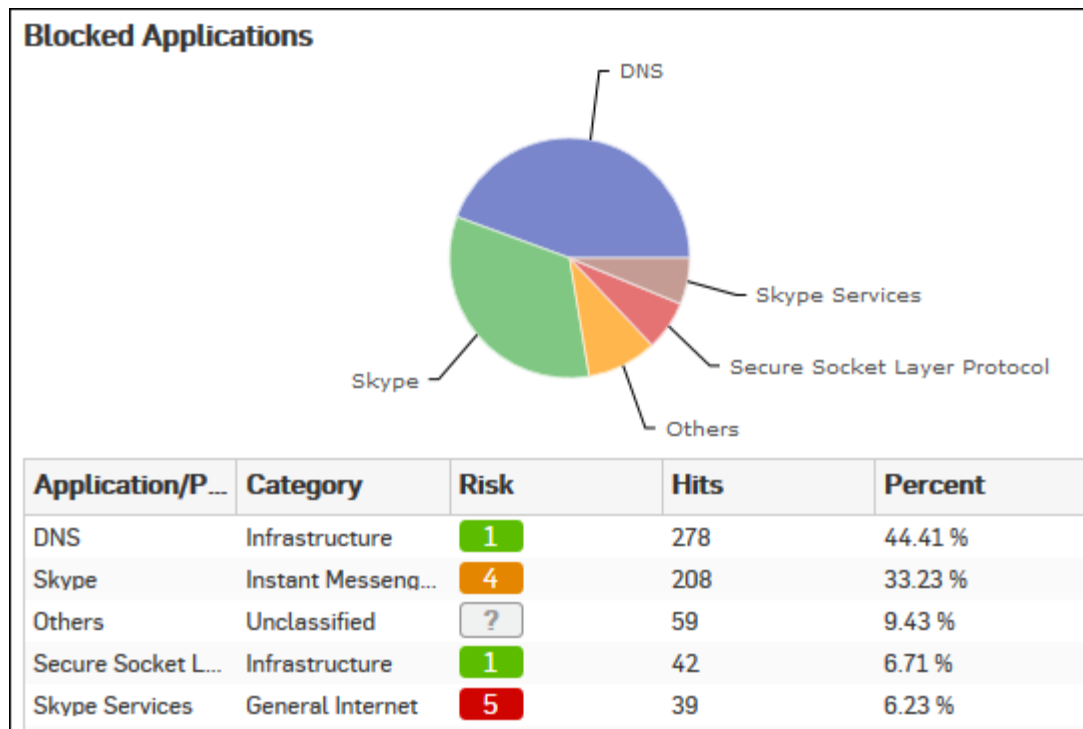


Figure 20: Blocked Applications

Click the Application hyperlink in table or pie chart to view [Filtered Blocked User Apps Reports](#).

Blocked Application Users

This Report displays a list of users who made the maximum attempts to access blocked applications.

View the report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Application Users**.

The Report is displayed using a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays relative percentage distribution of number of hits amongst the denied users, while the tabular report contains following information:

- User: Name of the denied user as defined in the Device.
- Hits: Number of attempts by a particular user to access blocked application(s).
- Percent: Relative percentage distribution amongst the denied users.

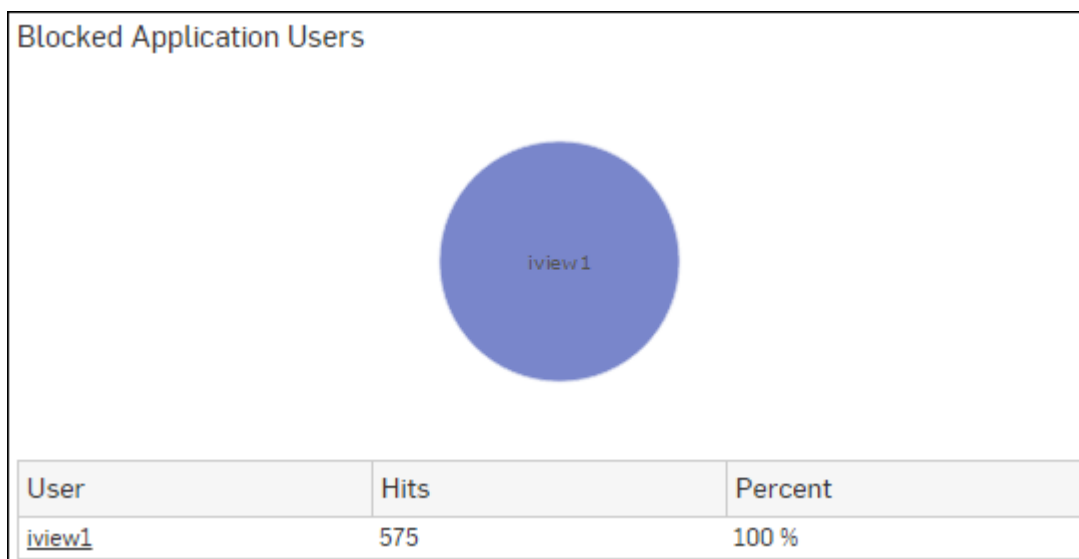


Figure 21: Blocked Application Users

Click the User hyperlink in the table or the pie chart to view [Filtered Blocked User Apps Reports](#).

Objectionable Web Categories

This Report displays a list of Objectionable web categories accessed over the selected time period along with domain count per Objectionable category, number of hits and amount of data transferred through the category.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Categories**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Categories** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category while the tabular report contains the following information:

- Category: Displays name of the web category categorized as Objectionable in the Device.
- Domain Count: Number of domains accessed per Objectionable web category.
- Hits: Number of hits to the category.
- Bytes: Amount of data transferred.

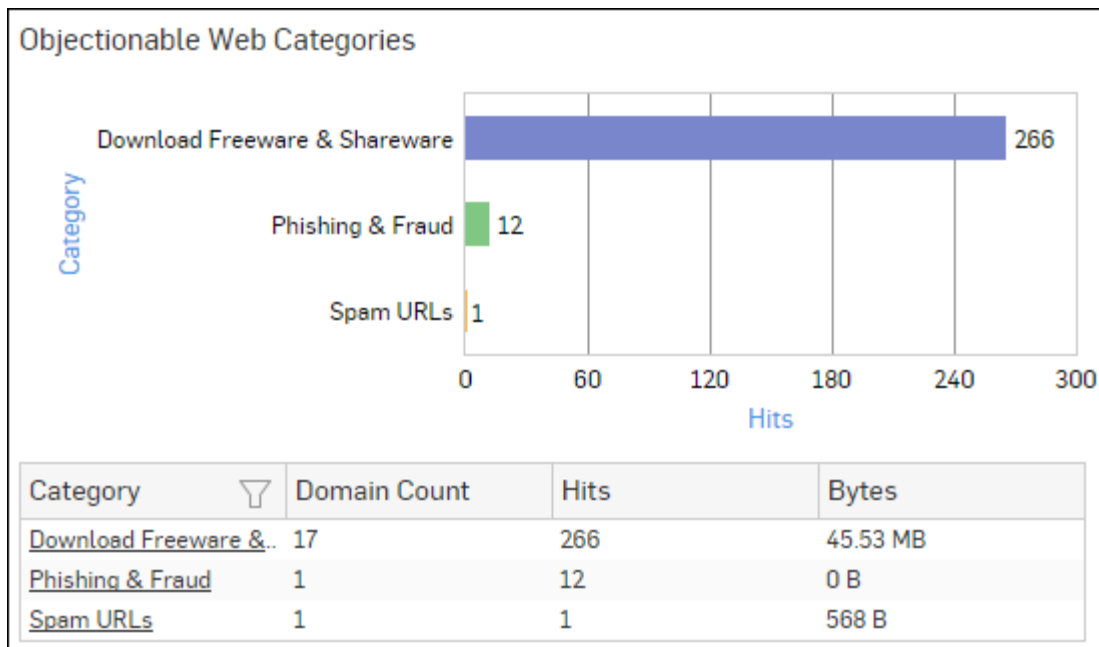


Figure 22: Objectionable Web Categories

Click the Category hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Objectionable Web Domains

This Report displays the list of Domains categorized under a Objectionable web category, along with number of hits and amount of data transferred through the domain.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Domains** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per domain while the tabular report contains the following information:

- Domain: Domain name or IP Address of the domain.
- Category: Name of the objectionable web category, under which the domain is categorized.
- Hits: Number of hits to the domain.
- Bytes: Amount of data transferred.

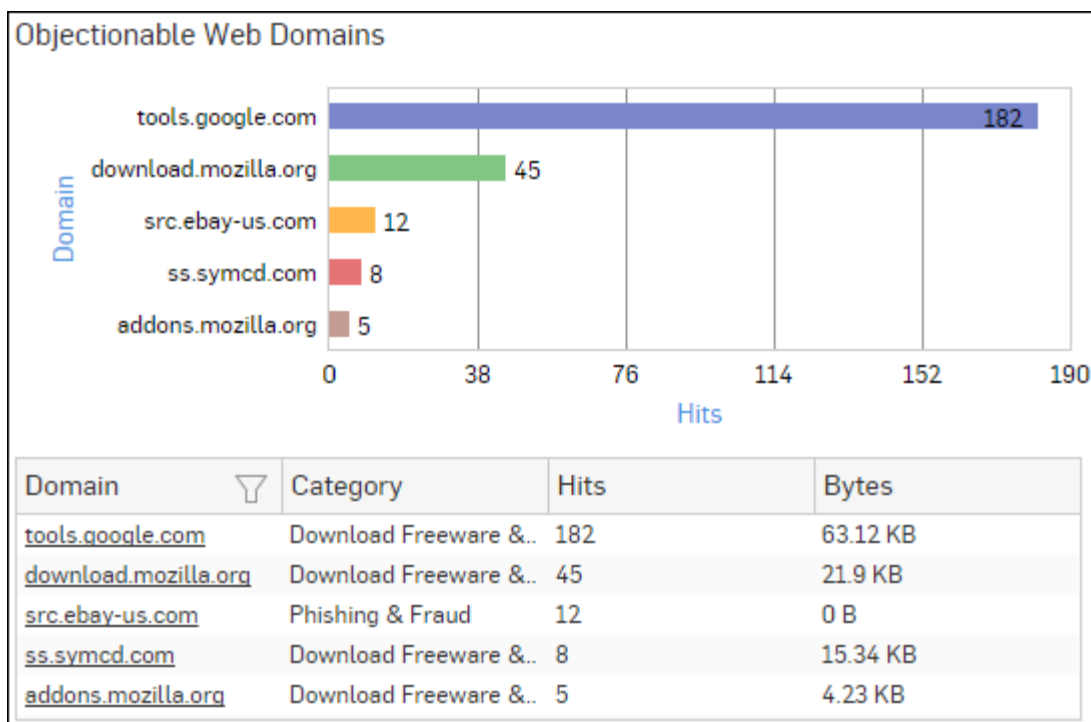


Figure 23: Objectionable Web Domains

Click the Domain hyperlink in table or graph to view the [Filtered Web Risks & Usage Reports](#).

Blocked Web Categories

This Report displays a list of blocked web categories that various users tried to access and the number of access attempts to each category.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Categories**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Categories** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of categories along with number of hits per category while the tabular report contains the following information:

- Category: Name of the category.
- Hits: Number of hits per category.

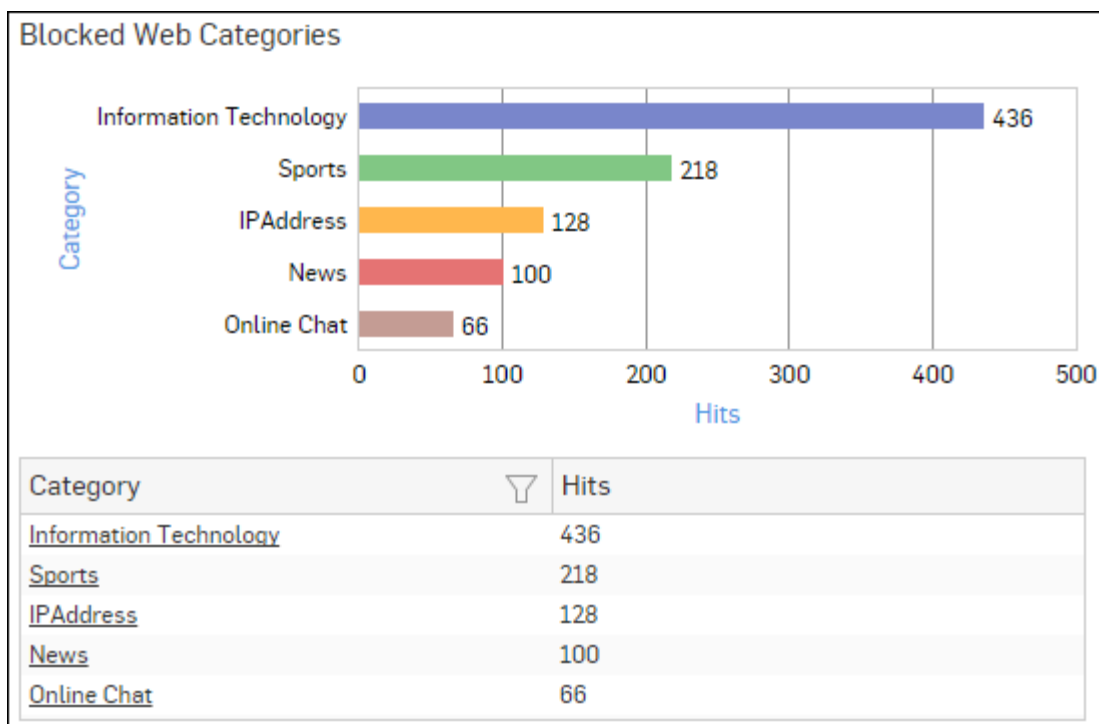


Figure 24: Blocked Web Categories

Click the Category hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Blocked Web Domains

This Report displays the list of blocked web domains that various users tried to access and the number of access attempts to each domain.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Domains** as well.

The Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of domains along with number of hits per domain while tabular report contains the following information:

- Domain: Name of the domain.
- Hits: Number of Hits.

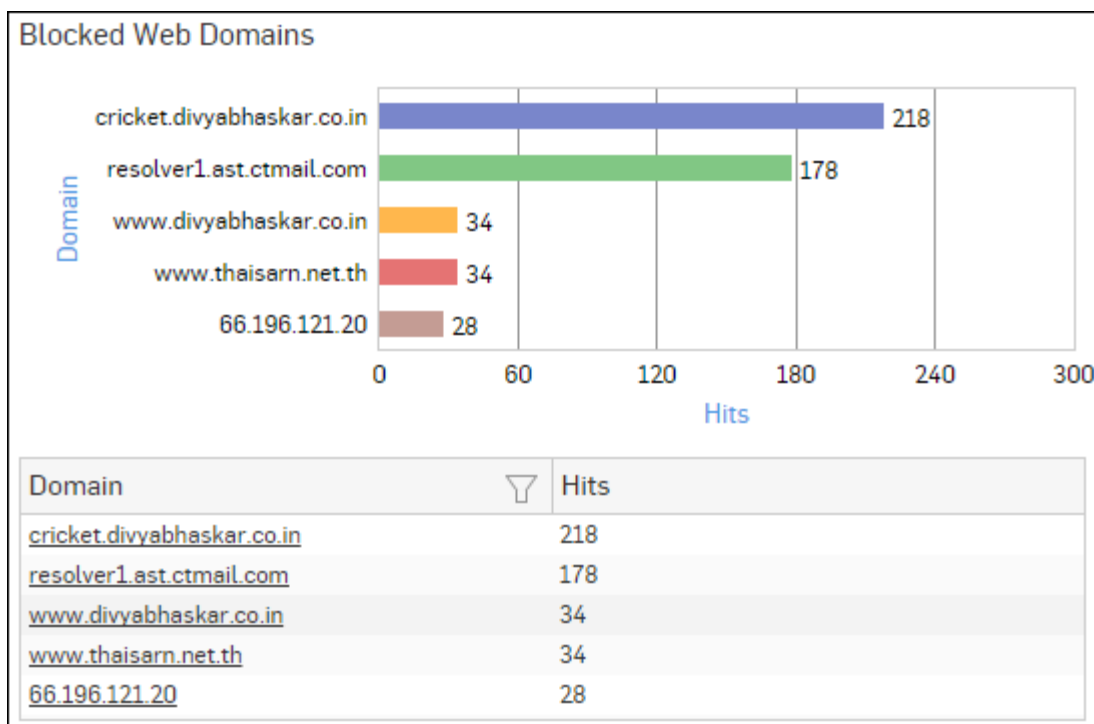


Figure 25: Blocked Web Domains

Click the Domain hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Objectionable Web Users

This Report displays a list of Users accessing Objectionable web sites / categories along with number of times the Objectionable web site and web category was accessed and amount of data transferred per user.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Users**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Users** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per user, while the tabular report contains the following information:

- Username: Username of the user as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Category Count: Number of times a Objectionable web category was accessed per user.
- Domain Count: Number of times a Objectionable domain was accessed per user.
- Hits: Total number of hits to Objectionable web site and web categories.
- Bytes: Amount of data transferred per user.

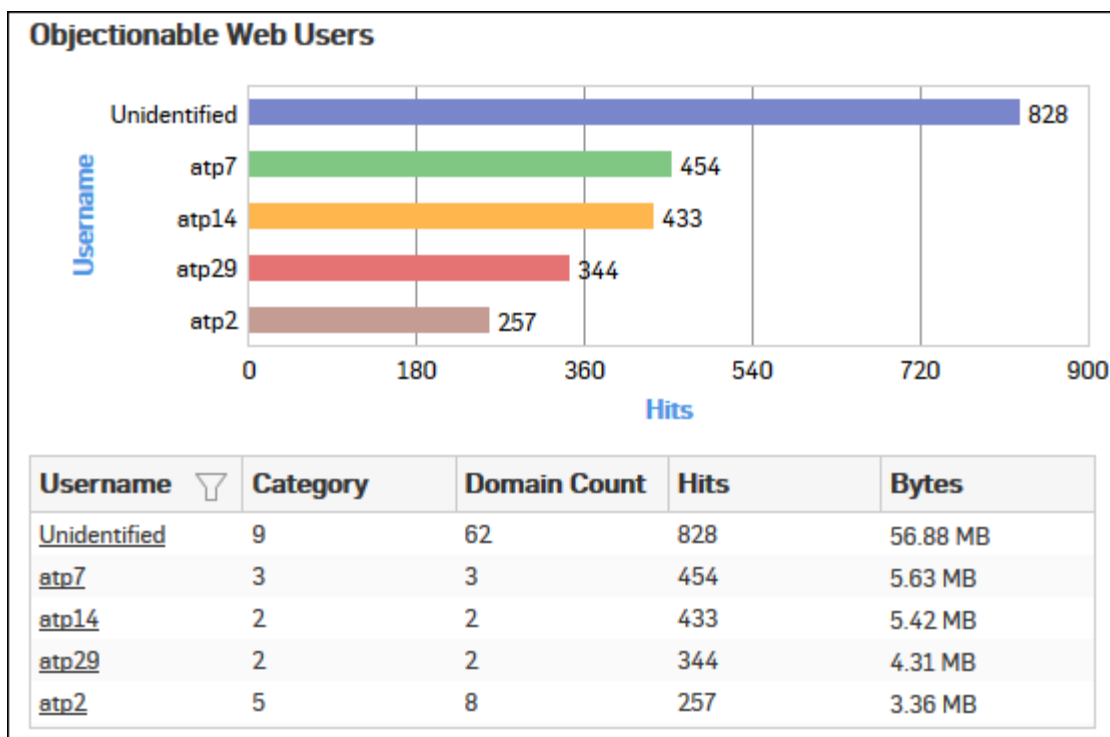


Figure 26: Objectionable Web Users

Click the Username hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Blocked Web Users

This Report displays a list of Users who made the most attempts to access blocked sites.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Users**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Users** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of blocked users along with number of hits per user while the tabular report contains the following information:

- User: Name of the User as defined in the Device.
- Hits: Number of Hits.

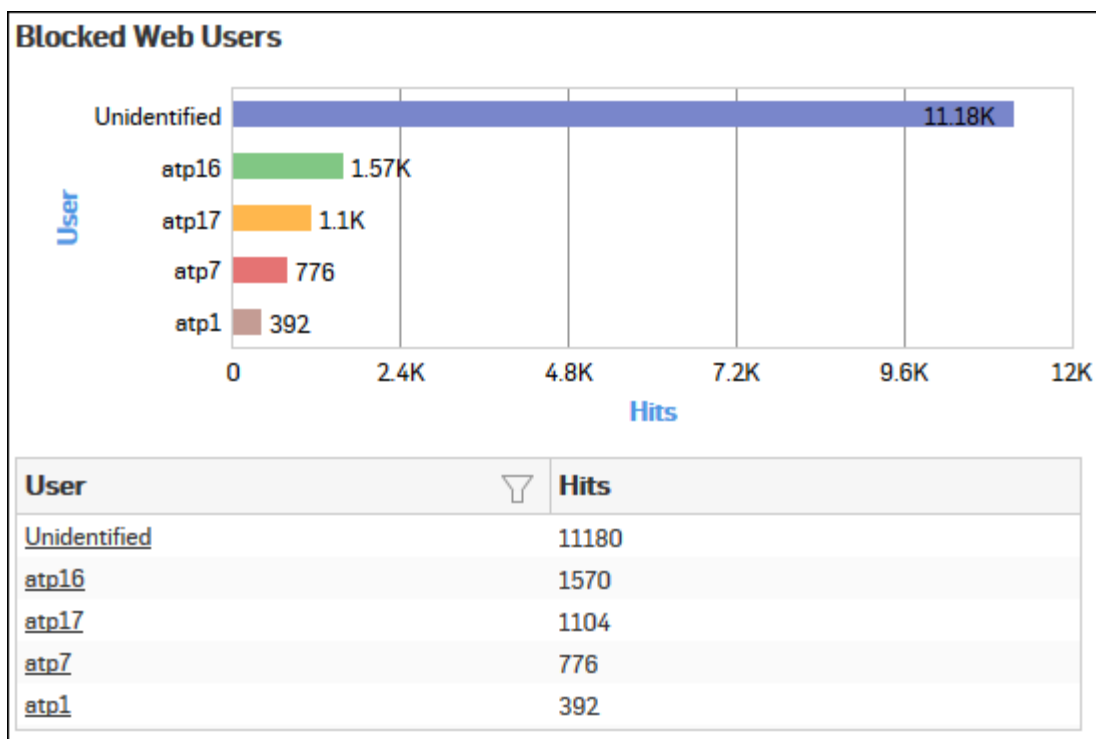


Figure 27: Blocked Web Users

Click the User hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Hosts - ATP

This report displays a comprehensive summary of host wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Hosts-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Hosts-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of events per host while the tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Threat Count: Number of threats per source host.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

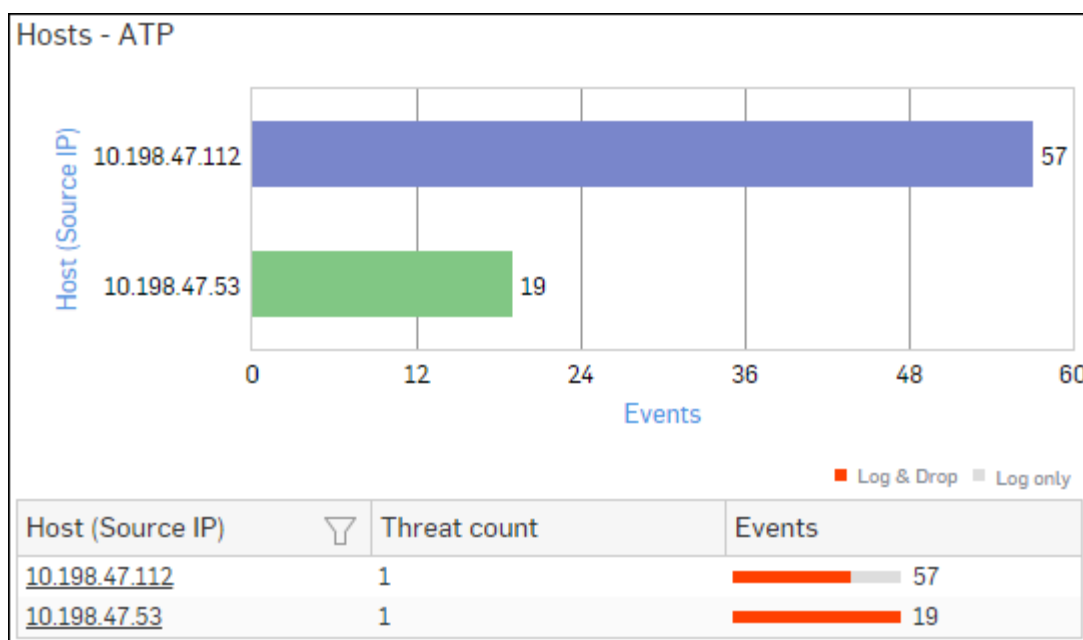


Figure 28: Hosts - ATP

Click Host hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Users - ATP

This report displays a comprehensive summary of user wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Users-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Users-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with total number of events per user while the tabular report contains the following information:

- User: User name of the infected user.
- Host Count: Number of hosts per user.
- Threat Count: Number of threats per user.
- Events: Total number of events per user. The number is summation of Log only and Log & Drop events.

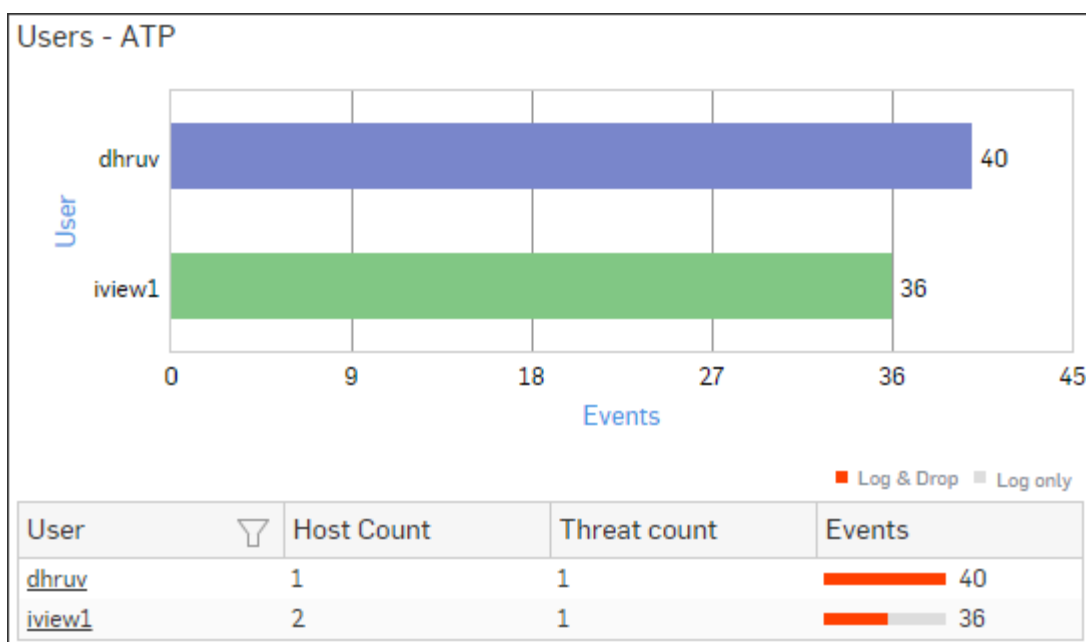


Figure 29: Users - ATP

Click User hyperlink in the table or graph to view the [Filtered ATP Reports](#).

Advanced Threats

This report displays a comprehensive summary of advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Advanced Threats**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Advanced Threats** as well.

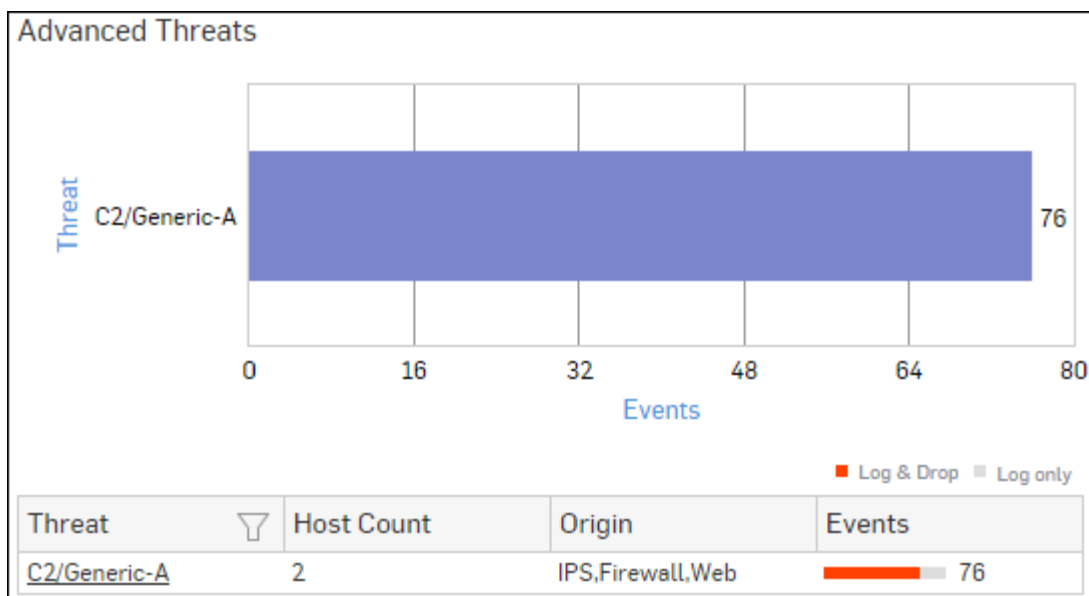
The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of threats along with total number of events per threat while the tabular report contains the following information:

- Threat: Name of the threat.
- Host Count: Number of hosts infected with the threat.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Events: Total number of events per threat. The number is summation of Log only and Log & Drop events.

Figure 30: Advanced Threats



Click Threat hyperlink in the table or graph to view the [Filtered ATP Reports](#).

Security Heartbeat - ATP

The report displays advanced threats associated with the endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Security Heartbeat - ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Heartbeat > Security Heartbeat - ATP** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Login User: User name of the user logged into the endpoint.
- Process User: Username of the user running the process.
- Executable: Name of the infected executable (.exe) file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the destination.
- Event Last Seen: Displays the date in YYYY-MM-DD HH:MM:SS format when the event was last seen.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP								
Host (Source IP)	Login User	Process User	Executable	Threat	Threat URL/IP	Event Last Seen	Events	
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1	

Figure 31: Security Heartbeat - ATP

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Intrusion Attacks

The Report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Attacks**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Attacks** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each attack, while the tabular report contains the following information:

- Attack: Name of the attack launched.
- Hits: Number of hits for each attack.

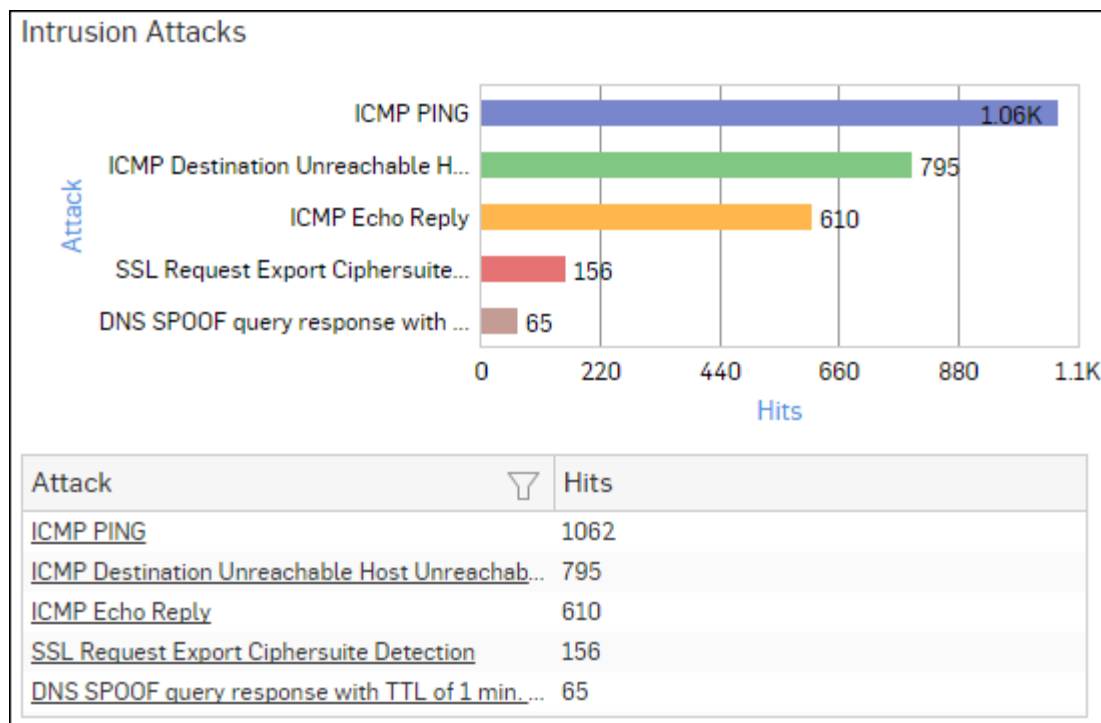


Figure 32: Intrusion Attacks

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Source

The Report enables to view the details of the attacker(s) who have hit the system and gives the detailed disintegration of attacks, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Source**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Source** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each attacker, while the tabular report contains the following information:

- Attacker: IP Address of the attacker.
- Hits: Number of hits for each attacker.

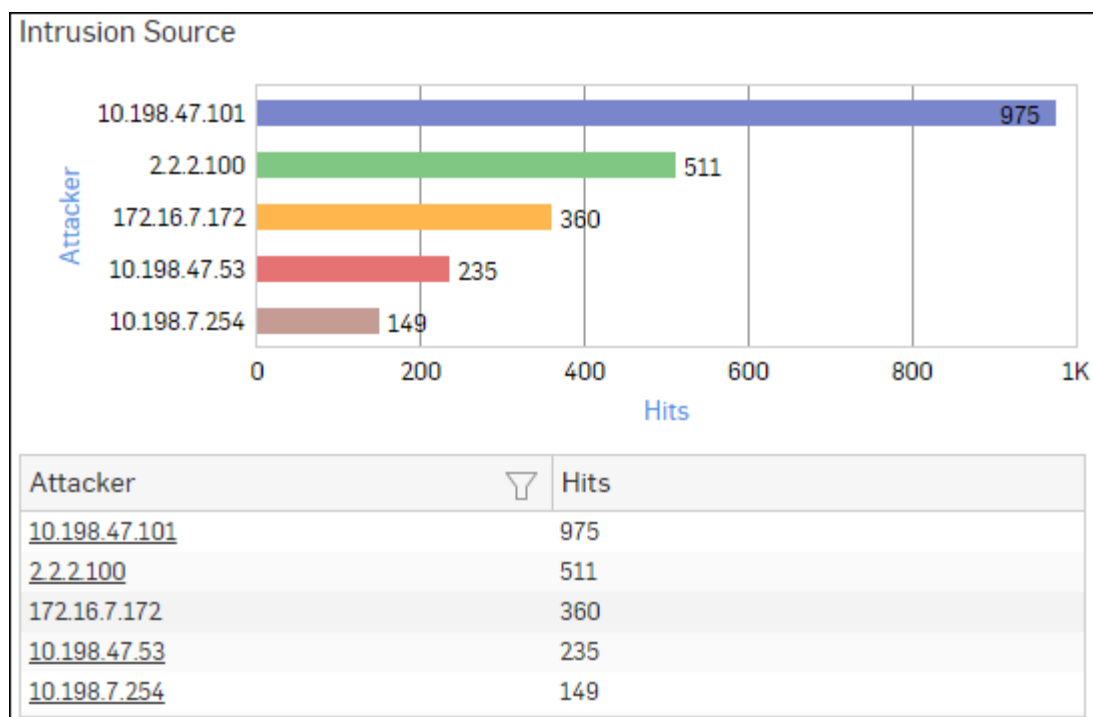


Figure 33: Intrusion Source

Click Attacker hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Virus Summary

This Report provides an overview of Virus traffic in your network, in terms of protocols through which viruses were introduced in the network as well as number of counts per protocol.

View the report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Virus Summary**.

The Report is displayed using a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays number of counts per protocol through which viruses were introduced in the network, while the tabular report contains following information:

- Application/Proto:Port: Name of the protocol through which viruses were introduced in the network.
- Count: Number of counts per protocol.

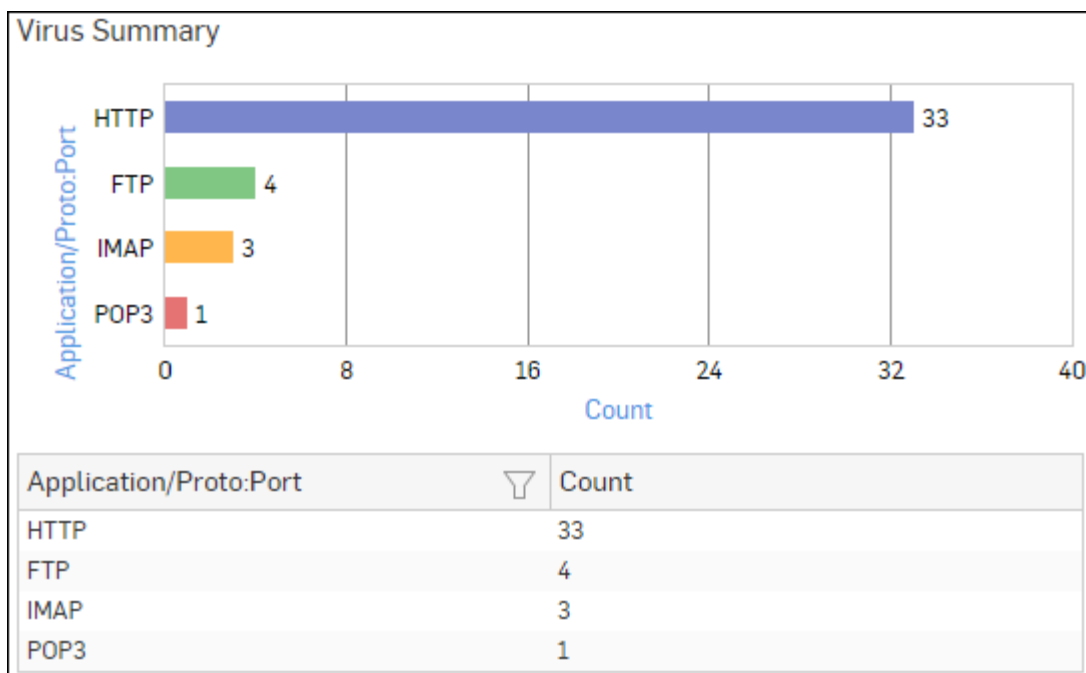


Figure 34: Virus Summary

Click Application hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Spam Senders

This Report displays a list of Spam Senders along with number of emails and percent distribution among the spam senders.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Senders**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Senders** as well.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of spam emails sent.
- Percent: Relative percent distribution among the spam sender.

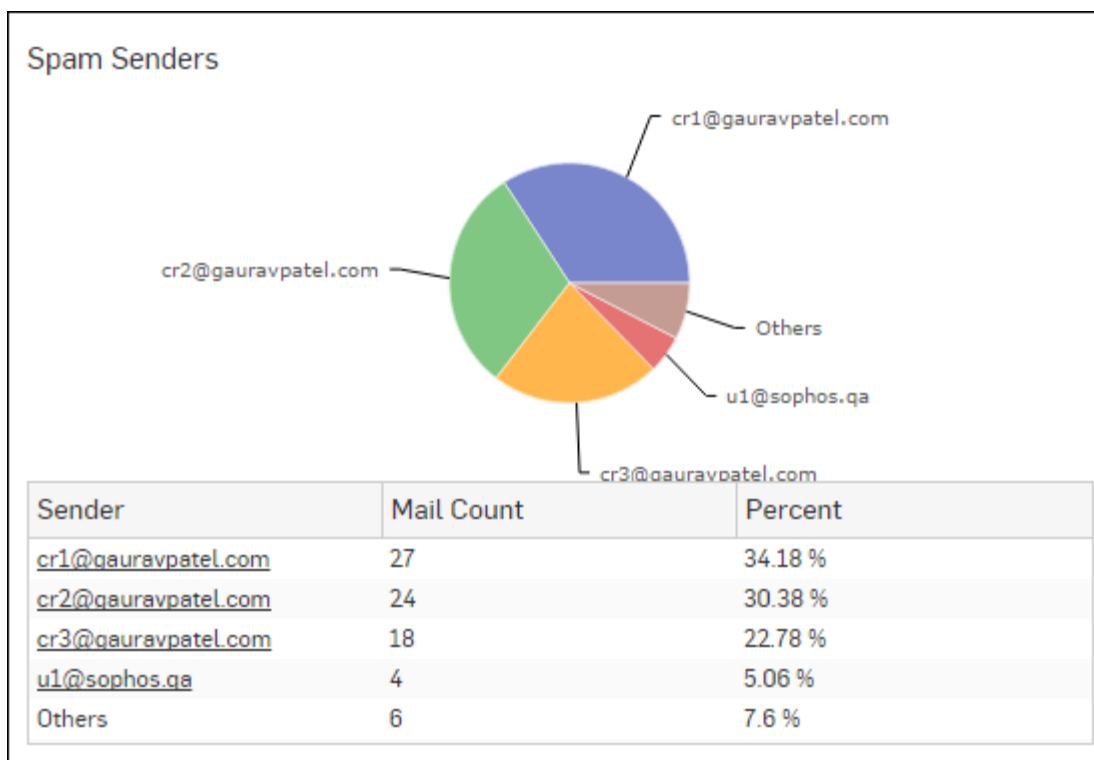


Figure 35: Spam Senders

Click the Sender hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Spam Recipients

This Report displays a list of Spam Recipients along with number of emails and percent distribution among the spam recipients.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Recipients**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Recipients** as well.

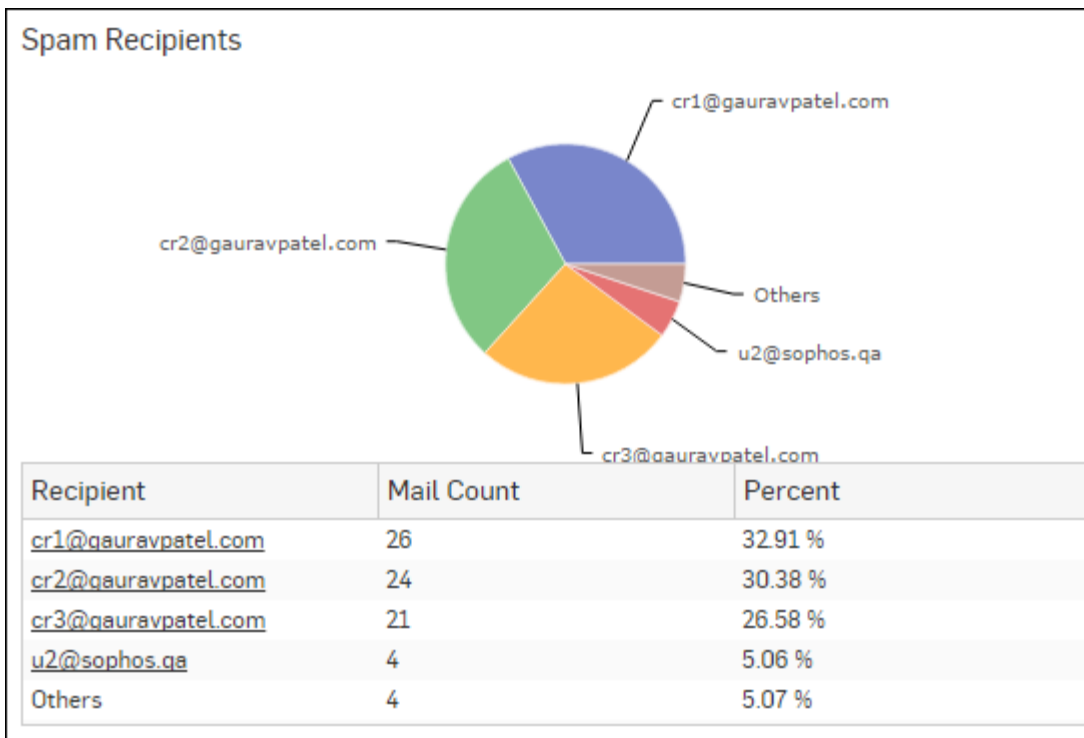
The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.
- Percent: Relative percent distribution among the spam recipients.

Figure 36: Spam Recipients



Click the Recipient hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Detailed View - Client Health

This report shows in-depth information regarding health status of endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Detailed View - Client Health**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Detailed View - Client Health** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Host Name: Name of the client.
- Health - Last Seen: Displays the latest health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.







Detailed View - Client Health				
Host (Source IP) 	Host Name 	Health - Last Seen		Last Health
10.20.41.8	TWIN8164BIT		Red	-
10.20.41.7	TWIN864		Yellow	-
10.198.38.8	TWIN764		Green	-
10.20.41.12	TWIN832		Green	-

Figure 37: Detailed View - Client Health

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Attacked Web Server Domains

This Report displays a list of attacked web servers along with the number of hits per server.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Attacked Web Server Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Attacked Web Server Domains** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of web servers along with the number of hits while the tabular report contains the following information:

- Web Server Domain: Displays name or IP Address of the attacked web server.
- Hits: Number of hits per web server.

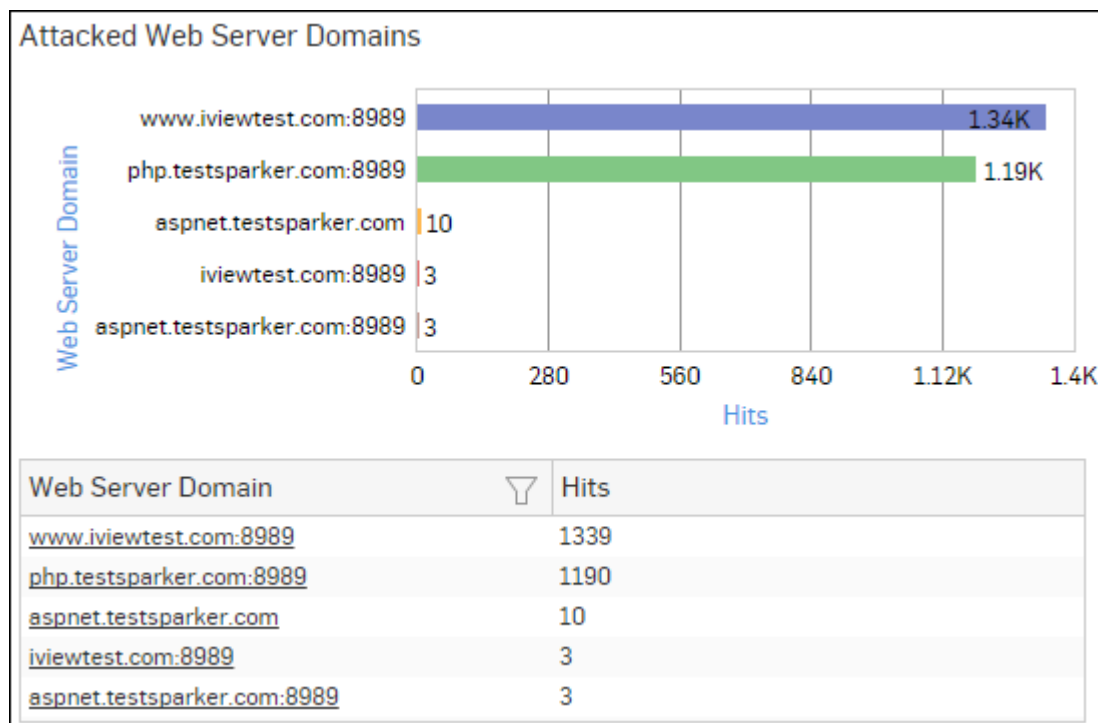


Figure 38: Attacked Web Server Domains

Click the Web Server Domain hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Blocked Web Server Requests

This Report displays a list of reasons of attacks blocked by the Device, along with the number of hits per attack.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Blocked Web Server Requests**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Server Requests** as well.

The bar graph displays the list of blocked reasons along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

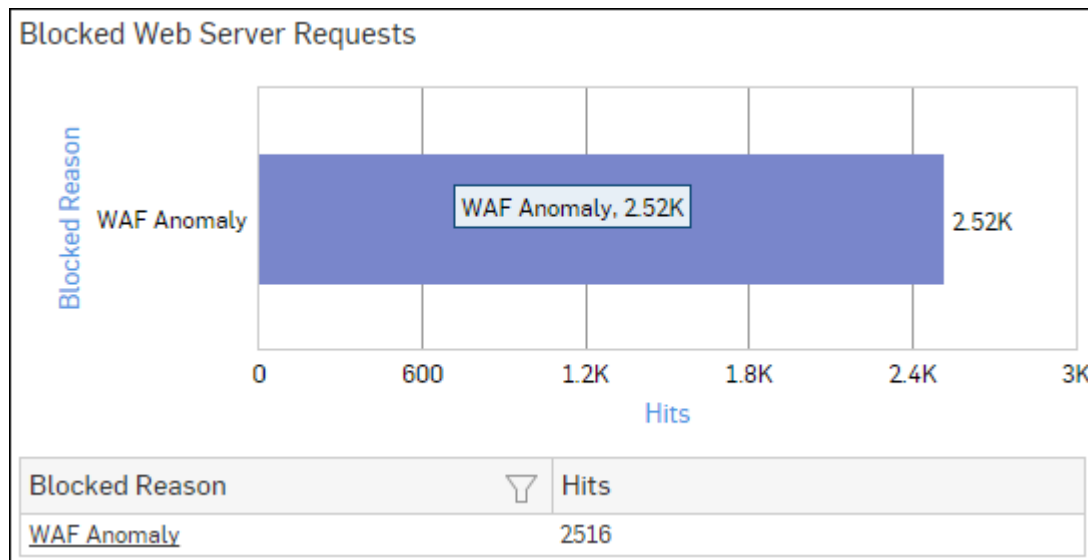


Figure 39: Blocked Web Server Requests

Click the Blocked Reason hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Executive Report

The Executive Report provides administrators with a collection of frequently viewed information regarding your Device, at single place.

This report summarizes variety of reports offered in the device to get insights, which in turn help you to implement robust security strategies.

View the report from **Monitor & Analyze > Reports > Dashboards > Executive Report**.

Executive Report consists following sub-sections:

- [Summary](#)
- [Applications & Web](#)
- [Network & Threats](#)
- [Email](#)
- [Resource Usage](#)

Summary

This section provides an overview of key information about your Device including Applications usage, Email usage & protection, Network & Threats, Web Admin Console Logins, System and Updates.

The section provides following information in a tabular format, for the selected time period:

- **Applications & Web**
 - Users & Data Transfer
 - User count: Total number of users accessing the Internet.
 - Total User Data Transfer: Total amount of data transferred by the users, in bytes.
 - User Applications
 - Applications accessed: Total number of accessed applications.
 - High Risk Applications accessed: Total number of allowed high risk applications (with risk level greater than or equal to 4).
 - App Risk Score (out of 5): Risk Score associated with overall application traffic.
 - Blocked Applications: Total number of denied applications.
 - Application data transfer: Total amount of data transferred by the applications, in bytes.
 - Web
 - Web domains accessed: Total number of accessed web domains.
 - Web domains blocked: Total number of denied web domains.
 - Objectionable Web domains accessed: Total number of Objectionable websites accessed.
 - Web data transfer: Total amount of data transfer through web traffic, in bytes.
 - Web Virus: Total number of blocked web viruses.
 - Business Applications
 - Web Server(s) count: Total number of business apps.
 - Blocked Web Server Requests: Total number of web server attacks blocked by the Device.
- **Network & Threats**
 - VPN
 - VPN connections: Total number of VPN connections.
 - VPN traffic: Total amount of data transfer through VPN traffic, in bytes.
 - RED
 - RED Usage: Total amount of data transfer, in bytes, through all RED devices connected with the Device.
 - Wireless
 - Wireless AP count: Total number of wireless APs, managed by the Device.
 - SSID count: Total number of SSIDs, managed by the Device.
 - Max clients per SSID: Maximum number of clients per SSID.
 - Avg clients per SSID: Average number of clients per SSID.
 - IPS
 - Intrusion attacks: Total number of Intrusion attacks on the Device.
 - Emergency + Critical attacks: Total number of attacks with Severity - Major & above.
 - Advanced Threat Protection
 - Host count: Total number of infected hosts.
 - Threat count: Total number of advanced threats detected by the Device.
 - Events: Total number of attack attempts on the Device.
- **Email**
 - Mails processed: Total number of mails processed by the Device.
 - Spam Mails: Total number of spam mails identified by the Device.
 - Virus Mails blocked: Total number of virus mails blocked by the Device.
- **Web Admin Console Logins**
 - Successful: Number of successful login attempts through Web Admin Console.
 - Failed: Number of failed login attempts through Web Admin Console.
- **System**

- System Restarts: Number of times the Device re-booted.
- **Updates**
 - Firmware updates installed: Number of times firmware updates were installed by the Device.
 - Pattern updates installed: Number of times pattern updates were installed by the Device.

Applications & Web

This section provides an overview of Web & Application usage in your network.

The section contains following reports in Widget format, for the selected time period:

- [Users](#)
- [User Threat Quotient](#)
- [Application Categories](#)
- [Applications](#)
- [High Risk Applications](#)
- [Blocked Applications](#)
- [Web Categories](#)
- [Web Category Types](#)
- [Objectionable Web Categories](#)
- [Objectionable Web Domains](#)
- [Web Server Domains](#)
- [Blocked Web Server Requests](#)

Network & Threats

This section provides an overview of intrusion attacks and advanced threats found in your network.

The section contains following reports in Widget format, for the selected time period:

- [Intrusion Attacks](#)
- [Severity wise Attacks](#)
- [Advanced Threats](#)
- [Users - ATP](#)
- [Client Health](#)
- [Detailed View - Client Health](#)
- [Security Heartbeat - ATP](#)

Email

This section provides an overview of Email usage as well as spam & virus associated with the Email traffic.

The section contains following reports in Widget format, for the selected time period:

- [Mail Traffic Summary](#)
- [Spam Senders](#)
- [Spam Recipients](#)
- [Mail Virus](#)

Resource Usage

This section provides an overview of hardware resources consumed, for the selected time period.

The section displays, for the selected time period, following details, in tabular format:

- [CPU Usage](#)
- [Memory Usage](#)
- [Disk Usage](#)
- [Live Users](#)

- [Interface](#)

Users

This Report displays a list of the Users along with the amount of data transferred and time used for data transfer.

View the reports from the User Data Transfer reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User Data Transfer Report > Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with amount of data transfer while the tabular report contains the following information:

- User: Name of the user as defined in the Device.
- Client Type: Type of client used for data transfer.
- Data: Total amount of data transferred (Upload + Download) by the user.
- Uploaded: Amount of uploaded data.
- Downloaded: Amount of downloaded data.
- Used Time: Time used for data transfer.

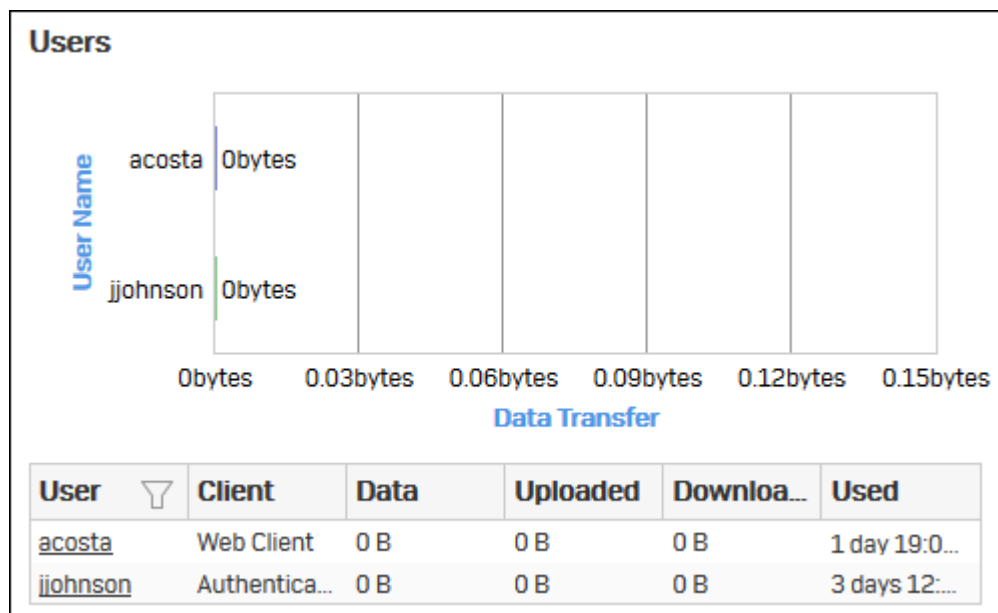


Figure 40: Users

Click the User hyperlink in the table or graph to view the [Filtered User Data Transfer Reports](#).

User Threat Quotient

This report provides actionable security intelligence to an administrator, by helping them to get quick visibility of risky users who are posing security threats on organization's network.

View the report from **Monitor & Analyze > Reports > Custom > Executive Report > User Threat Quotient**.

The report is displayed in a tabular format.

The tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined, then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Relative Threat Score: Threat posed by the user (in number), relative to the web behaviour of all the other users, for the selected period.

User Threat Quotient (FROM:2016-10-03 TO:2016-10-09)	
User	Relative Threat Score
amartin	22.03
batkins	21.88
jclark	21.83
acosta	21.80
bjones	12.13

Figure 41: User Threat Quotient

Click User hyperlink in the table to view [Reports by User and Date](#) for the selected period.

Application Categories

This report displays a list of top Application Categories along with number of hits per category and total amount of data transfer using that application.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Application Categories**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of application categories along with the number of hits while the tabular report contains the following information:

- Category: Displays name of the Application Category as defined in the Device.
- Hits: Number of hits per application category.
- Bytes: Amount of data transfer through the application category, in bytes.

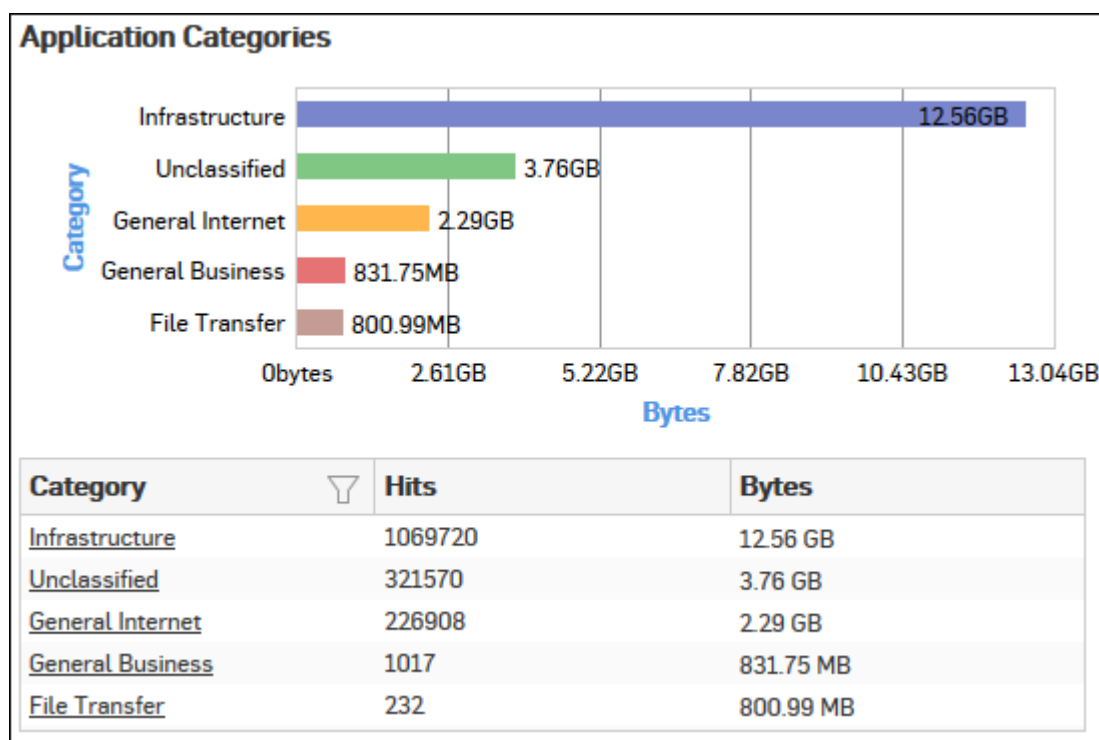


Figure 42: Application Categories

Click the Category hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Applications

This report displays a list of Applications along with the number of hits per application and the total amount of data transfer using that application.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Applications**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of application categories along with the number of hits while the tabular report contains the following information:

- Application/Proto: Port Displays name of the Application as defined in the Device. If the application is not defined in the Device then this field will display the application identifier as a combination of the protocol and port number.
- Risk: Level of risk associated with the application.
- Category: Name of the associated application category.
- Hits: Number of hits per application.
- Bytes: Amount of data transfer through the application, in bytes.

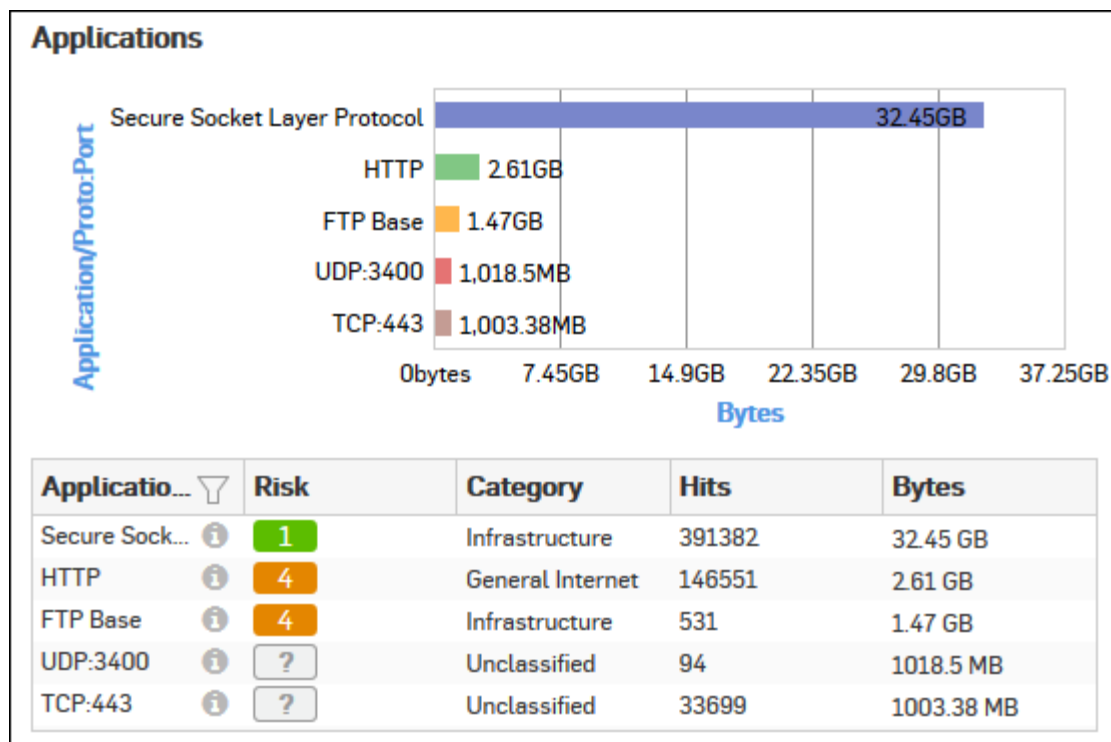


Figure 43: Applications

Click the Application hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

High Risk Applications

This Report displays a list of Applications with Risk Level greater than equal to 4, along with number of hits and total amount of data transfer per application.

View the report from User App Risks & Usage reports dashboard or **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > High Risk Applications**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > High Risk Applications** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. The date can be changed from the top most row of the page.

The bar graph displays the list of high risk applications along with amount of data transfer per application, while the tabular report contains the following information:

- Application/Proto: Port: Name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of the protocol and port number.
- Risk: Level of risk associated with the application.
- Hits: Number of hits per application.
- Bytes: Amount of data transfer through the application, in bytes.

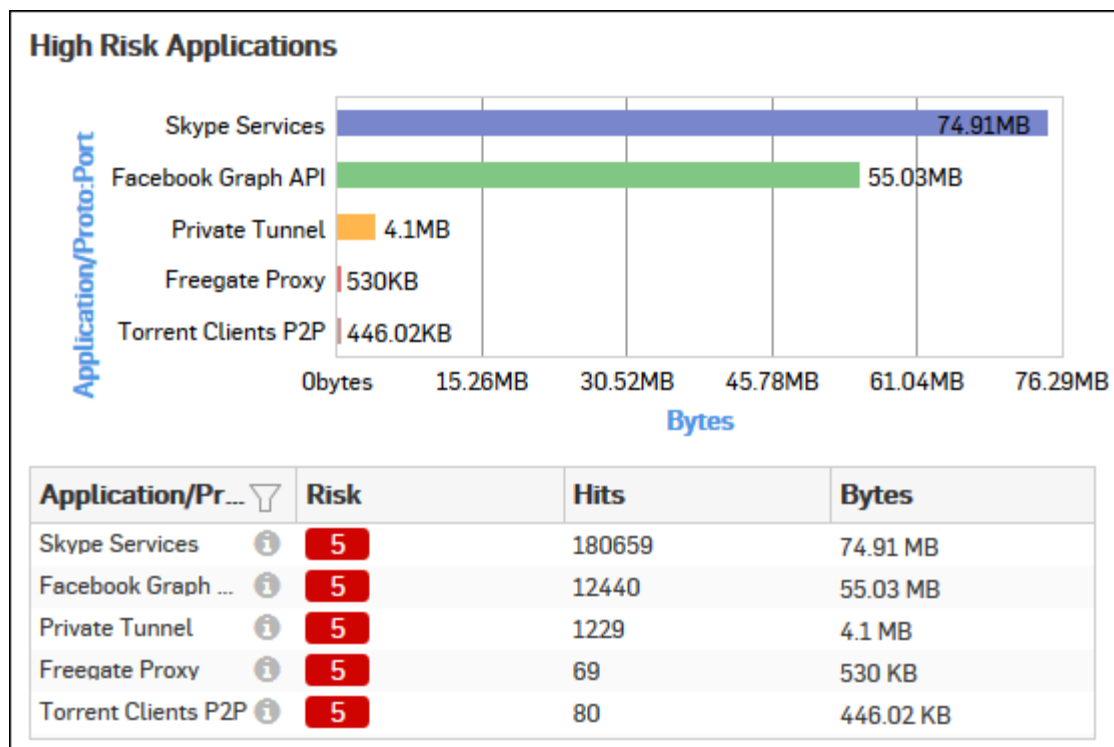


Figure 44: High Risk Applications

Click the Application hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Blocked Applications

This Report displays a list of top denied applications along with number of hits per application.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Applications**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied applications along with number of hits while tabular report contains following information:

- Application/Proto: Port: Displays name of the application as defined in the Device. If application is not defined in the Device, then this field will display application identifier as combination of protocol and port number.
- Risk: Displays risk level associated with the application. Higher number represents higher risk.
- Category: Displays name of the application category as defined in the Device.
- Hits: Number of hits per application category.

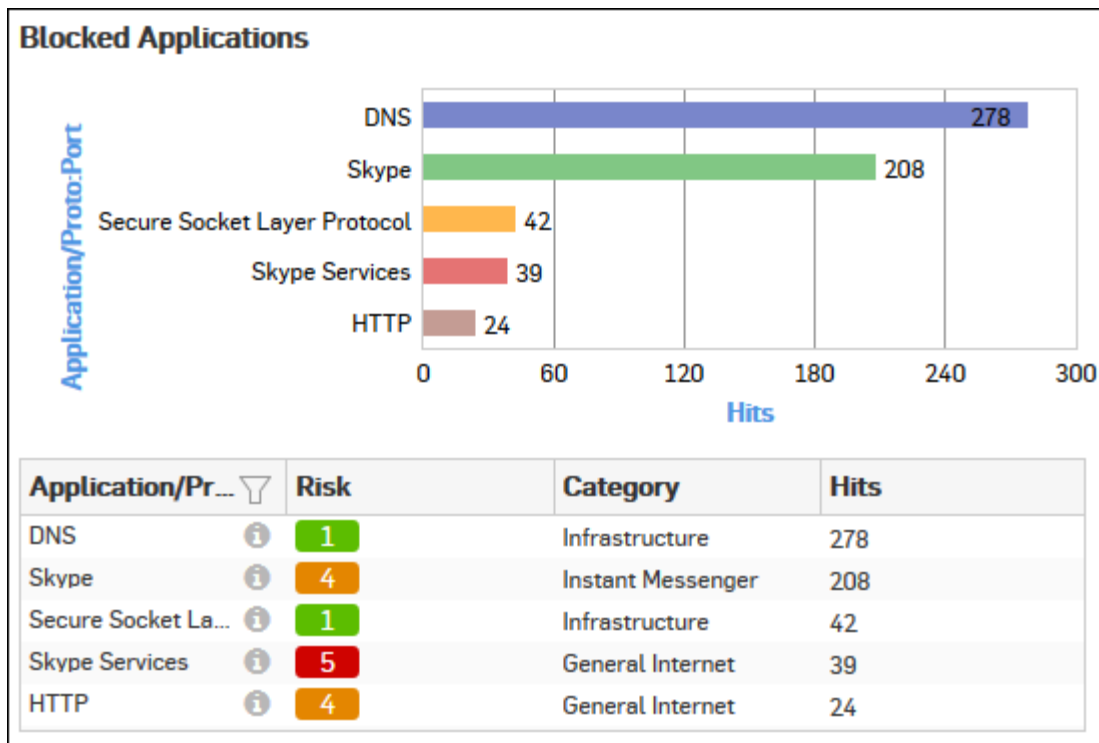


Figure 45: Blocked Applications

Click the Application hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Web Categories

This Report displays a list of web categories along with the category type and number of hits and amount of data transferred per category.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Categories**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category while the tabular report contains the following information:

- **Category:** Displays name of the category as defined in the Device. If category is not defined in the Device then this field will display 'Uncategorized' at place of category name.
- **Category Type:** Displays name of the category type as defined in the Device. If the category type is not defined in the Device then it will display 'Uncategorized' which means the traffic is generated by an uncategorized type. By default there are four category types defined in the Device.
 - Productive
 - Unproductive
 - Acceptable
 - Objectionable
- **Hits:** Number of hits to the category.
- **Bytes:** Amount of data transferred.

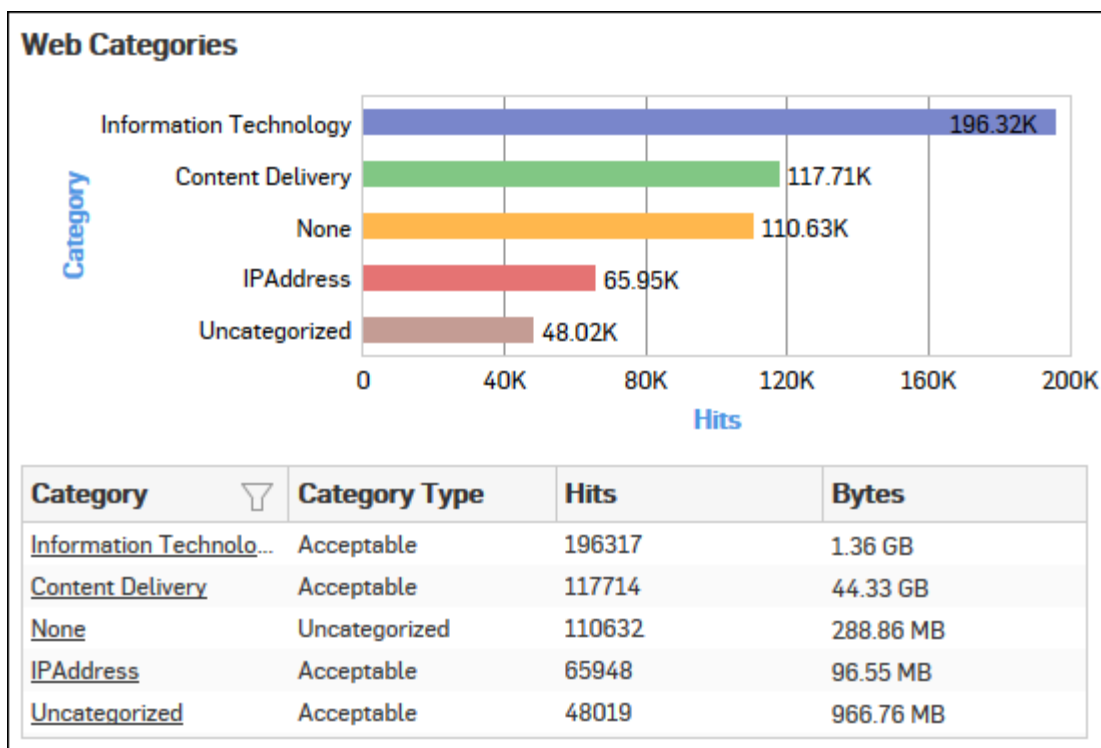


Figure 46: Web Categories

Click the Category hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Category Types

This Report displays list of Category Types along with the number of hits and amount of data transferred per category type.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Category Types**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category type while the tabular report contains the following information:

- **Category Type:** Displays name of the category type as defined in the Device. If the category type is not defined in the Device then it will display 'Uncategorized' which means the traffic is generated by an uncategorized type. By default there are four category types defined in the Device:
 - Productive
 - Acceptable
 - Unproductive
 - Objectionable
- **Hits:** Number of hits to the category type.
- **Bytes:** Amount of data transferred.

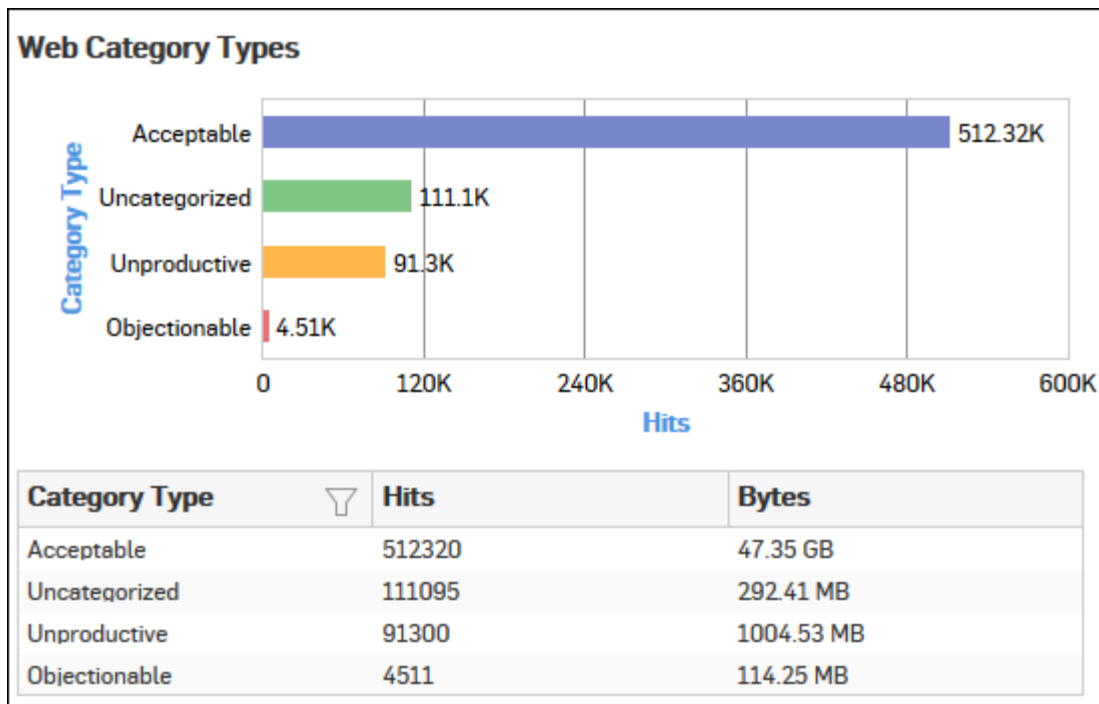


Figure 47: Web Category Types

Click the Category Type hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Objectionable Web Categories

This Report displays a list of Objectionable web categories accessed over the selected time period along with domain count per Objectionable category, number of hits and amount of data transferred through the category.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Categories**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Categories** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category while the tabular report contains the following information:

- Category: Displays name of the web category categorized as Objectionable in the Device.
- Domain Count: Number of domains accessed per Objectionable web category.
- Hits: Number of hits to the category.
- Bytes: Amount of data transferred.

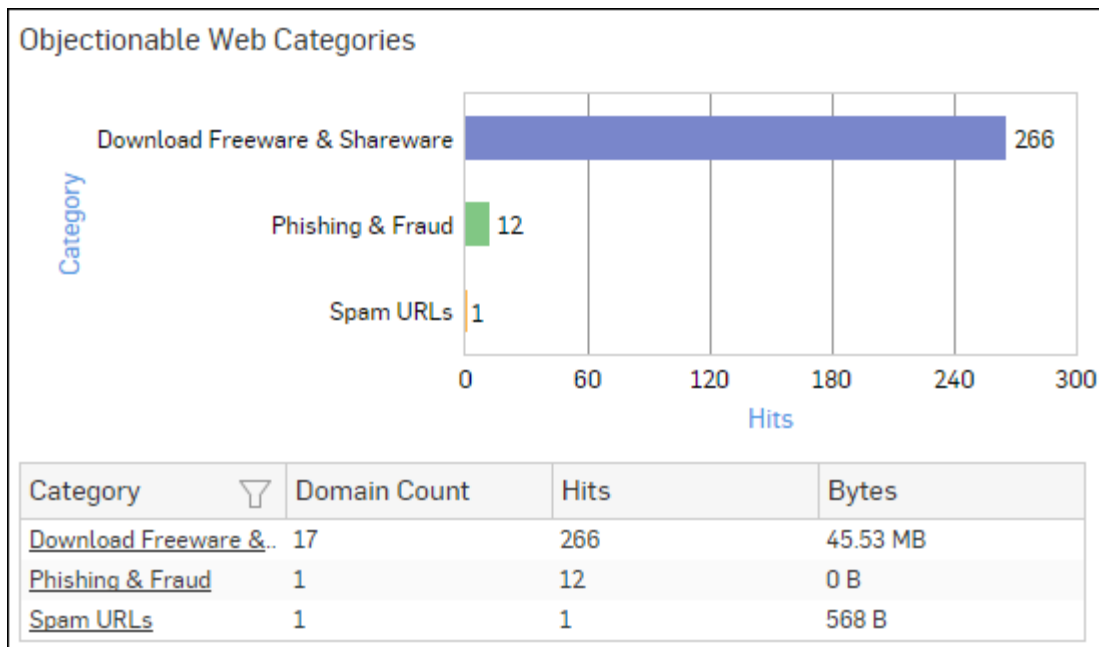


Figure 48: Objectionable Web Categories

Click the Category hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Objectionable Web Domains

This Report displays the list of Domains categorized under a Objectionable web category, along with number of hits and amount of data transferred through the domain.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Domains** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per domain while the tabular report contains the following information:

- Domain: Domain name or IP Address of the domain.
- Category: Name of the objectionable web category, under which the domain is categorized.
- Hits: Number of hits to the domain.
- Bytes: Amount of data transferred.

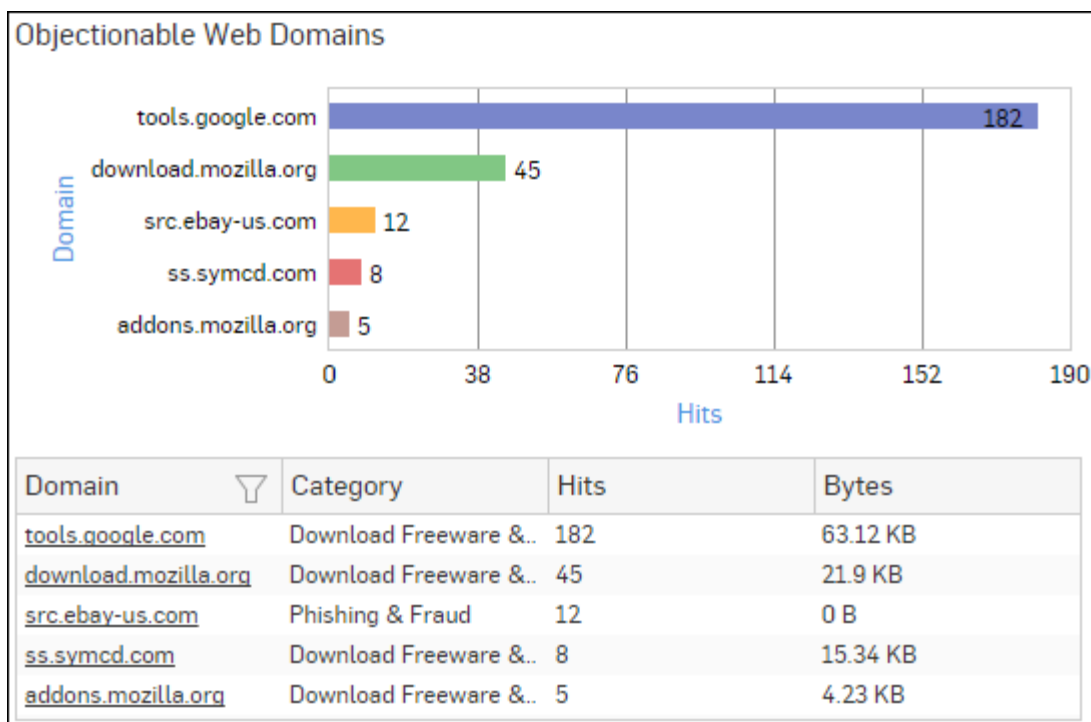


Figure 49: Objectionable Web Domains

Click the Domain hyperlink in table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Server Domains

This Report displays a list of frequently accessed web server domains according to the utilization of bandwidth, along with the number of requests per web server.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Web Server Domains** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of web servers along with the number of bytes while the tabular report contains the following information:

- Web Server Domain: Displays name of the web server domain.
- Bytes: Bandwidth used per web server domain.
- Requests: Number of requests per web server domain.

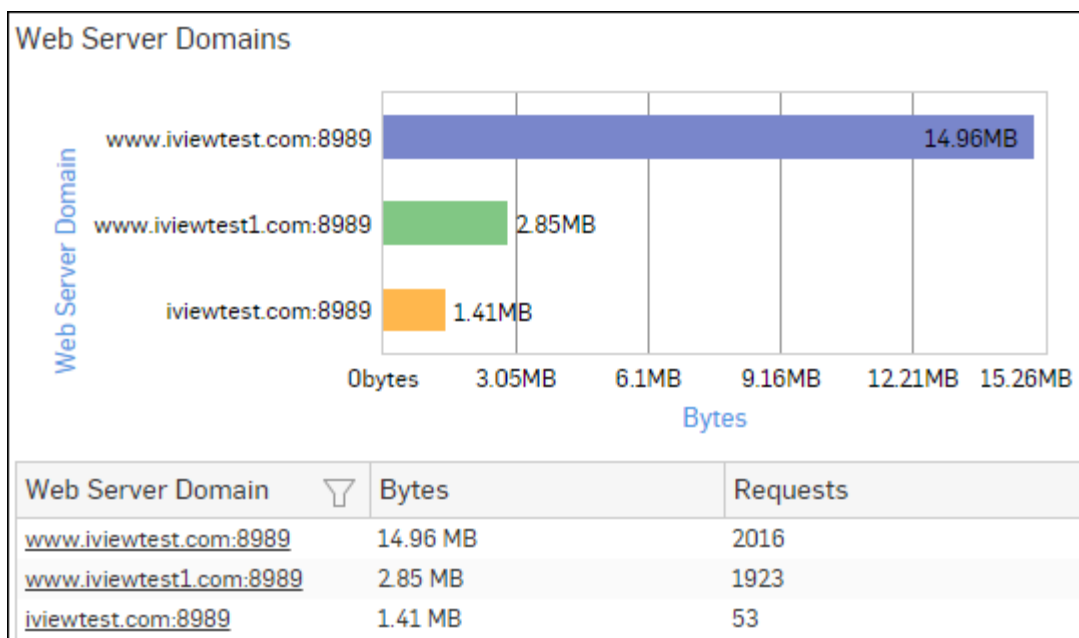


Figure 50: Web Server Domains

Click the Web Server Domain hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Blocked Web Server Requests

This Report displays a list of reasons of attacks blocked by the Device, along with the number of hits per attack.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Blocked Web Server Requests**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Server Requests** as well.

The bar graph displays the list of blocked reasons along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

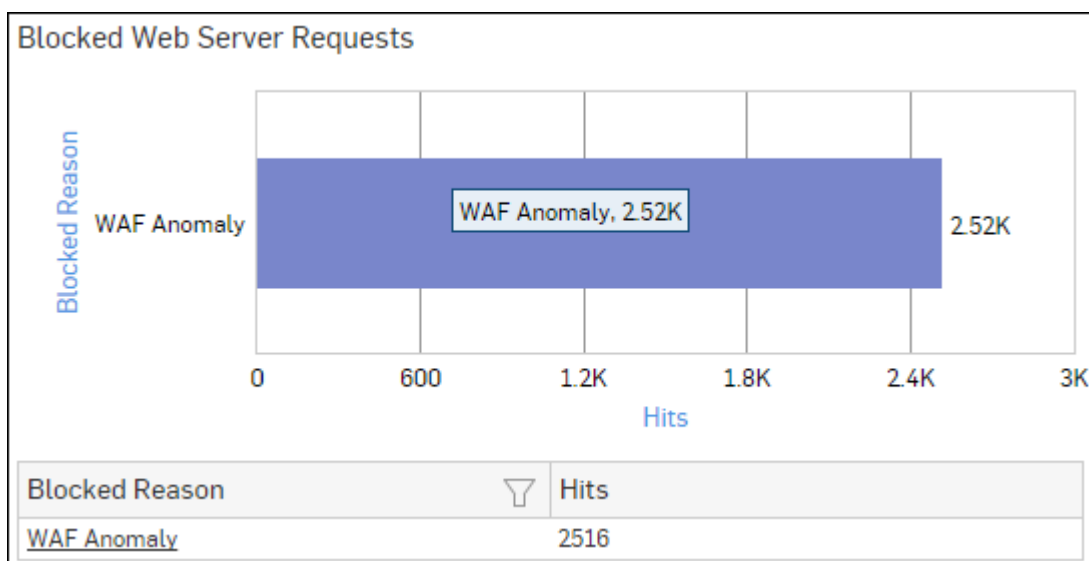


Figure 51: Blocked Web Server Requests

Click the Blocked Reason hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Intrusion Attacks

The Report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Attacks**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Attacks** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each attack, while the tabular report contains the following information:

- Attack: Name of the attack launched.
- Hits: Number of hits for each attack.

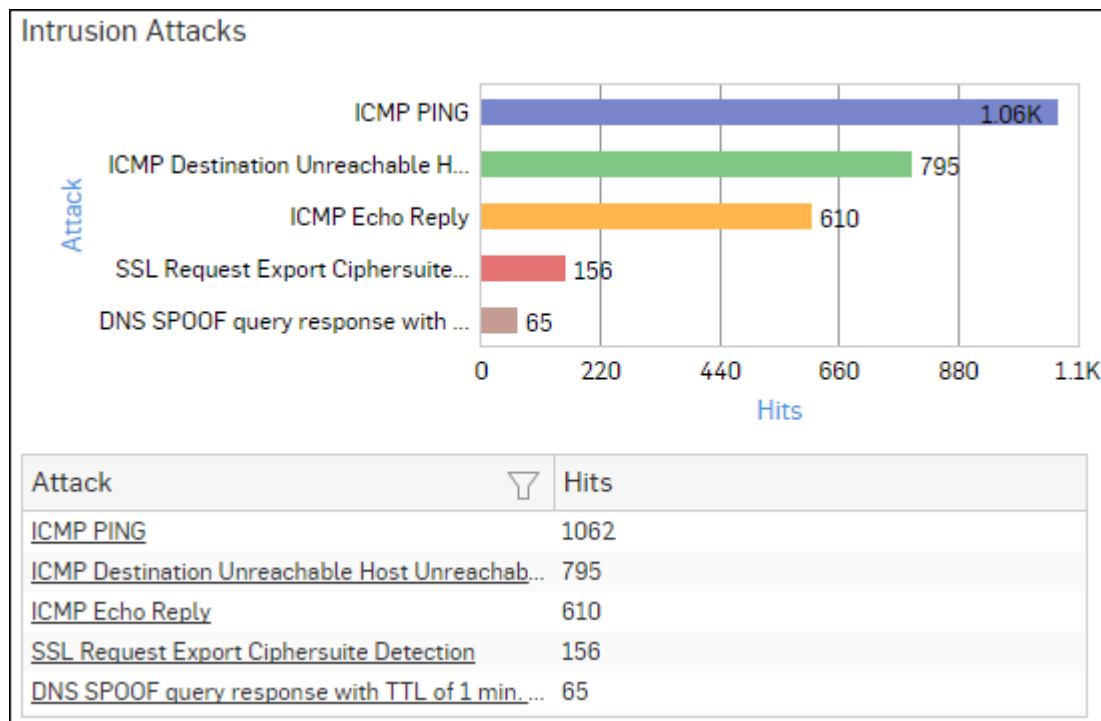


Figure 52: Intrusion Attacks

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Severity wise Attacks

The Report enables to view the severity of the attack that has hit the system and gives a detailed disintegration of the attacks, attackers, victims and applications through individual reports under severity.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Severity wise Attacks**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each severity, while the tabular report contains the following information:

- Severity: Severity level of the attack attempt. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION – Informational
 - DEBUG - Debug level messages
- Hits: Number of hits under each severity.

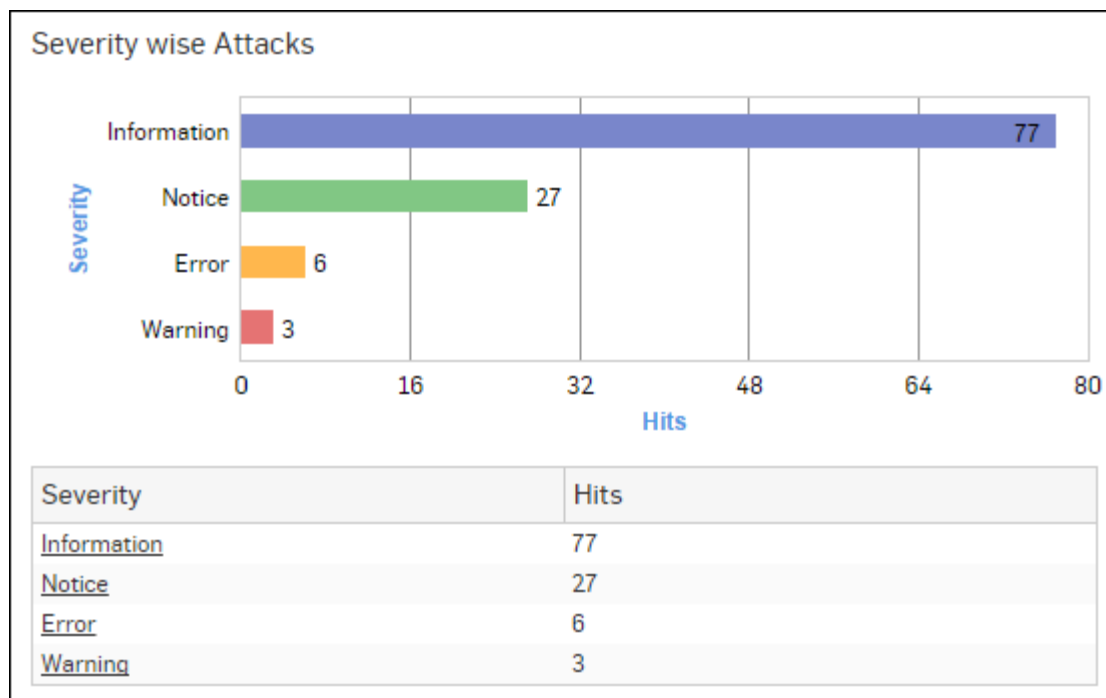


Figure 53: Severity wise Attacks

Click the Severity hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Advanced Threats

This report displays a comprehensive summary of advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Advanced Threats**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Advanced Threats** as well.

The report is displayed using a graph as well as in a tabular format.

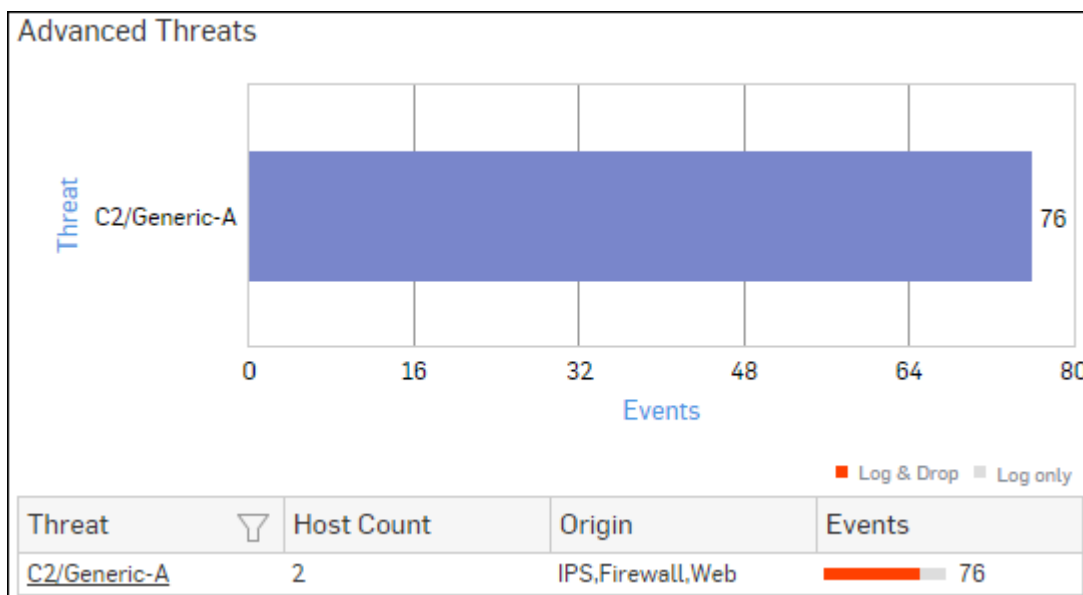
By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of threats along with total number of events per threat while the tabular report contains the following information:

- Threat: Name of the threat.

- Host Count: Number of hosts infected with the threat.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Events: Total number of events per threat. The number is summation of Log only and Log & Drop events.

Figure 54: Advanced Threats



Click Threat hyperlink in the table or graph to view the [Filtered ATP Reports](#).

Users - ATP

This report displays a comprehensive summary of user wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Users-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Users-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with total number of events per user while the tabular report contains the following information:

- User: User name of the infected user.
- Host Count: Number of hosts per user.
- Threat Count: Number of threats per user.
- Events: Total number of events per user. The number is summation of Log only and Log & Drop events.

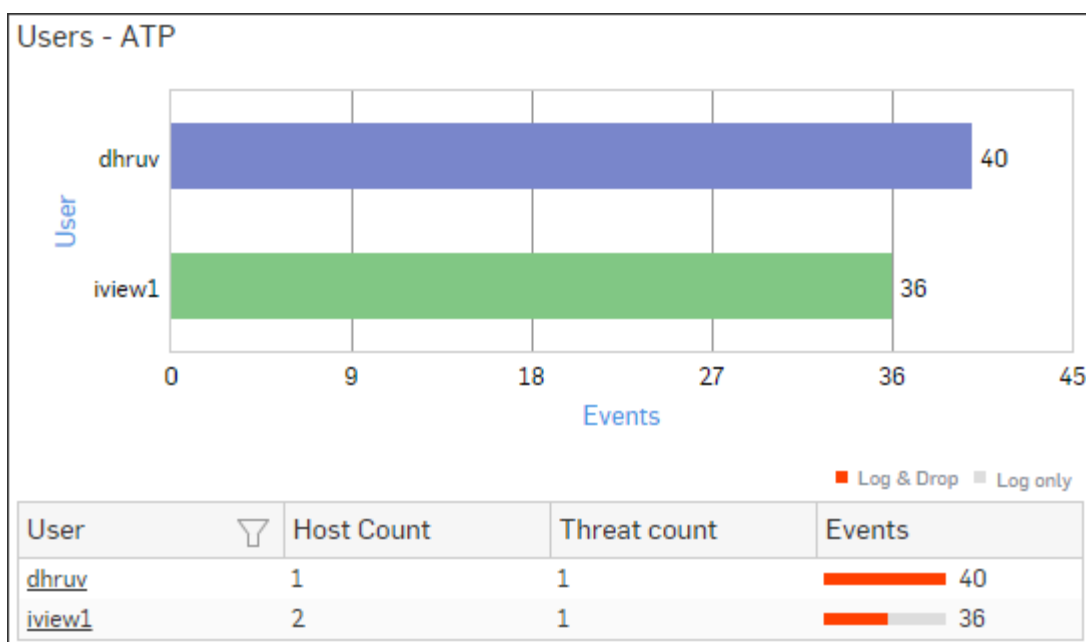


Figure 55: Users - ATP

Click User hyperlink in the table or graph to view the [Filtered ATP Reports](#).

Client Health

This report shows health status and number of endpoints per health status.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Client Health**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of endpoints per health status, while the tabular report contains the following information:

- Client Health: Displays client health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Count: Number of endpoints per health status.
- Percent: Percent-wise distribution among the client health status.

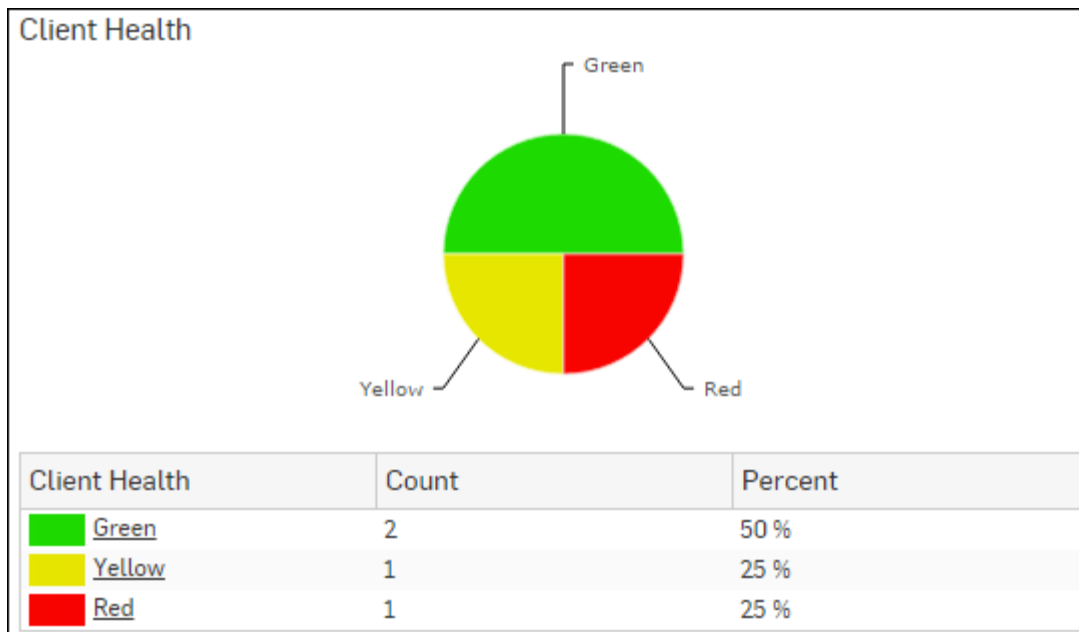


Figure 56: Client health

Click the Client Health status in the table or pie chart to view the [Filtered Security Heartbeat Reports](#).

Detailed View - Client Health

This report shows in-depth information regarding health status of endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Detailed View - Client Health**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Detailed View - Client Health** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Host Name: Name of the client.
- Health - Last Seen: Displays the latest health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.





Detailed View - Client Health				
Host (Source IP) ▾	Host Name ▾		Health - Last Seen	Last Health
10.20.41.8	TWIN8164BIT		Red	-
10.20.41.7	TWIN864		Yellow	-
10.198.38.8	TWIN764		Green	-
10.20.41.12	TWIN832		Green	-

Figure 57: Detailed View - Client Health

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Security Heartbeat - ATP

The report displays advanced threats associated with the endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Security Heartbeat - ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Heartbeat > Security Heartbeat - ATP** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Login User: User name of the user logged into the endpoint.
- Process User: Username of the user running the process.
- Executable: Name of the infected executable (.exe) file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the destination.
- Event Last Seen: Displays the date in YYYY-MM-DD HH:MM:SS format when the event was last seen.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP									
Host (Source IP) ▾	Login User ▾	Process User ▾	Executable ▾	Threat ▾	Threat URL/IP ▾	Event Last Seen	Events		
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1		

Figure 58: Security Heartbeat - ATP

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Mail Traffic Summary

This Report displays type of Email traffic along with number of emails and percentage distribution among the traffic type.

View the report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Mail Traffic Summary**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays relative percentage distribution of traffic types, while the tabular report contains the following information:

- Traffic: The type of Email traffic. Possible types are :

- Clean Mail
- Spam
- Probable Spam
- Virus
- Mail Count: Number of emails per traffic type.
- Percent: Relative percentage distribution among the traffic types.

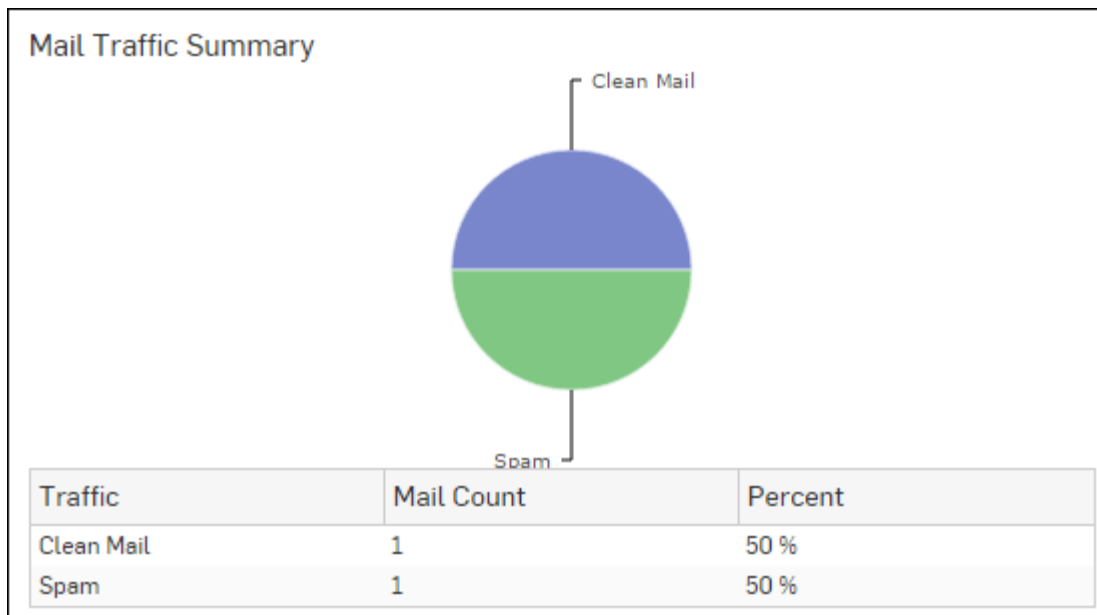


Figure 59: Mail Traffic Summary

Click the Traffic hyperlink in the table or the pie chart to view the [Filtered Email Usage Reports](#).

Spam Senders

This Report displays a list of Spam Senders along with number of emails and percent distribution among the spam senders.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Senders**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Senders** as well.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of spam emails sent.
- Percent: Relative percent distribution among the spam sender.

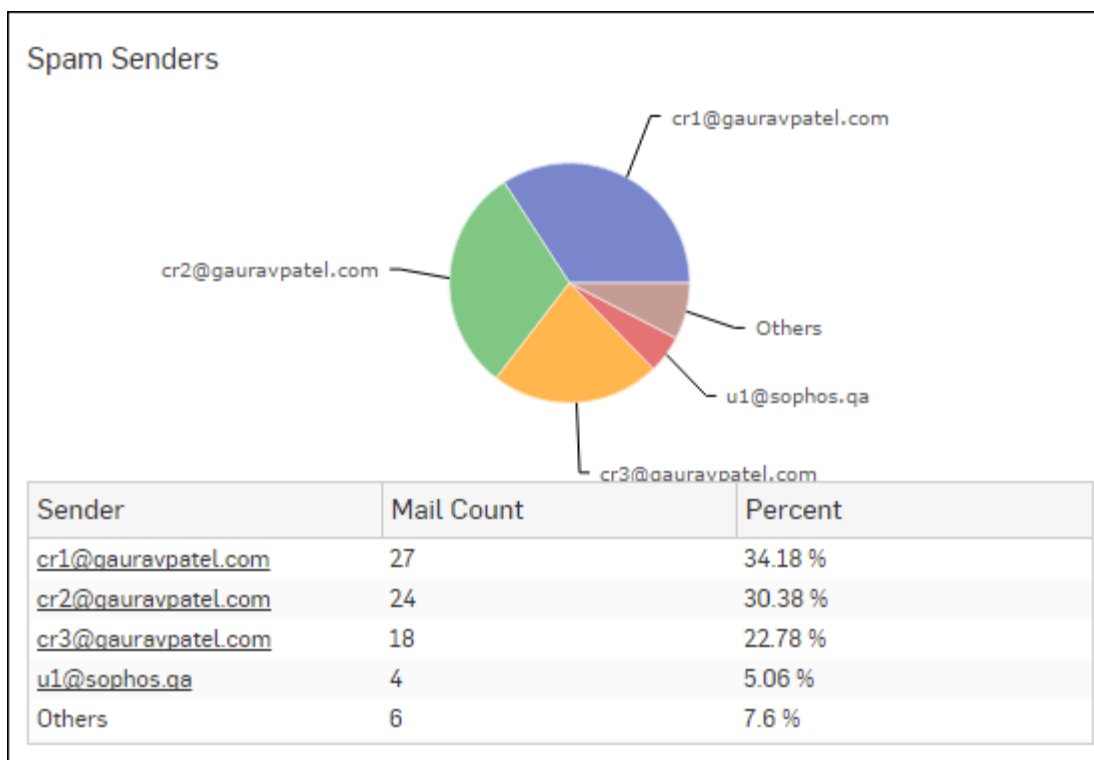


Figure 60: Spam Senders

Click the Sender hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Spam Recipients

This Report displays a list of Spam Recipients along with number of emails and percent distribution among the spam recipients.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Recipients**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Recipients** as well.

The Report is displayed as a pie chart as well as in a tabular format.

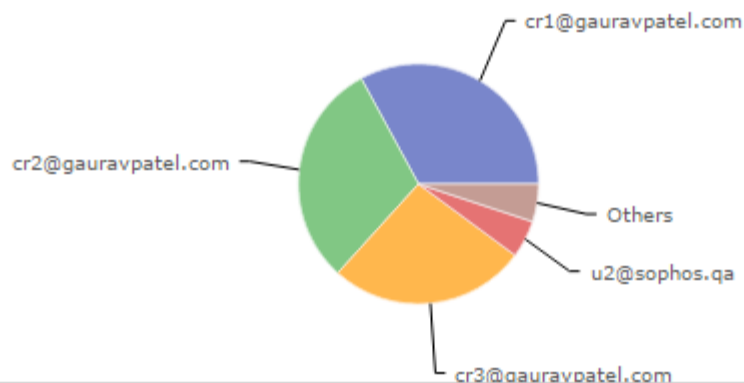
By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.
- Percent: Relative percent distribution among the spam recipients.

Figure 61: Spam Recipients

Spam Recipients



Recipient	Mail Count	Percent
cr1@gauravpatel.com	26	32.91 %
cr2@gauravpatel.com	24	30.38 %
cr3@gauravpatel.com	21	26.58 %
u2@sophos.qa	4	5.06 %
Others	4	5.07 %

Click the Recipient hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Mail Virus

This Report displays Viruses detected in your network along with number of hits per Virus.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus while the tabular report contains the following information:

- Virus: Name of the virus.
- Count: Number of counts per mail virus.

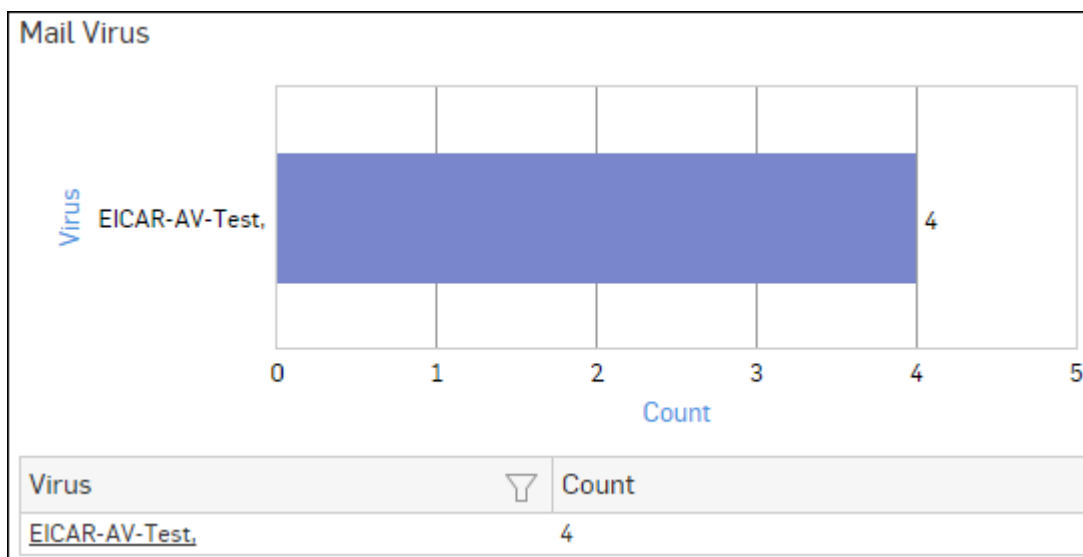


Figure 62: Mail Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Virus Reports](#).

CPU Usage

The report displays CPU usage by the Users and System components.

View the report from **Monitor & Analyze > Reports > Custom > Executive Report > CPU Usage**.

The report is displayed in tabular format.

The report displays following details:

- CPU: CPU usage by the Users and System components. Possible options are:
 - User: CPU usage by User.
 - SystemConfiguration: CPU usage by System.
 - Idle: CPU Idle time
- Max: Maximum CPU usage, in percent.
- Min: Minimum CPU usage, in percent.
- Average: Average CPU usage, in percent.

CPU Usage			
CPU	Max	Min	Average
User	27.36%	0.78%	2.09%
SystemConfiguration	0.56%	0.05%	0.13%
Idle	99.15%	72.45%	97.78%

Figure 63: CPU Usage

Memory Usage

The report displays information related to Device memory including memory used, free memory and total available memory.

View the report from **Monitor & Analyze > Reports > Custom > Executive Report > Memory Usage**.

The report is displayed in tabular format.

The report displays following details:

- Memory: Displays memory usage status. Possible options are:

- Free: Amount of free memory.
- Used: Amount of used memory.
- Total: Total amount of memory.
- Max: Maximum memory usage, in Bytes.
- Min: Minimum memory usage, in Bytes.
- Average: Average memory usage, in Bytes.

Memory Usage			
Memory	Max	Min	Average
Free	4.19 GB	4.02 GB	4.14 GB
Used	1.79 GB	1.62 GB	1.67 GB
Total	5.81 GB	5.81 GB	5.81 GB

Figure 64: Memory Usage

Disk Usage

The report displays the minimum, maximum and average amount of disk usage in percentage by various components.

View the report from **Monitor & Analyze > Reports > Custom > Executive Report > Disk Usage**.

The report is displayed in tabular format.

The report displays following details:

- Partition: Displays partition name. Possible options are:
 - Signature
 - Config
 - Reports
 - Temp
- Max: Maximum disk usage in percentage by each partition.
- Min: Minimum disk usage in percentage by each partition.
- Average: Average disk usage in percentage by each partition.

Disk Usage			
Partition	Max	Min	Average
Signature	8.00%	8.00%	8.00%
Config	13.00%	13.00%	13.00%
Reports	1.00%	1.00%	1.00%
Temp	0.00%	0.00%	0.00%

Figure 65: Disk Usage

Live Users

The report displays the number of live user for the selected time duration.

View the report from **Monitor & Analyze > Reports > Custom > Executive Report > Live Users**.

The report is displayed in tabular format.

The report displays following details:

- Live User: Number of users (live) connected to the Internet.
- Max: Maximum number of connected users during the selected graph period.
- Min: Minimum number of connected users during the selected graph period.

- Average: Average number of connected users during the selected graph period.

Live Users			
Live User	Max	Min	Average
LiveUsers	14.00	13.00	13.75

Figure 66: Live Users

Interface

The report displays details of network traffic processed by Ethernet interfaces in the Device.

View the report from **Monitor & Analyze > Reports > Custom > Executive Report > Interface**.

The report is displayed in tabular format.

The report displays following details:

- Port: Name of the port.
- Transfer Type: Type of data transfer. Possible options are:
 - Bits Received (Kbits/sec)
 - Bits Transmitted (Kbits/sec)
- Max: Maximum amount of data transferred through the interface during the selected time period.
- Min: Minimum amount of data transferred through the interface during the selected time period.
- Average: Average amount of data transferred through the interface during the selected time period.

Interface				
PORT	Transfer Type	Max	Min	Average
eth0	ReceivedKBits	196.54	12.48	38.49
eth0	TransmittedKBits	1429.93	151.74	331.29
eth1	ReceivedKBits	849.44	36.6	146.79
eth1	TransmittedKBits	202.51	3.18	32.46
eth2	ReceivedKBits	0.0	0.0	0.0

Figure 67: Interface

User Threat Quotient (UTQ)

User Threat Quotient (UTQ) report provides actionable security intelligence to an administrator, by helping them to get quick visibility of risky users who are posing security threats on organization's network.



Note: Either Web Protection or Network Protection subscription is required to view the UTQ reports.

Correlating data from various logs and reports to identify the risky users takes time and analytical skills for administrators, not to forget the chances of human oversight. UTQ gives automatic analysis of user's Internet behavior, saving the administrators to go through the hassle of correlating the data.

Sophos Firewall calculates UTQ score of each user based on following two criteria:

1. Web surfing behaviour (Only Allowed, but potentially risky and Denied Web traffic for each user)
2. Advanced Threat Protection (ATP) logs (Infected clients/hosts or clients that are part of botnet)

UTQ helps administrator to:

- Spot risky users at a glance.
- Identify which clients/hosts within the network are infected or part of botnet
- Find out malicious insiders.
- Avoid chances of human oversight in correlating data from various logs and reports.

- Take appropriate actions like fine-tuning security policies, security awareness training etc.

Given below are the terms and icons used in UTQ along with their meanings:

- Relative Threat Score – Maximum threat posed by the user (in number), relative to the web behaviour of all other users for the selected date or date range.
- Relative Risk Ranking – Rank of the user (in number), in terms of posing security risk on the organization's network, relative to the web behaviour of all the other users for the selected date or date range.
- **UTQ score : 5.28** – UTQ Risk Meter, which displays average threat score for the selected user, relative to the threat scores of all other users for the selected date or date range.

UTQ report is displayed in the form of bubble graph as well as in a tabular format. The bubble graph is plotted between Relative Risk Ranking and Relative Threat Score; where the bubble represents the user and bubble size represents Relative Threat posed by the user. Mouse over on the bubble displays details like Username, Relative Threat Score and Relative Risk Ranking of a user.

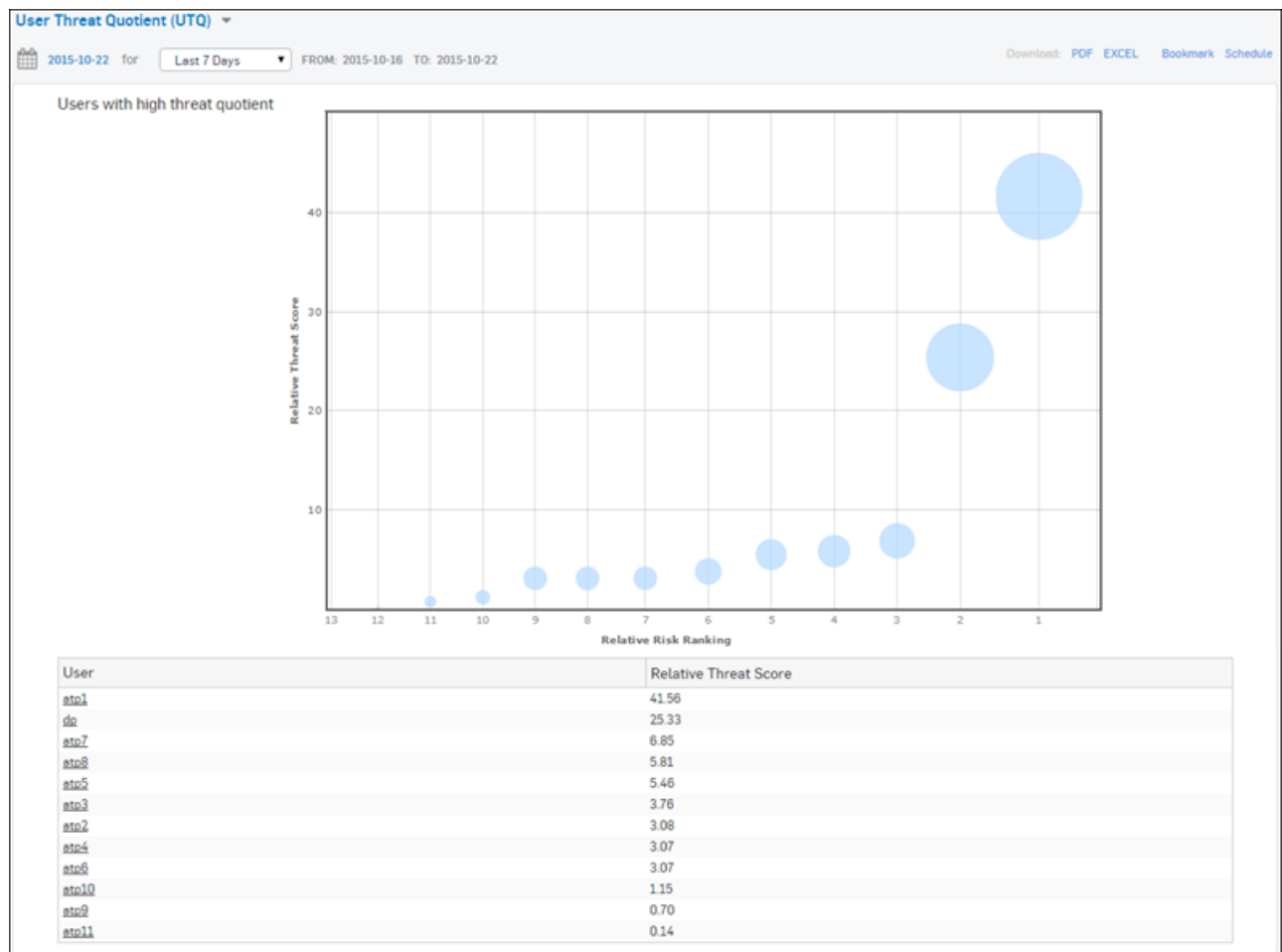


Figure 68: User Threat Quotient (UTQ)

The bubble graph area is divided into three sections where;

- Top 10% are marked as High Risk Users
- Next 40% are marked as Medium Risk Users
- Last 50% are marked as Low Risk Users



Note: When the number of users for the selected period is less than 20, all the users are displayed as Blue bubbles and the sections mentioned above are not displayed.

The tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined, then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Relative Threat Score: Threat posed by the user (in number), relative to the web behaviour of all the other users, for the selected period.

Please note that UTQ is calculated and displayed after 24 hours only, which means there is no UTQ for current day. UTQ can be viewed for:

- Last 14 Days
- Last 7 Days
- Last 1 Day

By default, UTQ displays up to 100 risky users for the last 7 days along with their Relative Threat Score and Relative Risk Ranking.

Top most right corner of the screen displays UTQ Risk Meter, which displays relative threat score for the selected user.

Click User hyperlink in the table or bubble in the graph to view [Reports by User and Date](#) for the selected period.

Reports by User and Date

To view the following reports for a particular user and date, go to **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**:

- [Advanced Threats](#)
- [Detailed View - ATP](#)
- [Client Insights - ATP](#)
- [High Risk Web Categories](#)
- [High Risk Web Domains](#)
- [Blocked High Risk Web Categories](#)
- [Blocked High Risk Web Domains](#)

Advanced Threats widget

Widget report displays a comprehensive summary of advanced threats in your network.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of threats along with total number of attempts per threat while the tabular report contains the following information:

- Threat: Name of the threat.
- Host Count: Number of hosts infected with the threat.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Attempts: Total number of attempts per threat. The number is summation of Log only and Log & Drop attempts.

Detailed View - ATP widget

Widget report provides a detailed summary of advanced threats in your network.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Date: Date in YYYY-MM-DD format
- Host (Source IP): IP Address of the source host.
- Threat: Name of the threat.
- Destination: IP Address of the infected destination.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Attempts: Total number of attempts. The number is summation of Log only and Log & Drop attempts.
- Action: Action performed by the Device when a threat is detected. Possible options:
 - Log & Drop: The data packet is logged and dropped.
 - Log only: The data packet is logged.

Security Heartbeat - ATP widget

Widget report provides an insight into advanced threats related to endpoints in your network.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**.

The report is displayed in a tabular format. The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Login User: Username of the infected user.
- Process User: Username of the user owning the process.
- Executable: Name of the infected executable file.
- Threat: Name of the threat.
- Destination: IP Address of the infected destination.
- Event Last Seen: Time when the infected executed file was last found in the host.
- Attempts: Total number of attempts. The number is summation of Log only and Log & Drop attempts.

High Risk Web Categories widget

Widget report displays list of top allowed web categories along with number of hits per web category.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per web category while tabular report contains following information:

- Category: Name of the Web category as defined in the Device.
- Hits: Number of hits to the Web category.

Click Category hyperlink or graph to view list of [High Risk Web Domains](#) for the selected User, Date / Date Range and Web Category.

High Risk Web Domains widget


Widget report displays list of top allowed web domains along with number of hits per web domain.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per web domain while tabular report contains following information:

- Domain: Name/IP Address of the domain.
- Category: Name of the Web category for the domain.
- Hits: Number of hits to the domain.

Click  icon view the [list of URLs](#) that the selected user has accessed for the domain.

Click  icon to view the [list of users](#) who have accessed this domain.

Blocked High Risk Web Categories widget

Widget report displays list of top denied web categories along with number of hits per web category.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per denied web category while tabular report contains following information:

- Category: Name of the Web category as defined in the Device.
- Hits: Number of hits to the Web category.

Click Category hyperlink or graph to view list of [Blocked High Risk Web Domains](#) for the selected User, Date / Date Range and Web Category.

Blocked High Risk Web Domains widget


Widget report displays list of top denied web domains along with number of hits per domain.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per denied web domain while tabular report contains following information:

- Domain: Name/IP Address of the domain.
- Category: Name of the Web category for the domain.
- Hits: Number of hits to the domain.

Click  icon view the [list of URLs](#) that the selected user has accessed for the domain.

Click  icon to view the [list of users](#) who have accessed this domain.

High Risk Web Domains


Widget report displays list of top allowed risky web domains along with number of hits per domain.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User > High Risk Web Categories widget > Category**

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per web domain while tabular report contains following information:

- Domain: Name/IP Address of the domain.
- Category: Name of the Web category for the domain.
- Hits: Number of hits to the domain.

Click  icon view the [list of URLs](#) that the selected user has accessed for the domain.

Click  icon to view the [list of users](#) who have accessed this domain.

Blocked High Risk Web Domains

Widget report displays list of top denied risky web domains along with number of hits per domain.

View the report from **Monitor & Analyze > Reports > Dashboards > User Threat Quotient (UTQ) > User > Blocked High Risk Web Categories widget > Category.**

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per denied web domain while tabular report contains following information:

- Domain: Name/IP Address of the domain.
- Category: Name of the Web category for the domain.
- Hits: Number of hits to the domain.

Click  icon to view the [list of users](#) who have accessed this domain.

Detailed Report

Detailed report displays list of URLs accessed by selected user for the selected domain.

The detailed report contains following information:

- Time : Time in YYYY-MM-DD HH:MM:SS format .
- Host : IP Address or name of the host.
- URL: IP Address or URL name.

Click View hyperlink against an URL to access the URL.

Domain-wise Users

Report displays list of users who have accessed the particular domain.

Domain wise users report contains following information.

- User : Name of the user as defined in the Device.
- Hits: Number of hits to the domain by the user.

Click  icon to view the [detailed report](#) showing a list of URLs that the selected user has accessed for the domain.

Applications & Web

This section provides insight about usage of Applications, Web, Internet and FTP traffic in your network.



Note: The Applications & Web sub sections can be accessed by selecting drop-down 1 given at the upper left corner of the page.

This report contains following sub-sections.

- [User App Risks & Usage](#)
- [Blocked User Apps](#)
- [Web Risks & Usage](#)
- [Blocked Web Attempts](#)
- [Search Engine](#)
- [Web Server Usage](#)
- [Web Server Protection](#)
- [User Data Transfer Report](#)
- [FTP Usage](#)
- [FTP Protection](#)

User App Risks & Usage

The User App Risks & Usage reports dashboard provides an insight about the usage of various applications and associated risks.

View the reports dashboard from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The Device provides a Risk Meter on the top right corner of all application reports. This risk calculator indicates the overall risk associated with the application(s). The overall risk is calculated on the basis of individual risk associated with the application and number of hits on that application.

User App Risks & Usage reports dashboard enable you to view traffic generated by:

- [Source Zones](#)
- [Destination Zones](#)
- [Application Categories](#)
- [Applications](#)
- [Application Users](#)
- [Application Technologies](#)
- [High Risk Applications](#)
- [Application Risk Levels](#)
- [High Risk Application Users](#)
- [Hosts - High Risk Applications](#)
- [Hosts](#)
- [Source Countries](#)
- [Destination Countries](#)
- [Allowed Policies](#)

Source Zones

This Report displays a list of Source Zones along with the type of zone, number of hits per zone and zone wise total amount of data transfer.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Source Zones**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of network zones along with the amount of data transfer while the tabular report contains the following information:

- Source Zone: Displays name of the zone as defined in the Device.
- Zone Type: Type of the Zone. Possible types are: LAN, WAN, DMZ, VPN and WiFi.
- Hits: Number of hits per zone.
- Bytes: Amount of data transferred.

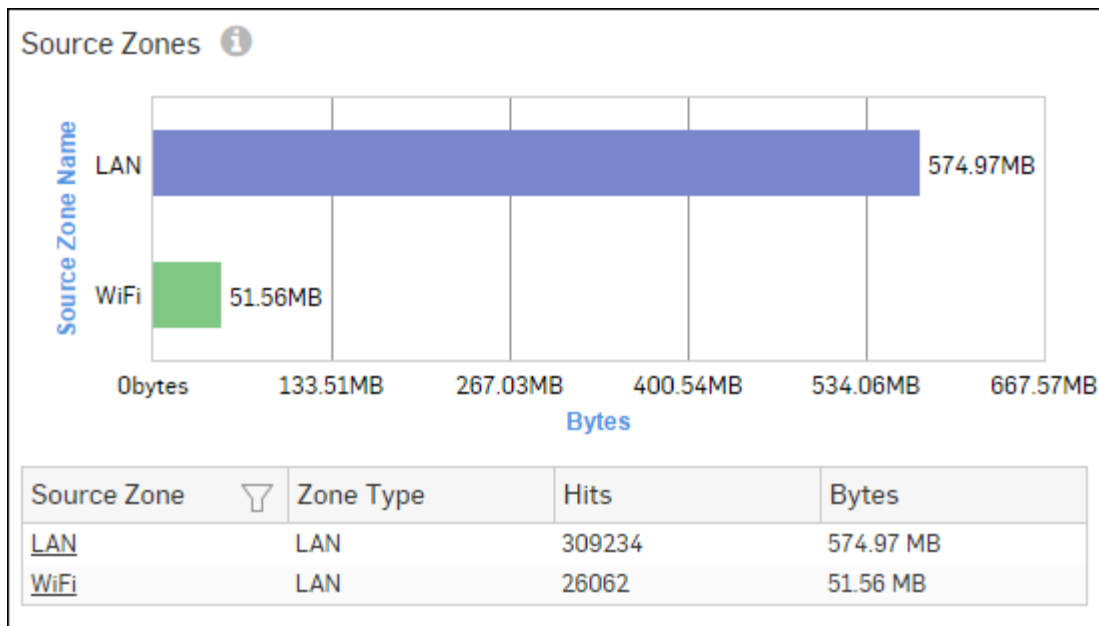


Figure 69: Source Zones

Click the Source Zone hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Destination Zones

This report displays a list of top destination zones along with the type of zone, number of hits per zone and zone wise total amount of data transfer.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Destination Zones**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of destination network Zones along with the amount of data transfer while the tabular report contains the following information:

- Destination Zone: Displays name of the zone as defined in the Device.
- Zone Type: Type of the Zone. Possible types are: LAN, WAN, DMZ, VPN and WiFi.
- Hits: Number of hits per zone.
- Bytes: Amount of data transferred.

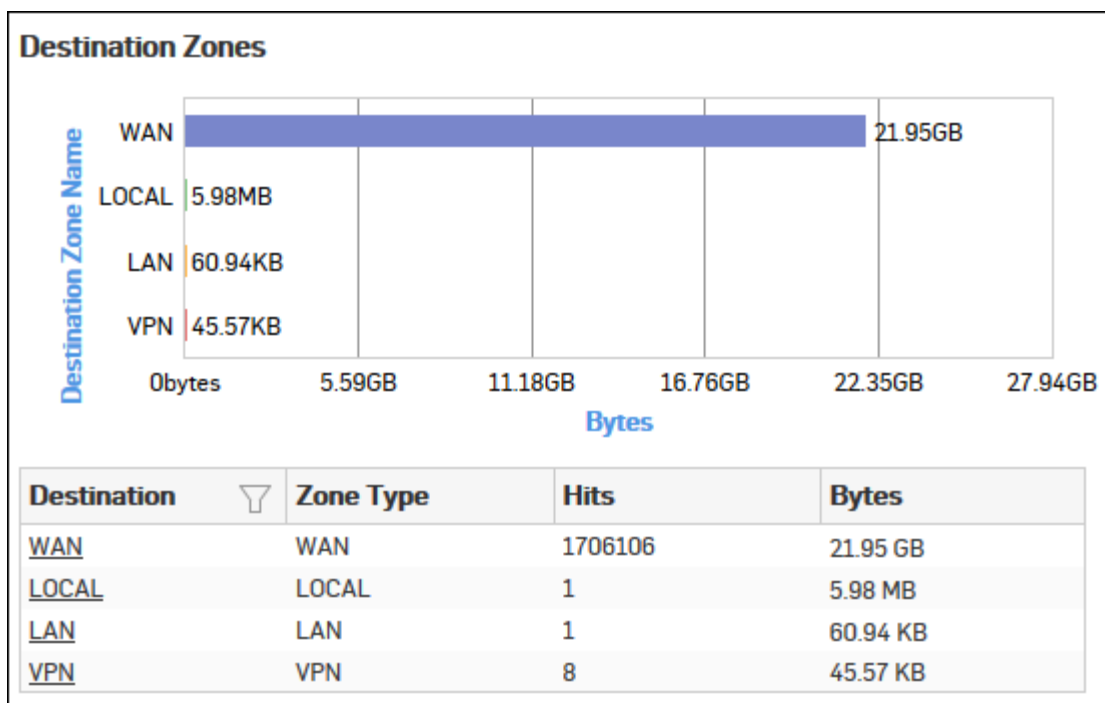


Figure 70: Destination Zones

Click the Destination Zone hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Application Categories

This report displays a list of top Application Categories along with number of hits per category and total amount of data transfer using that application.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Application Categories**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of application categories along with the number of hits while the tabular report contains the following information:

- Category: Displays name of the Application Category as defined in the Device.
- Hits: Number of hits per application category.
- Bytes: Amount of data transfer through the application category, in bytes.

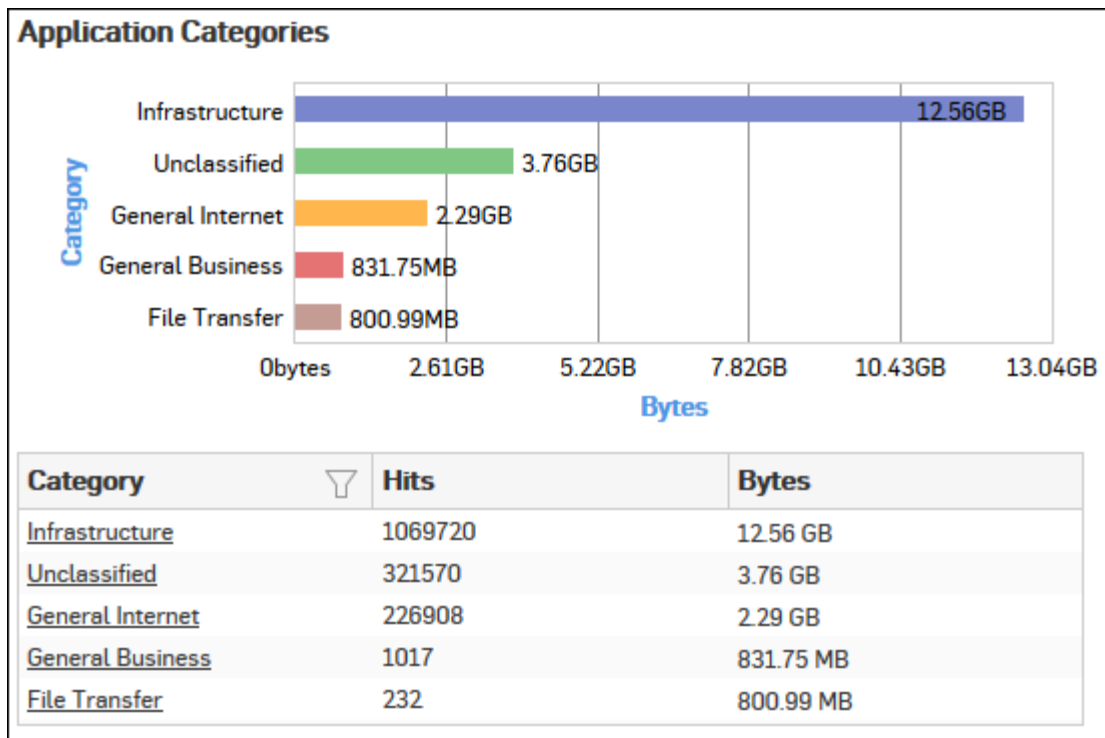


Figure 71: Application Categories

Click the Category hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Applications

This report displays a list of Applications along with the number of hits per application and the total amount of data transfer using that application.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Applications**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of application categories along with the number of hits while the tabular report contains the following information:

- Application/Proto: Port Displays name of the Application as defined in the Device. If the application is not defined in the Device then this field will display the application identifier as a combination of the protocol and port number.
- Risk: Level of risk associated with the application.
- Category: Name of the associated application category.
- Hits: Number of hits per application.
- Bytes: Amount of data transfer through the application, in bytes.

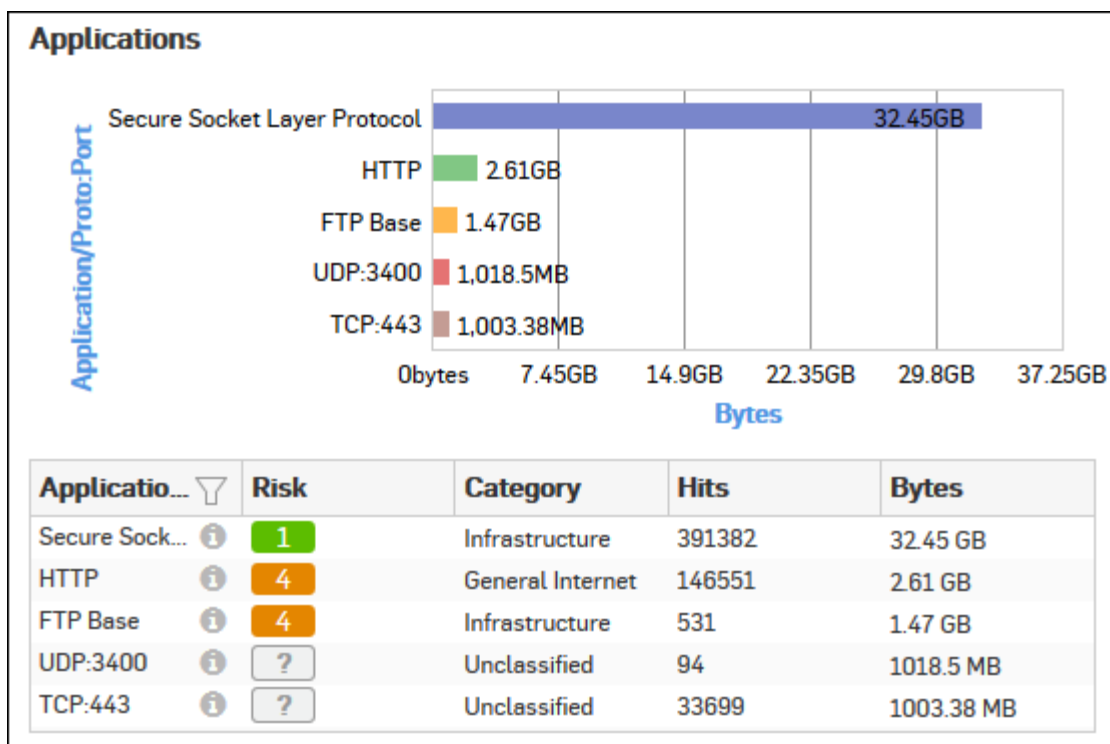


Figure 72: Applications

Click the Application hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Application Users

This report displays a list of Users along with the number of hits per user and total amount of data transfer by each user.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Application Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with number of hits while the tabular report contains the following information:

- User: Username of the user as defined in the monitored device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Hits: Number of hits per user.
- Bytes: Amount of data transfer through the user, in bytes.

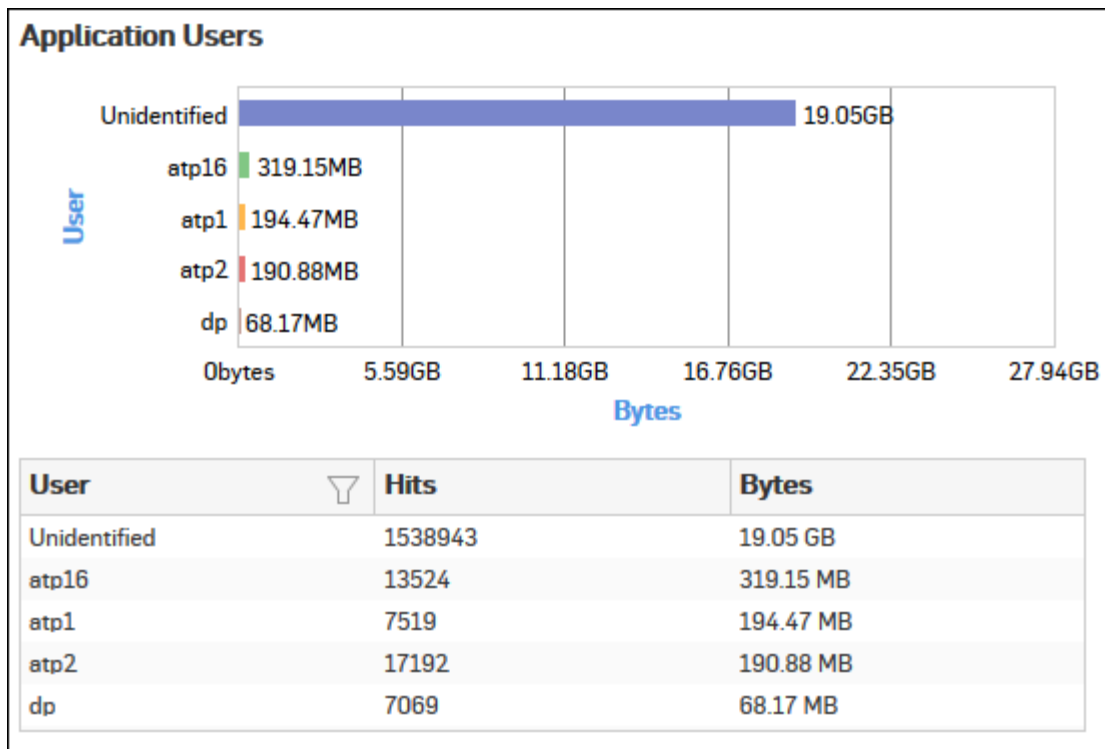


Figure 73: Application Users

Click the User hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Application Technologies

This report displays a list of application Technologies along with the number of hits per technology and the total amount of data transfer by the technology.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Application Technologies**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of technologies along with the amount of data transfer while the tabular report contains the following information:

- Technology: Displays name of the technology as defined in the Device.
- Hits: Number of hits per technology.
- Bytes: Amount of data transfer through the technology, in bytes.

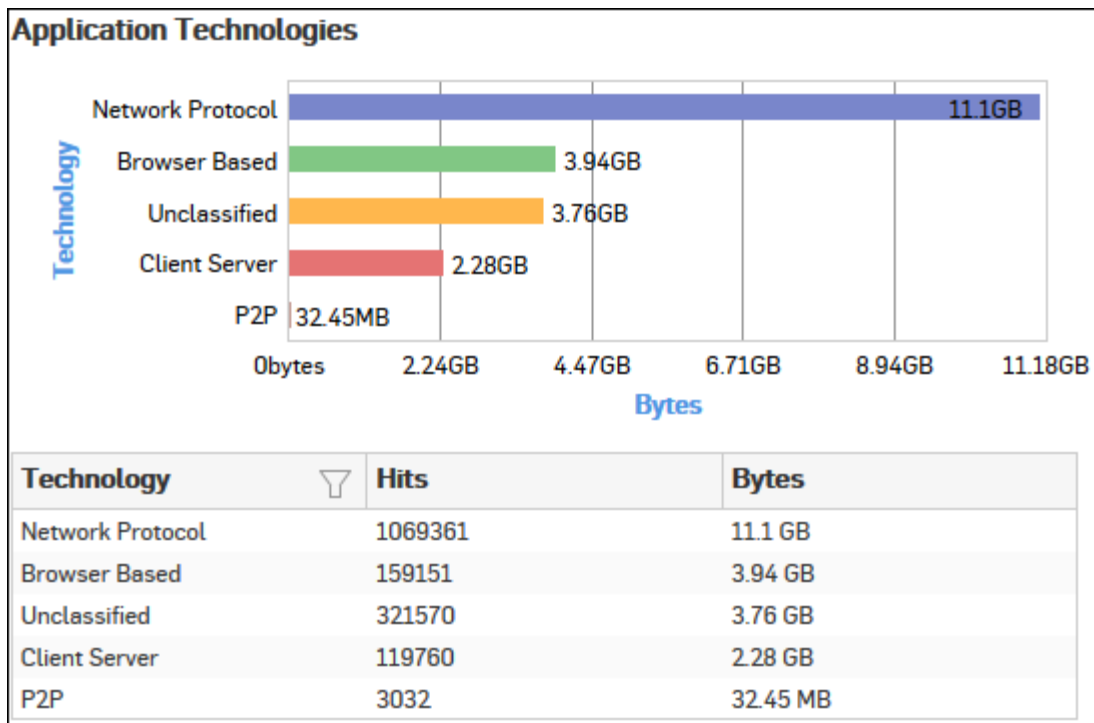


Figure 74: Application Technologies

Click the Technology hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

High Risk Applications

This Report displays a list of Applications with Risk Level greater than equal to 4, along with number of hits and total amount of data transfer per application.

View the report from User App Risks & Usage reports dashboard or **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > High Risk Applications**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > High Risk Applications** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. The date can be changed from the top most row of the page.

The bar graph displays the list of high risk applications along with amount of data transfer per application, while the tabular report contains the following information:

- Application/Proto: Port: Name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of the protocol and port number.
- Risk: Level of risk associated with the application.
- Hits: Number of hits per application.
- Bytes: Amount of data transfer through the application, in bytes.

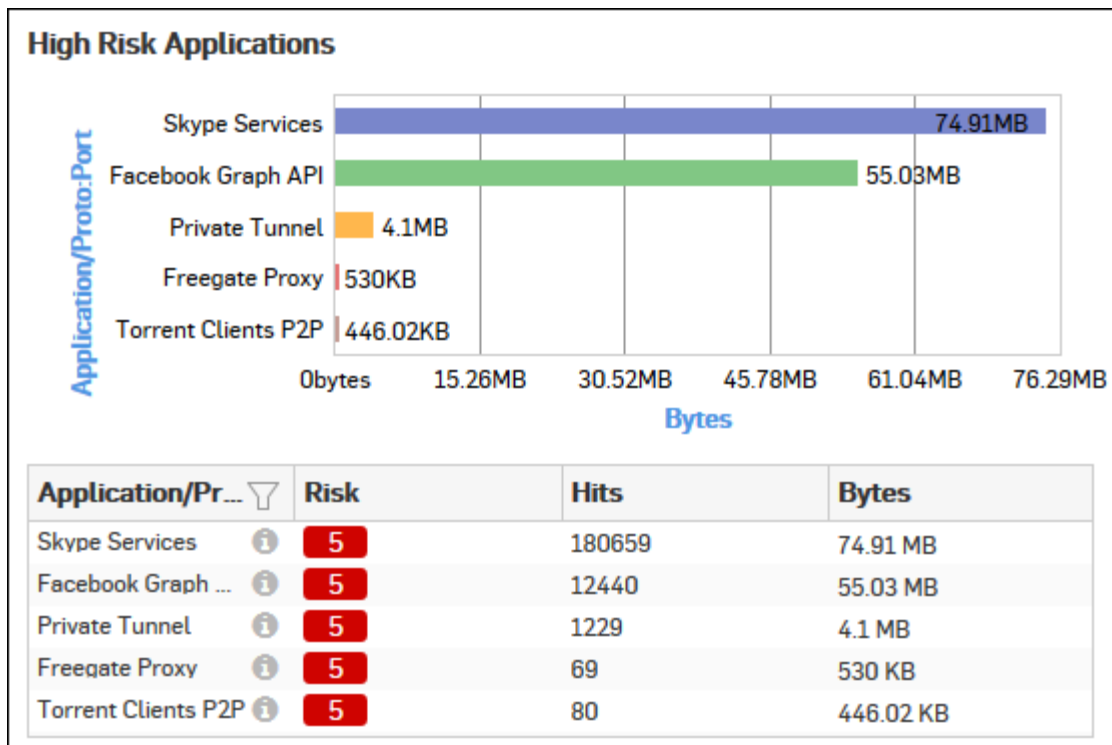


Figure 75: High Risk Applications

Click the Application hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Application Risk Levels

This report displays a list of Risk Levels associated with the various applications accessed in the network, along with the number of hits and total amount of data transfer per risk level.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Application Risk Levels**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of risk levels along with the amount of data transfer while the tabular report contains the following information:

- Risk: Risk associated with an application. Higher number shows higher risk.
- Application Count: Number of applications accessed per risk level.
- Hits: Number of hits to the applications with mentioned risk level.
- Bytes: Amount of data transfer through the applications with mentioned risk level, in bytes.

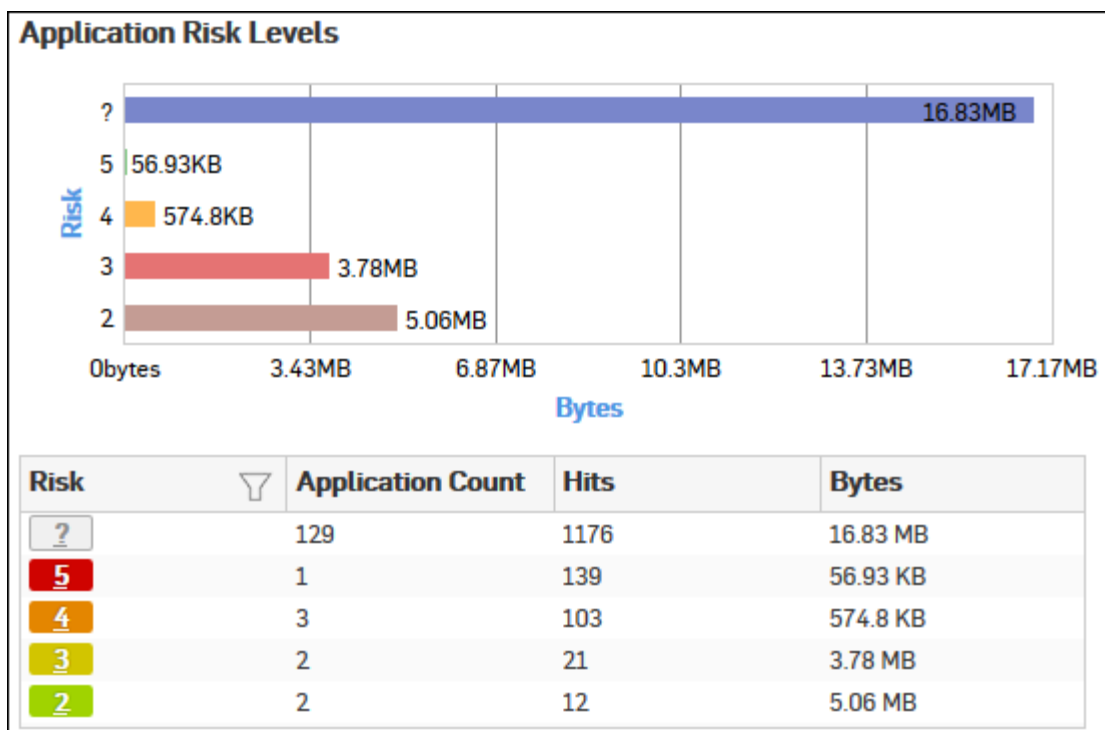


Figure 76: Application Risk Levels

Click the Risk level hyperlink in the table or pie chart to view the [Filtered User App Risks & Usage Reports](#).

High Risk Application Users

This Report displays a list of Users accessing high risk applications (Risk Level greater than or equal to 4), along with application count, total number of hits to the applications and total amount of data transfer by each user.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > High Risk Application Users**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > High Risk Application Users** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with number of hits while the tabular report contains the following information:

- **Username:** Username of the user as defined in the monitored device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- **Application Count:** Number of applications accessed per user.
- **Hits:** Number of hits to the high risk applications accessed by the user.
- **Bytes:** User-wise amount of data transfer through the high risk applications, in bytes.

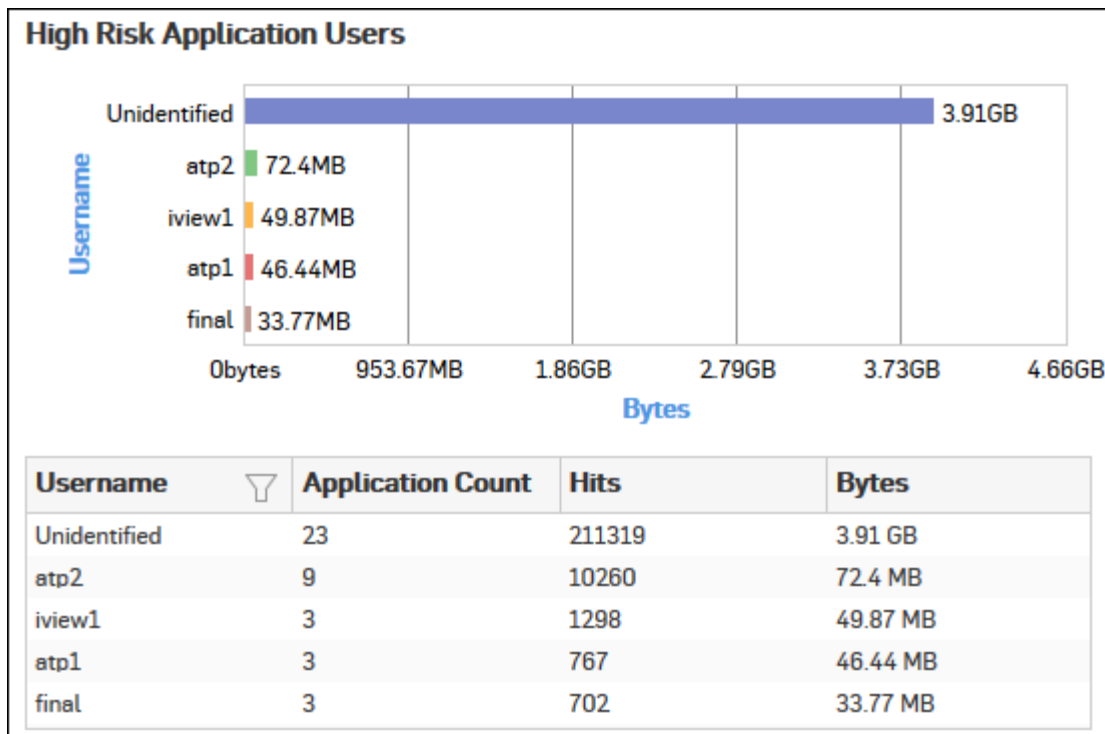


Figure 77: High Risk Application Users

Click the Username hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Hosts - High Risk Applications

This Report displays a list of Hosts accessing high risk applications (with Risk Level greater than or equal to 4), along with number of hits to the applications and total amount of data transfer by the host.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Hosts - High Risk Applications**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays amount of data transfer by each host while the tabular report contains the following information:

- Host: IP Address of the host.
- Application Count: Number of applications accessed per host.
- Hits: Number of times the application was accessed by the client.
- Bytes: Client-wise amount of data transfer through the application, in bytes.

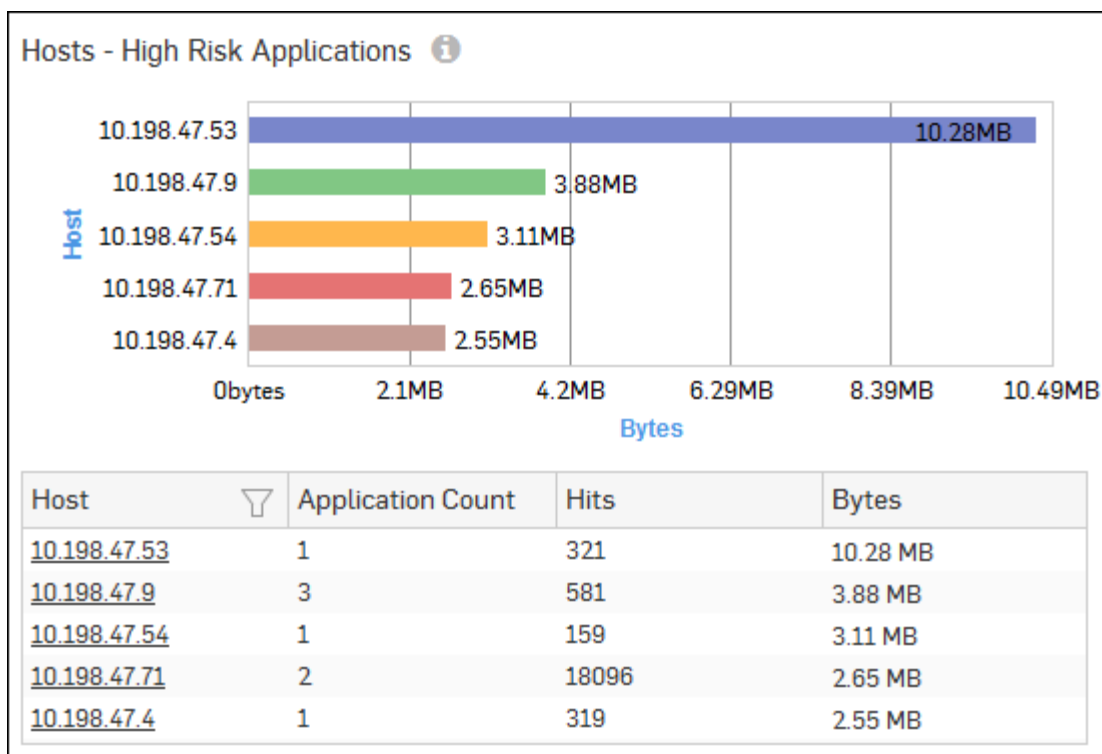


Figure 78: Hosts - High Risk Applications

Click the Host hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Hosts

This report displays a list of Hosts along with the number of hits per host and the total amount of data transfer by the host.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Hosts**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of hits while the tabular report contains the following information:

- Host: IP Address of the host.
- Hits: Number of hits per host.
- Bytes: Amount of data transfer through the host.

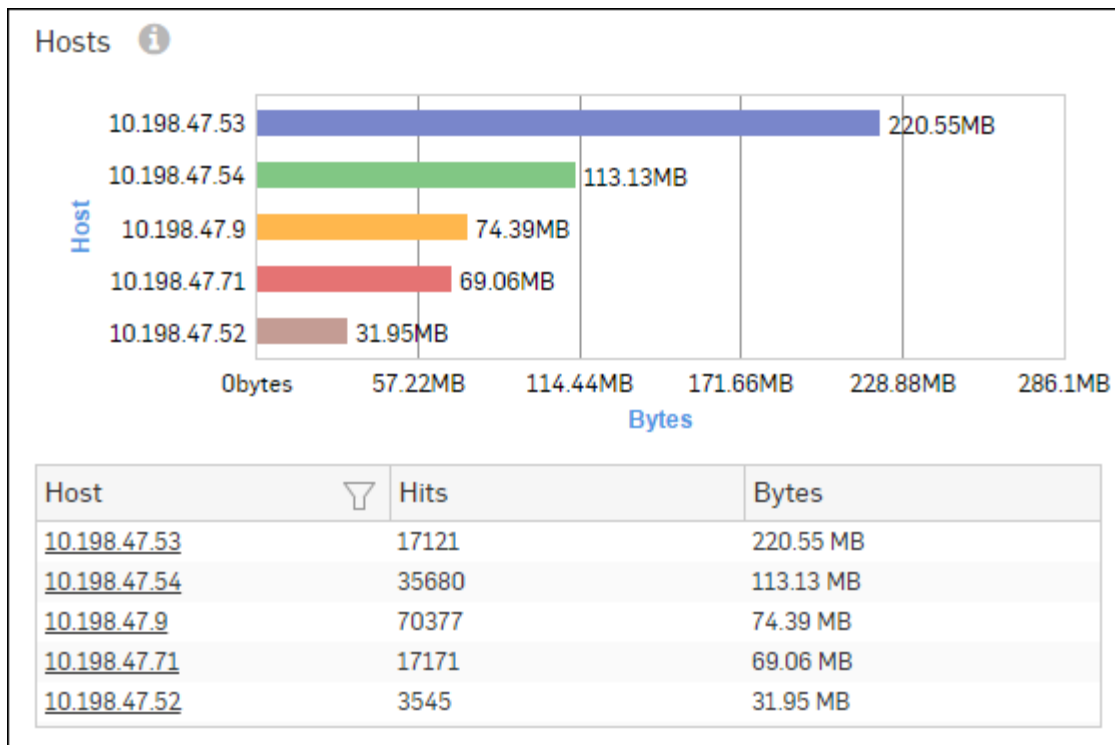


Figure 79: Hosts

Click the Host hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Source Countries

This Report displays a list of countries from where the maximum volume of Internet traffic is originated, along with number of hits and the total amount of data transfer per country.

The report is helpful when you need to identify where your web visitors are coming from. To cite a use-case scenario - you might have an e-commerce website, and would like to know the country to which your potential customers belong.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Source Countries**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of countries along with number of hits while the tabular report contains the following information:

- Source Country: Name of the source country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per country.
- Bytes: Amount of data transfer through the country, in bytes.

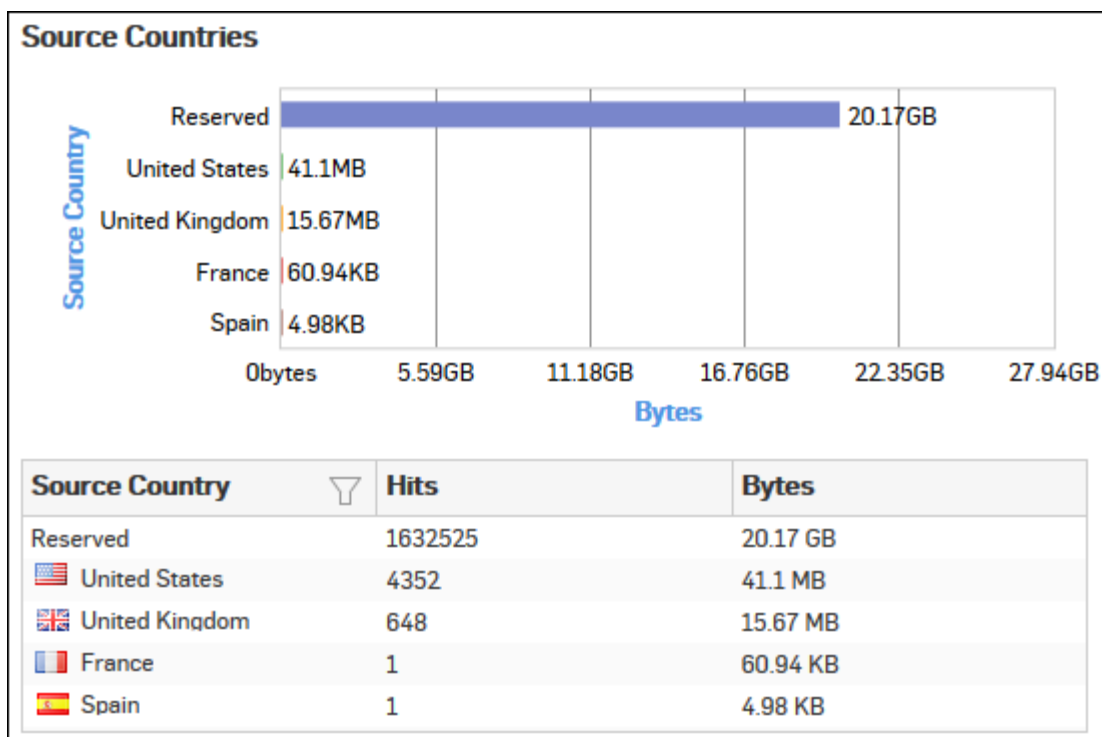


Figure 80: Source Countries

Click the Source Country hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Destination Countries

This Report displays a list of those countries which are destined to most of the Internet traffic along with number of hits and the total amount of data transfer per country.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Destination Countries**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of countries along with the number of hits while the tabular report contains the following information:

- Destination Country: Name of the destination country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per country.
- Bytes: Amount of data transfer through the country, in bytes.

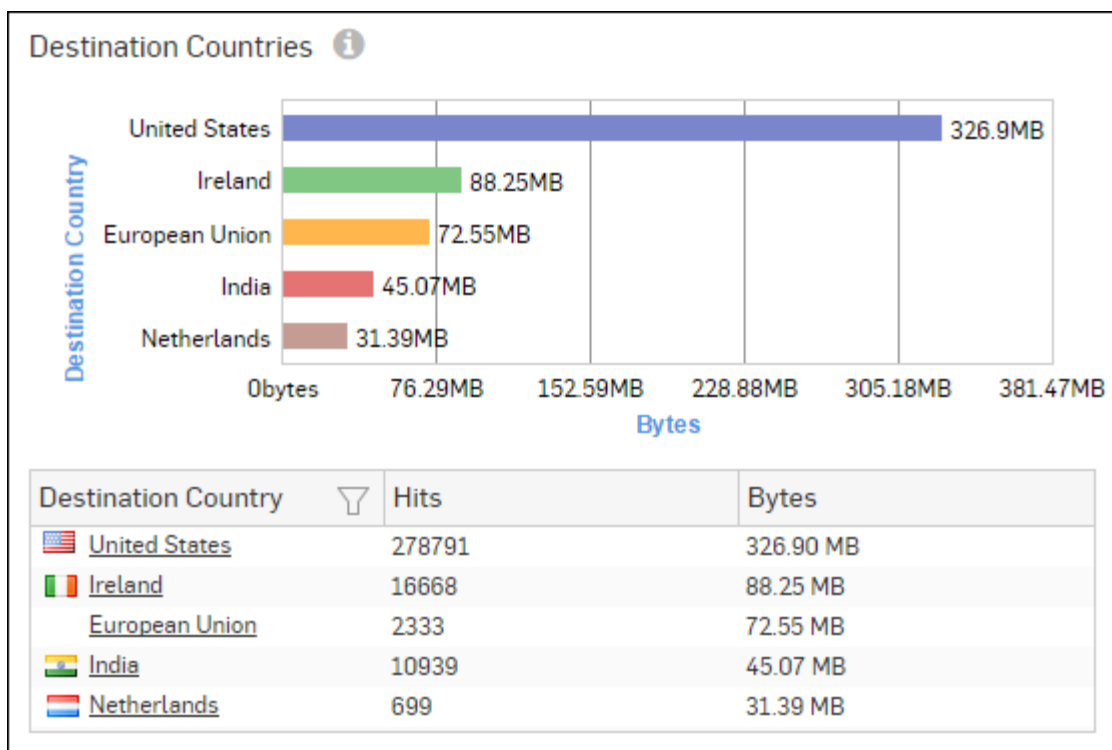


Figure 81: Destination Countries

Click the Destination Country hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Allowed Policies

This report displays a list of firewall rule ID(s) along with the number of hits per firewall rule and the total amount of data transfer through the firewall rule.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User App Risks & Usage > Allowed Policies**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of the firewall rule IDs along with the number of hits while the tabular report contains the following information:

- Policy Rule: Number displaying firewall rule ID.
- Hits: Number of hits per firewall rule.
- Bytes: Amount of data transfer through the firewall rule, in bytes.



Note: The amount of data transfer displayed in this report may not match with that shown on the Policies page.

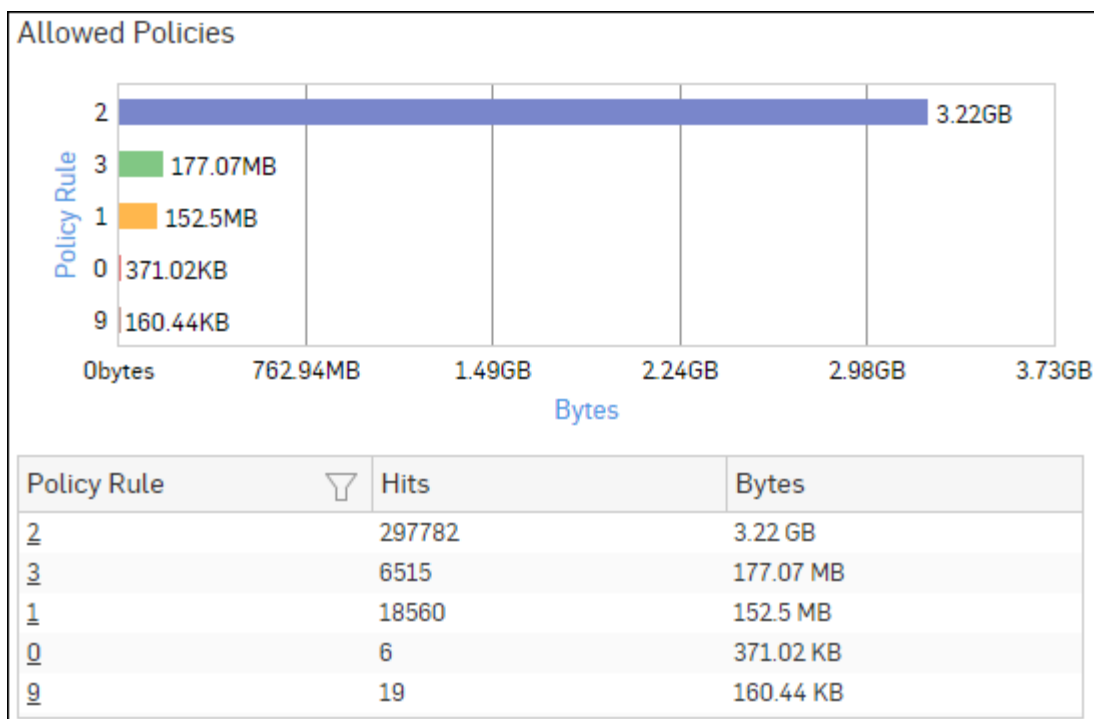


Figure 82: Allowed Policies

Click the Policy Rule hyperlink in the table or graph to view the [Filtered User App Risks & Usage Reports](#).

Filtered User App Risks & Usage Reports

The User App Risks & Usage Reports can be filtered to get the following set of reports.

- [Source Zones](#)
- [Destination Zones](#)
- [Application Categories](#)
- [Applications](#)
- [Application Users](#)
- [Application Technologies](#)
- [High Risk Applications](#)
- [Application Risk Levels](#)
- [High Risk Application Users](#)
- [Hosts - High Risk Applications](#)
- [Hosts](#)
- [Source Countries](#)
- [Destination Countries](#)
- [Allowed Policies](#)
- [Destinations](#)

To get filtered User App Risks & Usage reports, you need to choose one of the following filter criteria:

- Zone Name from [Source Zones](#) Report
- Zone Name from [Destination Zones](#) Report
- Category from [Application Categories](#) Report
- Application from [Applications](#) Report
- User from [Application Users](#) Report
- Technology from [Application Technologies](#) Report
- Application from [High Risk Applications](#) Report

- Risk from [Application Risk Levels](#) Report
- User from [High Risk Application Users](#) Report
- Host from [Hosts - High Risk Applications](#) Report
- Host from [Hosts](#) Report
- Country from [Source Countries](#) Report
- Country from [Destination Countries](#) Report
- Rule ID from [Allowed Policies](#) Report

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Source Zones widget

This widget report displays a list of Source Zones along with the number of hits and the amount of data transfer per zone.



Note: This widget will not be displayed for filter criterion Source Zone.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred per zone while the tabular report contains the following information:

- Source Zone: Name of the network zone as defined in the Device.
- Zone Type: Type of the Zone. Possible types are: LAN, WAN, DMZ, VPN and WiFi.
- Hits: Number of hits per zone.
- Bytes: Amount of data transferred.

Destination Zones widget

This widget report displays the list of destination zones along with the number of hits and the amount of data transfer per zone.



Note: This widget will not be displayed for filter criterion Destination Zone.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred per zone while the tabular report contains the following information:

- Destination Zone: Name of the network zone as defined in the Device.
- Zone Type: Type of the Zone. Possible types are: LAN, WAN, DMZ, VPN and WiFi.
- Hits: Number of hits per zone.
- Bytes: Amount of data transferred.

Application Categories widget

This widget report displays a list of Application Categories along with the number of Hits per category and total amount of data transfer using that application.



Note: This widget will not be displayed for filter criterion Application Category.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the list of application categories and the amount of data transfer while the tabular report contains the following information:

- Category: Displays name of the application category as defined in the Device.
- Hits: Number of hits per category.
- Bytes: Amount of data transfer through the application category, in bytes.

Applications widget

This widget report displays a list of the Applications along with the number of hits per application and the total amount of data transfer using that application.



Note: This widget will not be displayed for filter criterion Application.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the list of applications along with number of hits while the tabular report contains the following information:

- Application/Proto:Port: Displays the name of the application. If the application is not defined in the Device then this field displays the application identifier as combination of protocol and port number.
- Risk: Risk level associated with the application. The risk level is a numeric value. Higher value represents higher risk.
- Category: Name of application category as defined in the Device.
- Hits: Number of hits per application.
- Bytes: Amount of data transferred per application.

Application Users widget

This Widget report displays the list of network Users along with the number of hits and the amount of data transfer per user.



Note: This widget will not be displayed for filter criterion User.

The report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred per user while the tabular report contains the following information:

- User: Username of the user as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means that the traffic is generated by an unauthenticated user.
- Hits: Number of hits per user.
- Bytes: Amount of data transferred.

Application Technologies widget

This widget report displays a list of Technologies along with the number of Hits per technology and the total amount of data transfer using that technology.



Note: This widget will not be displayed for filter criterion Technology.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the list of technologies along with the number of hits while the tabular report contains the following information:

- Technology: Displays name of the technology as defined in the Device. Possible technology type: Browser Based, Client Server, Mobile, Network Protocol, P2P.
- Hits: Number of hits per technology.
- Bytes: Amount of data transfer through the technology, in bytes.

High Risk Applications widget

This widget report displays a list of Applications with Risk Level greater than equal to 4, along with number of hits and total amount of data transfer per application.



Note: This widget will not be displayed for filter criterion Application.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the list of high risk applications along with amount of data transfer per application, while the tabular report contains the following information:

- Application/Proto: Port: Name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of the protocol and port number.
- Risk: Level of risk associated with the application.
- Hits: Number of hits per application.
- Bytes: Amount of data transfer through the application, in bytes.

Application Risk Levels widget

This widget report displays a list of Risks along with the number of hits per Risk level and the total amount of data transfer using that technology.



Note: This widget will not be displayed for filter criterion Risk.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of risk levels along with amount of data transfer while the tabular report contains the following information:

- Risk: Risk associated with the application. Higher number shows higher risk.
- Hits: Number of hits per risk.
- Bytes: Amount of data transfer through the risk level, in bytes.

High Risk Application Users widget

This widget report displays a list of Users accessing high risk applications (Risk Level greater than or equal to 4), along with application count, total number of hits to the applications and total amount of data transfer by each user.



Note: This widget will not be displayed for filter criterion User.

The bar graph displays the list of users along with number of hits while the tabular report contains the following information:

- Username: Username of the user as defined in the monitored device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Application Count: Number of applications accessed per user.
- Hits: Number of hits to the high risk applications accessed by the user.
- Bytes: User-wise amount of data transfer through the high risk applications, in bytes.

Hosts - High Risk Applications widget

This widget report displays a list of Hosts accessing high risk applications (with Risk Level greater than or equal to 4), along with number of hits to the applications and total amount of data transfer by the host.



Note: This widget will not be displayed for filter criterion User.

The bar graph displays amount of data transfer by each host while the tabular report contains the following information:

- Host: IP Address of the host.
- Application Count: Number of applications accessed per host.
- Hits: Number of times the application was accessed by the client.
- Bytes: Client-wise amount of data transfer through the application, in bytes.

Hosts widget

This widget report displays the list of Hosts along with the number of hits and the amount of data transfer per host.



Note: This widget will not be displayed for filter criterion Host.

The report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred per host while the tabular report contains the following information:

- Host: IP Address of the host.
- Hits: Number of hits per host.
- Bytes: Amount of data transferred.

Source Countries widget

This widget displays a list of countries from where the maximum volume of Internet traffic is originated, along with number of hits and the total amount of data transfer per country.



Note: This widget will not be displayed for filter criterion Source Country.

The report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transfer per Source Country while the tabular report contains the following information:

- Source Country: Name of country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per country.
- Bytes: Total data transfer per source country.

Destination Countries widget

This widget report displays the list of the Destination Countries where the web traffic is directed along with a country wise distribution of the total data transfer and the number of hits.



Note: This widget will not be displayed for filter criterion Destination Country.

The report is displayed as bar graph as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transfer per destination country while the tabular report contains the following information:

- Destination Country: Name of the county. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per country.
- Bytes: Total data transfer per destination country.

Allowed Policies widget

This widget report displays a list of firewall rule IDs along with the rule-wise distribution of the total data transfer and the number of hits to those rules.



Note: This widget will not be displayed for filter criterion Rule ID.

The report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays various firewall Rule IDs and the amount of data transfer using that firewall rule while the tabular report contains the following information:

- Policy Rule: Displays firewall rule ID.
- Hits: Number of hits per firewall rule ID.
- Bytes: Amount of data transferred per firewall Rule ID.

Destinations widget

This widget report displays a list of destination IP Addresses along with number of hits and amount of data transfer per destination.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred per destination while the tabular report contains the following information:

- Destination: IP Address of the destination.
- Hits: Number of hits per destination.
- Bytes: Amount of data transferred per destination.

Blocked User Apps

The Blocked User Apps reports dashboard provides an insight into blocked attempts for accessing various applications.

View the reports dashboard from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Blocked User Apps reports dashboard consist of following reports:

- [*Blocked Application Categories*](#)
- [*Blocked Applications*](#)
- [*Blocked Technologies*](#)
- [*Blocked Application Risk Levels*](#)
- [*Blocked Application Users*](#)
- [*Blocked Hosts*](#)
- [*Blocked Source Countries*](#)
- [*Blocked Destination Countries*](#)
- [*Blocked Policies*](#)

Blocked Application Categories

This Report displays a list of top denied application categories along with number of hits per application category.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Application Categories**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied application categories along with number of hits while tabular report contains following information:

- Category: Displays name of the application category as defined in the Device.
- Hits: Number of hits per application category.

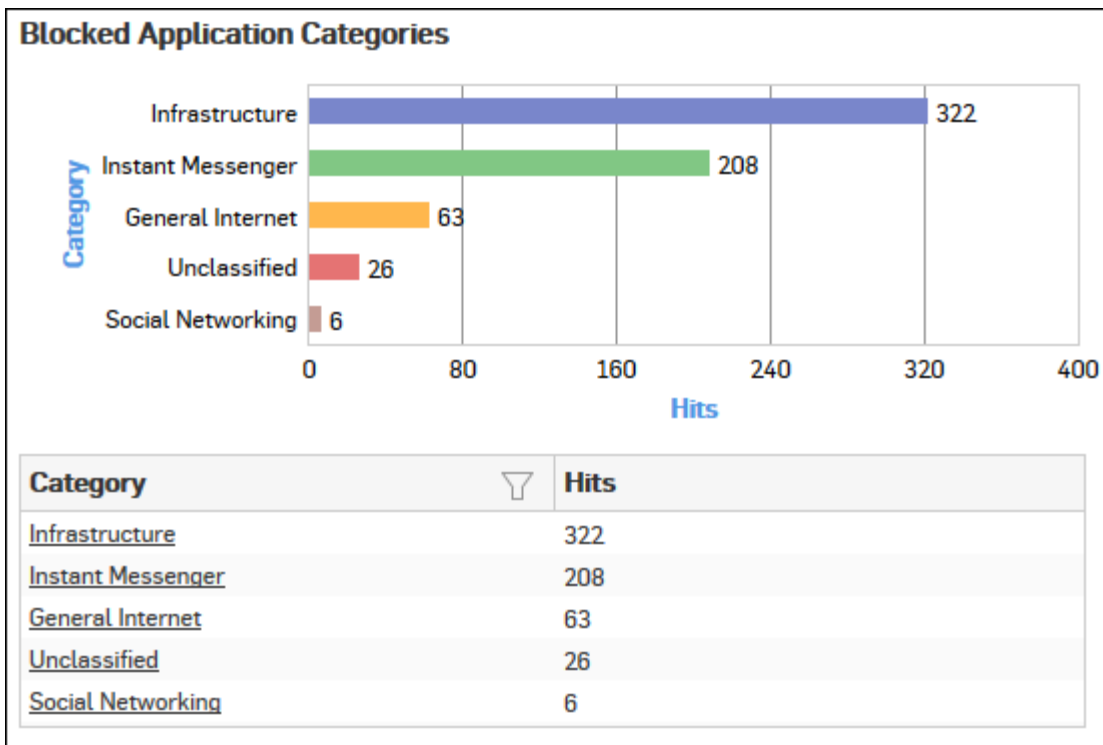


Figure 83: Blocked Application Categories

Click the Category hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Applications

This Report displays a list of top denied applications along with number of hits per application.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Applications**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied applications along with number of hits while tabular report contains following information:

- **Application/Proto: Port:** Displays name of the application as defined in the Device. If application is not defined in the Device, then this field will display application identifier as combination of protocol and port number.
- **Risk:** Displays risk level associated with the application. Higher number represents higher risk.
- **Category:** Displays name of the application category as defined in the Device.
- **Hits:** Number of hits per application category.

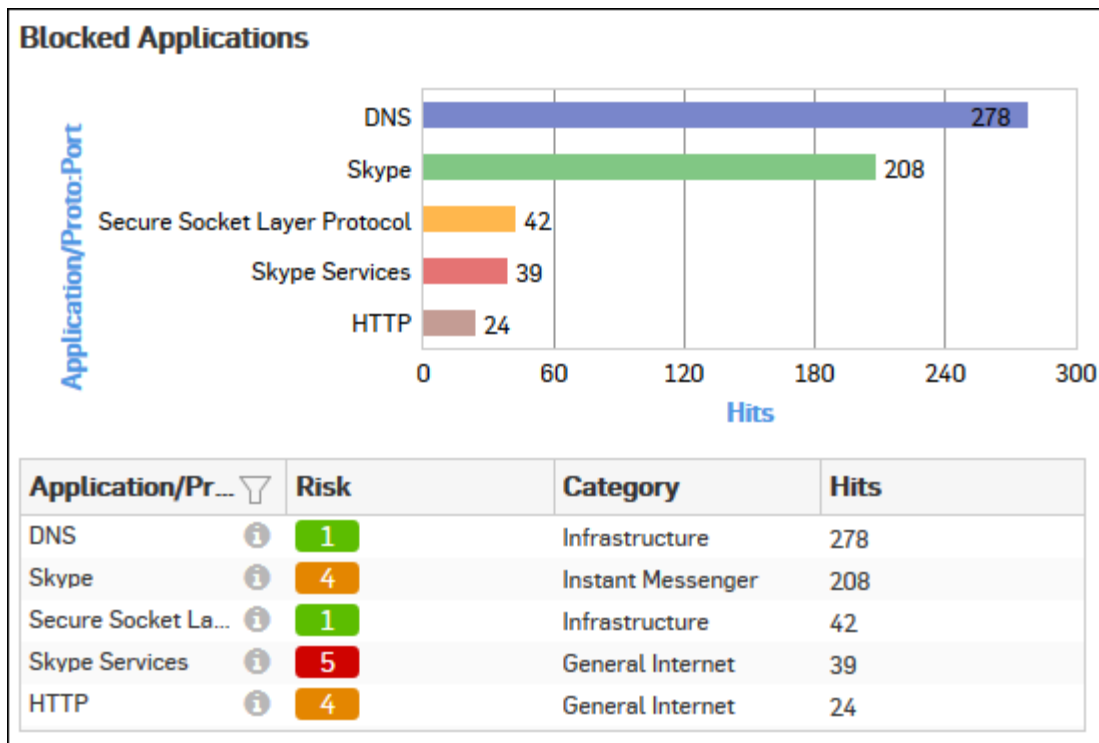


Figure 84: Blocked Applications

Click the Application hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Technologies

This Report displays a list of top denied technologies along with number of hits per technology.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Technologies**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied technologies along with number of hits while tabular report contains following information:

- Technology: Displays name of the technology as defined in the Device.
- Hits: Number of hits per technology.

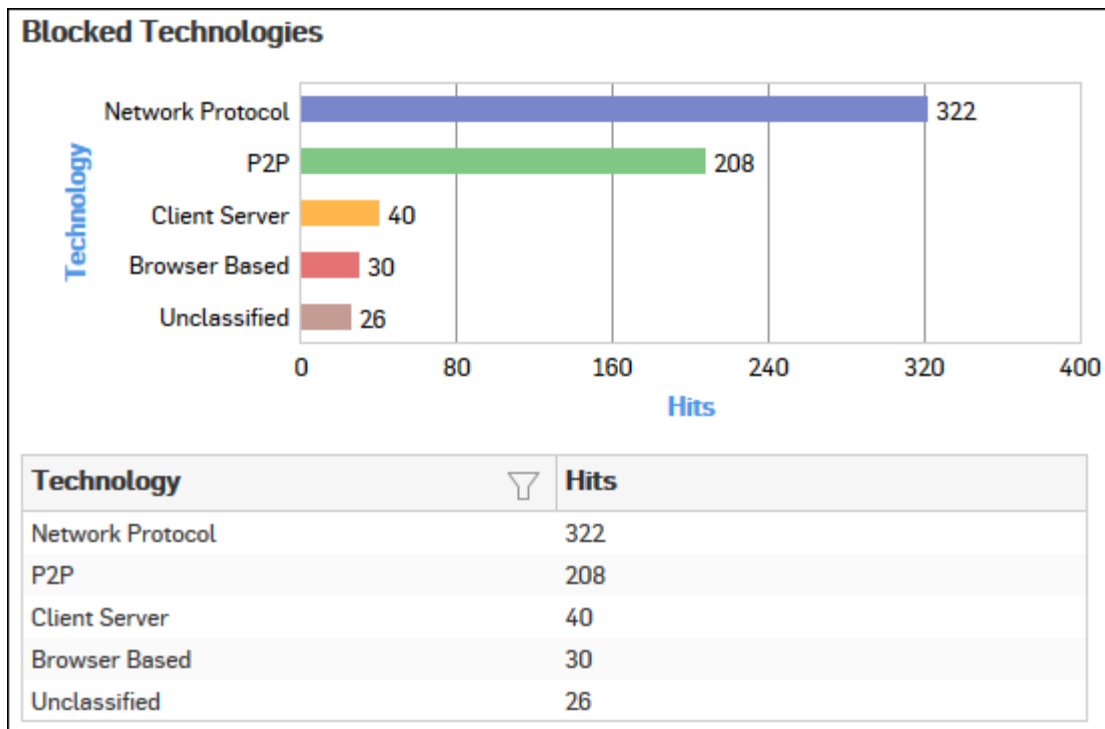


Figure 85: Blocked Technologies

Click the Technology hyperlink in table or the graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Application Risk Levels

This Report displays a list of top denied risk levels along with number of hits per risk level.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Application Risk Levels**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied risks level along with number of hits while tabular report contains following information:

- Risk: Displays risk level. Higher number displays higher risk.
- Hits: Number of hits per technology.

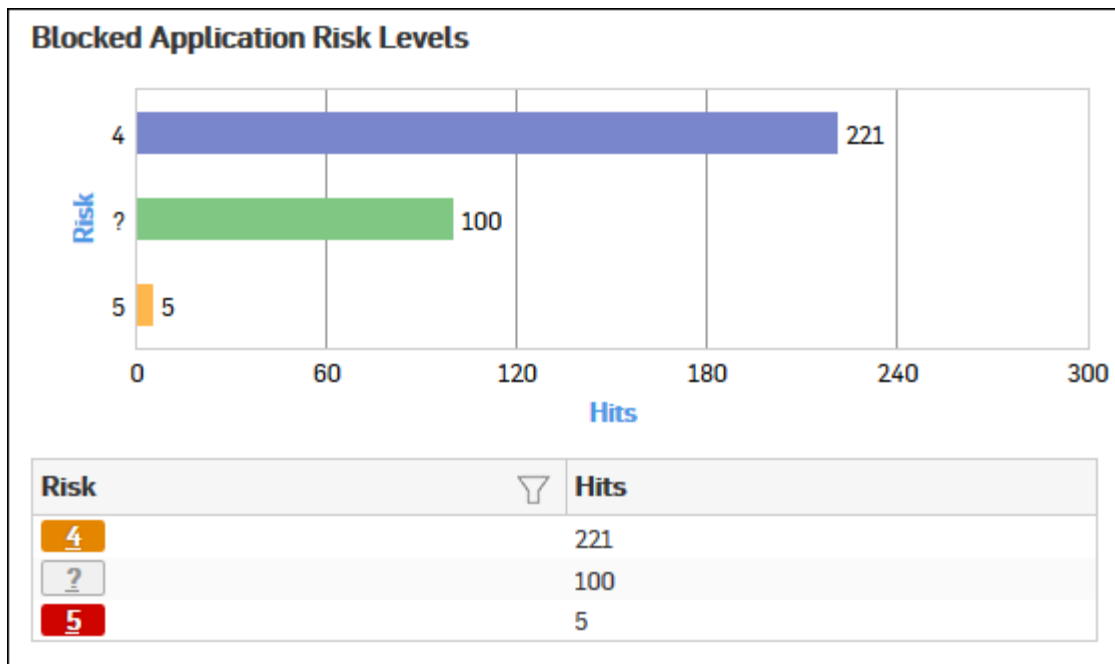


Figure 86: Blocked Applications Risk Levels

Click the Risk level hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Application Users

This Report displays a list of denied users along with number of hits per user.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Application Users**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied users along with number of hits while tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined, then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Hits: Number of hits per user.

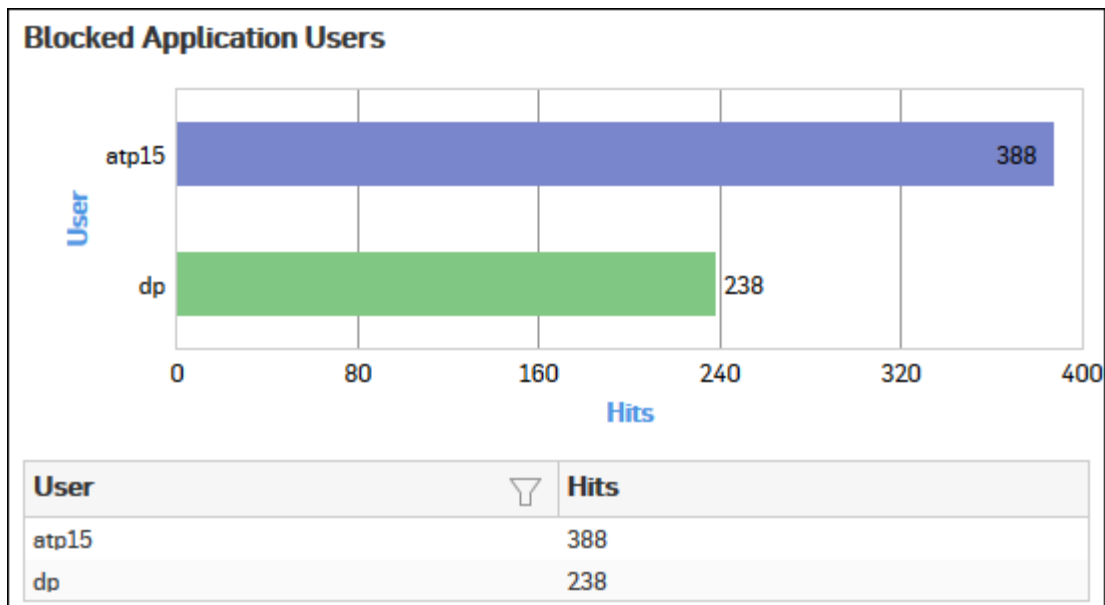


Figure 87: Blocked Application Users

Click the User hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Hosts

This Report displays a list of top denied hosts along with number of hits per host.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Hosts**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied hosts along with number of hits while tabular report contains following information:

- Host: IP Address or name of the host.
- Hits: Number of hits per host.

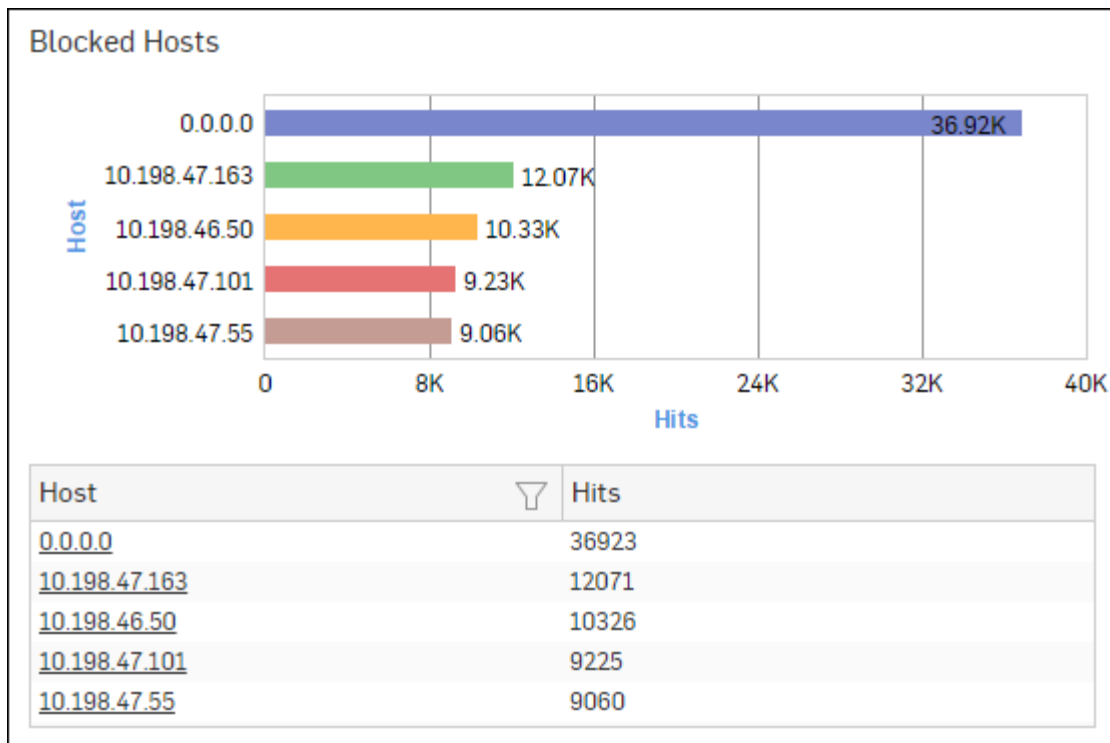


Figure 88: Blocked Hosts

Click the Host hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Source Countries

This Report displays a list of countries from where the maximum volume of Internet traffic is denied along with number of hits per country.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Source Countries**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied source Countries along with number of hits while tabular report contains following information:

- Source Country: Name of the Country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per source country.

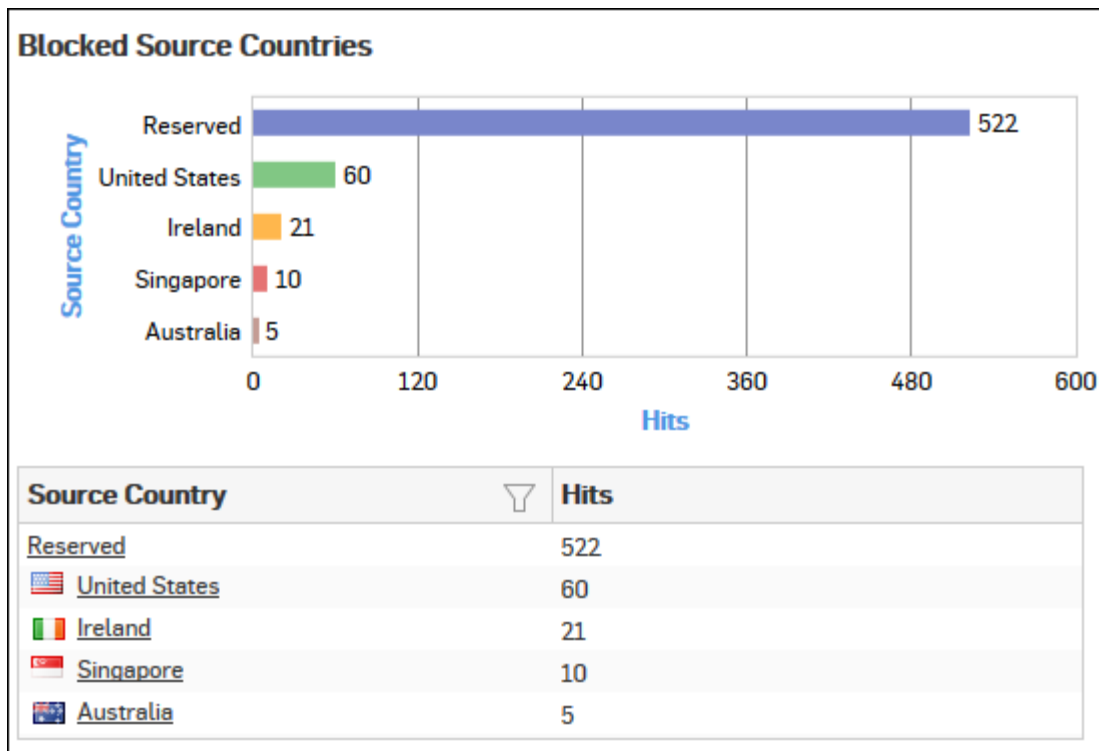


Figure 89: Blocked Source Countries

Click the Source Country hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Destination Countries

This Report displays a list of countries to where the maximum volume of Internet traffic is denied along with number of hits per country.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Destination Countries**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of denied destination countries along with number of hits while tabular report contains following information:

- Destination Country: Name of the country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per destination country.

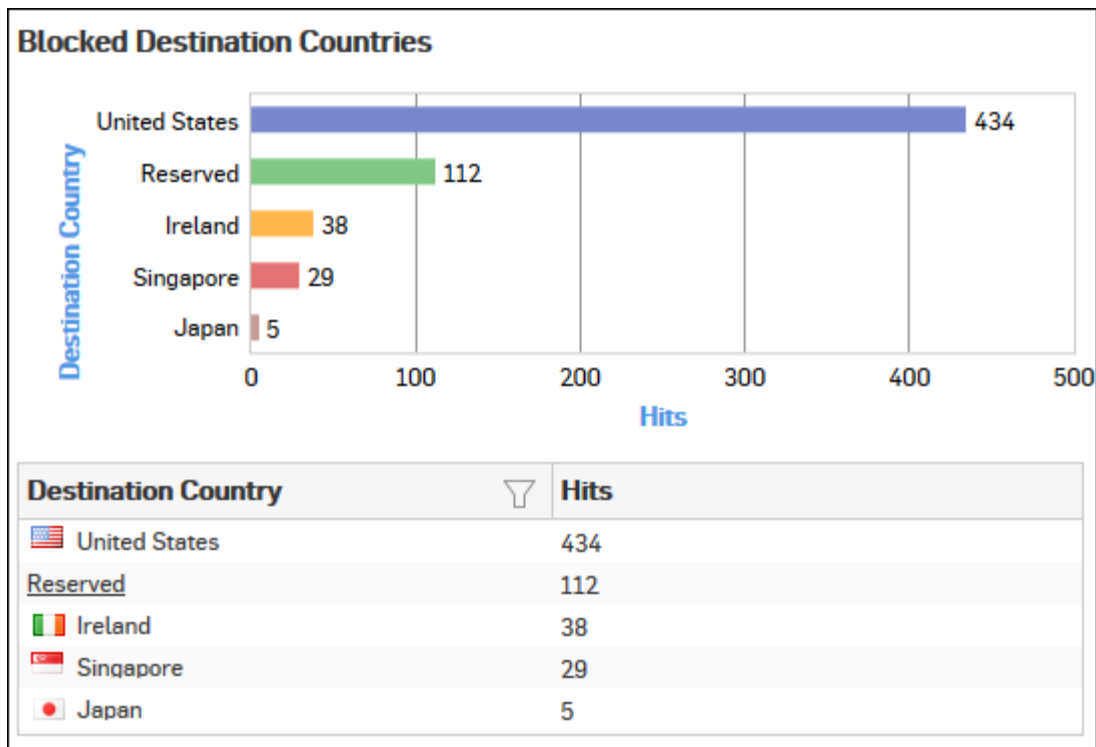


Figure 90: Blocked Destinations Countries

Click the Destination Country hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Blocked Policies

This Report displays a list of firewall rule ID along with number of hits per firewall rule.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked User Apps > Blocked Policies**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of firewall rule IDs along with number of hits while tabular report contains following information:

- Policy Rule: Number displaying firewall rule ID.
- Hits: Number of hits per firewall rule.

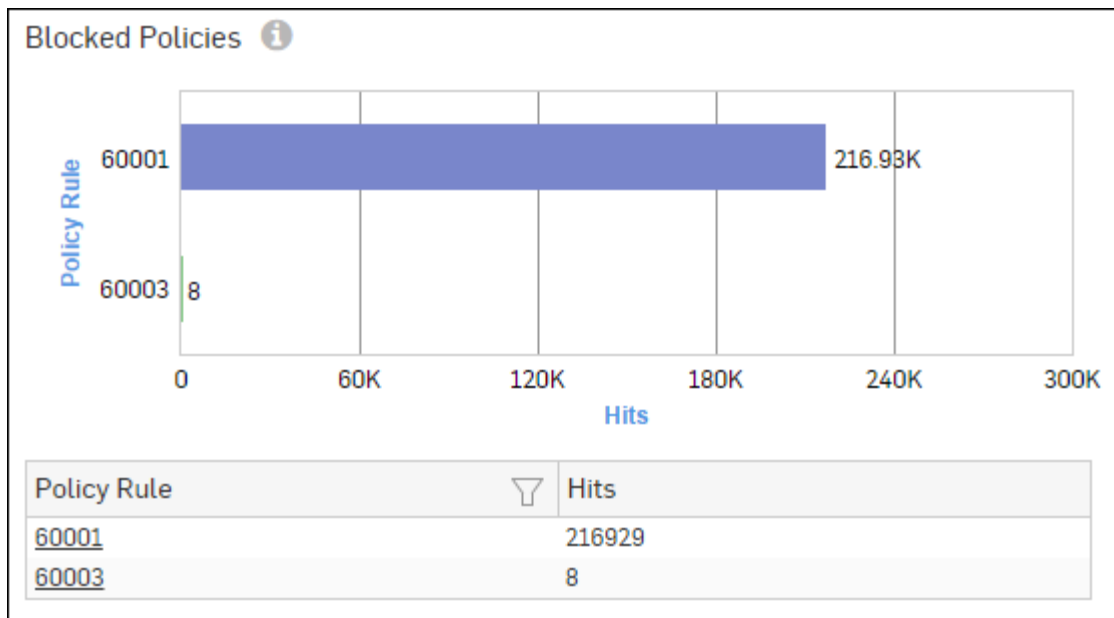


Figure 91: Blocked Policies

Click the Policy Rule hyperlink in the table or graph to view the [Filtered Blocked User Apps Reports](#).

Filtered Blocked User Apps

The Blocked User Apps Reports can be filtered to get the following set of reports:

- [Blocked Application Categories](#)
- [Blocked Applications](#)
- [Blocked Technologies](#)
- [Blocked Application Risk Levels](#)
- [Blocked Application Users](#)
- [Blocked Hosts](#)
- [Blocked Source Countries](#)
- [Blocked Destination Countries](#)
- [Blocked Policies](#)

To get filtered Blocked User Apps reports, you need to choose one of the following filter criteria:


- Category from [Blocked Application Categories](#) Report
- Application from [Blocked Applications](#) Report
- Technology from [Blocked Technologies](#) Report
- Risk Level from [Blocked Application Risk Levels](#) Report
- User from [Blocked Application Users](#) Report
- Host from [Blocked Hosts](#) Report
- Country from [Blocked Source Countries](#) Report
- Country from [Blocked Destination Countries](#) Report
- Rule ID from [Blocked Policies](#) Report

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Blocked Application Categories widget

This widget report displays a list of denied application categories along with number of hits per application category.

 **Note:** This widget will not be displayed for filter criterion Application Category.


The Report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied application categories along with number of hits while tabular report contains following information:

- Category: Displays name of the application category as defined in the Device.
- Hits: Number of hits per application category.

Blocked Applications widget

This widget report displays a list of denied applications along with number of hits per application.

 **Note:** This widget will not be displayed for filter criterion Application.


The Report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied applications along with number of hits while tabular report contains following information:

- Application/Proto: Port: Displays name of the application as defined in the Device. If application is not defined in the Device, then this field will display application identifier as combination of protocol and port number.
- Risk: Displays risk level associated with the application. Higher number represents higher risk.
- Category: Displays name of the application category as defined in the Device.
- Hits: Number of hits per application category.

Blocked Technologies widget

This widget report displays a list of denied technologies along with number of hits per technology.

 **Note:** This widget will not be displayed for filter criterion Technology.


The Report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied technologies along with number of hits while tabular report contains following information:

- Technology: Displays name of the technology as defined in the Device.
- Hits: Number of hits per technology.

Blocked Application Risk Levels widget

This widget report displays a list of denied risk levels along with number of hits per risk level.

 **Note:** This widget will not be displayed for filter criterion Risk.


The Report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied risks level along with number of hits while tabular report contains following information:

- Risk: Displays risk level. Higher number displays higher risk.
- Hits: Number of hits per technology.

Blocked Application Users widget

This widget report displays a list of denied users along with number of hits per user.

 **Note:** This widget will not be displayed for filter criterion User.

The Report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied users along with number of hits while tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined, then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Hits: Number of hits per user.

Blocked Hosts widget

This widget report displays a list of denied hosts along with number of hits per host.



Note: This widget will not be displayed for filter criterion Host.

The Report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied hosts along with number of hits while tabular report contains following information:

- Host: IP Address or host name of the host.
- Hits: Number of hits per host.

Blocked Source Countries widget

This widget displays a list of countries from where the maximum volume of Internet traffic is denied along with number of hits per country.



Note: This widget will not be displayed for filter criterion Source Country.

The Report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied source Countries along with number of hits while tabular report contains following information:

- Source Country: Name of the country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per country.

Blocked Destination Countries widget

This widget displays a list of countries to where the maximum volume of Internet traffic is denied along with number of hits per country.



Note: This widget will not be displayed for filter criterion Destination Country.

The report is displayed in the form of a bar graph as well as in a tabular format.

Bar graph displays list of denied destination countries along with number of hits while tabular report contains following information:

- Destination Country: Name of the country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits per country.

Blocked Policies widget

This widget report displays a list of firewall rule ID along with number of hits per firewall rule.



Note: This widget will not be displayed for filter criterion Rule ID.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of firewall rule IDs along with number of hits while tabular report contains following information:

- Policy Rule: Number displaying firewall rule ID.
- Hits: Number of hits per firewall rule.

Web Risks & Usage

Web Risks & Usage reports dashboard provide a snapshot of web usage through your network, in addition to associated risks.

These reports help to identify highest traffic generators who are affecting the overall network traffic. It provides statistics based on traffic generated by User Data Transfer.

The reports can help determine the Internet usage behavior and provide a basis for fine-tuning the configuration to efficiently control traffic flow.

View the reports dashboard from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage**.

Web Risks & Usage reports dashboard enables viewing of traffic generated by:

- [Web Domains](#)
- [Web Categories](#)
- [Web Category Types](#)
- [Web Users](#)
- [Web User Groups \(Primary Group\)](#)
- [Web Activity](#)
- [Objectionable Web Categories](#)
- [Objectionable Web Domains](#)
- [Objectionable Web Users](#)
- [Web Content](#)
- [Web Hosts](#)
- [Allowed Policies](#) on page 118
- [File Uploaded via Web](#)
- [Trend - Web Usage](#)
- [Warned Summary](#)

Web Domains

This Report displays list of web domains along with the number of hits and amount of data transferred per domain.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Domains**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per domain while the tabular report contains the following information:

- Domain: Domain name or IP address of the domain.
- Hits: Number of hits to the domain.
- Bytes: Amount of data transferred.

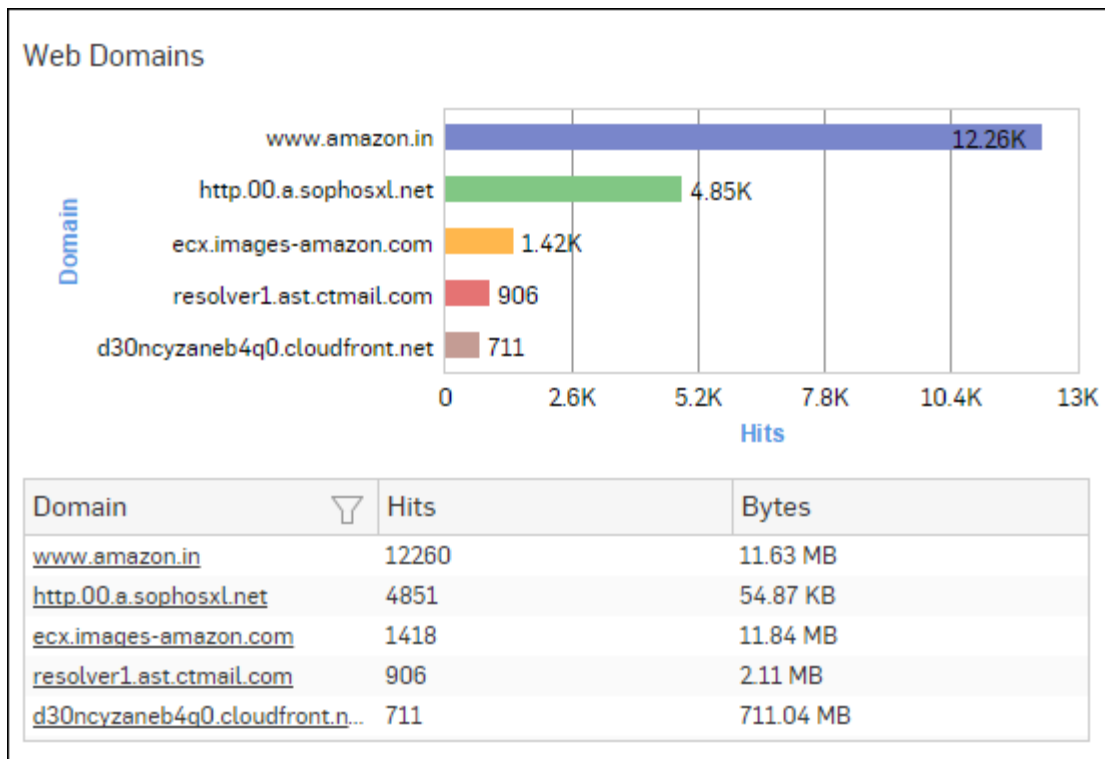


Figure 92: Web Domains

Click the Domain hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Categories

This Report displays a list of web categories along with the category type and number of hits and amount of data transferred per category.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Categories**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category while the tabular report contains the following information:

- **Category:** Displays name of the category as defined in the Device. If category is not defined in the Device then this field will display 'Uncategorized' at place of category name.
- **Category Type:** Displays name of the category type as defined in the Device. If the category type is not defined in the Device then it will display 'Uncategorized' which means the traffic is generated by an uncategorized type. By default there are four category types defined in the Device.
 - Productive
 - Unproductive
 - Acceptable
 - Objectionable
- **Hits:** Number of hits to the category.
- **Bytes:** Amount of data transferred.

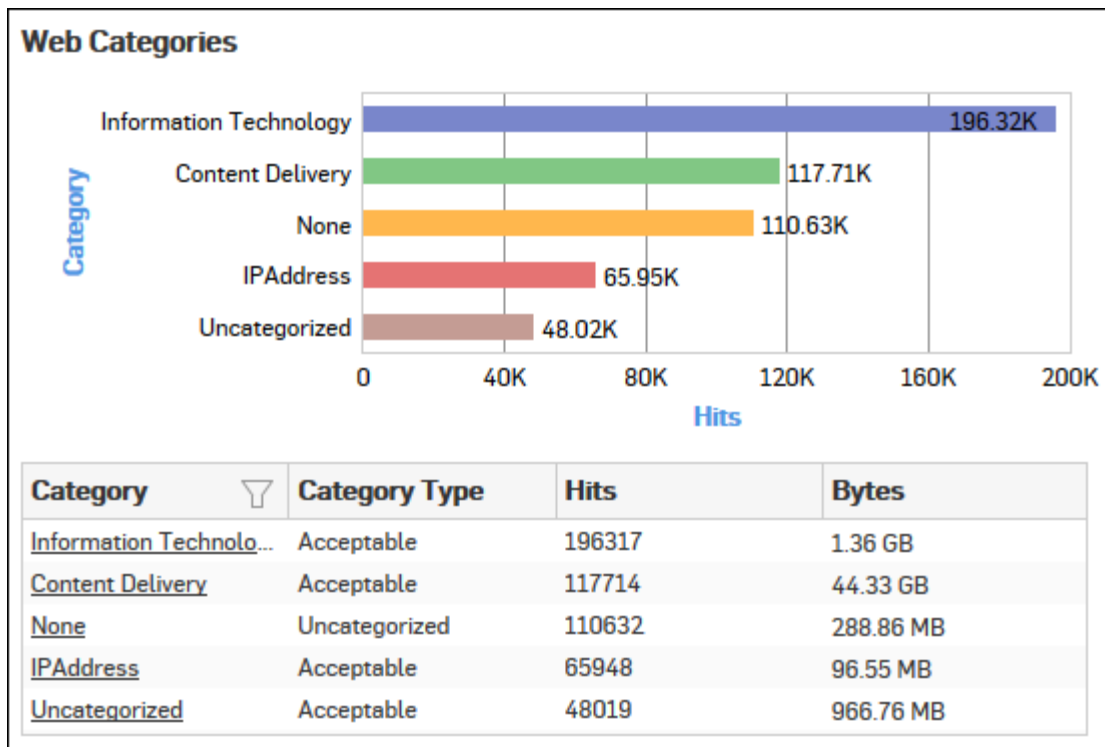


Figure 93: Web Categories

Click the Category hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Category Types

This Report displays list of Category Types along with the number of hits and amount of data transferred per category type.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Category Types**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category type while the tabular report contains the following information:

- **Category Type:** Displays name of the category type as defined in the Device. If the category type is not defined in the Device then it will display 'Uncategorized' which means the traffic is generated by an uncategorized type. By default there are four category types defined in the Device:
 - Productive
 - Acceptable
 - Unproductive
 - Objectionable
- **Hits:** Number of hits to the category type.
- **Bytes:** Amount of data transferred.

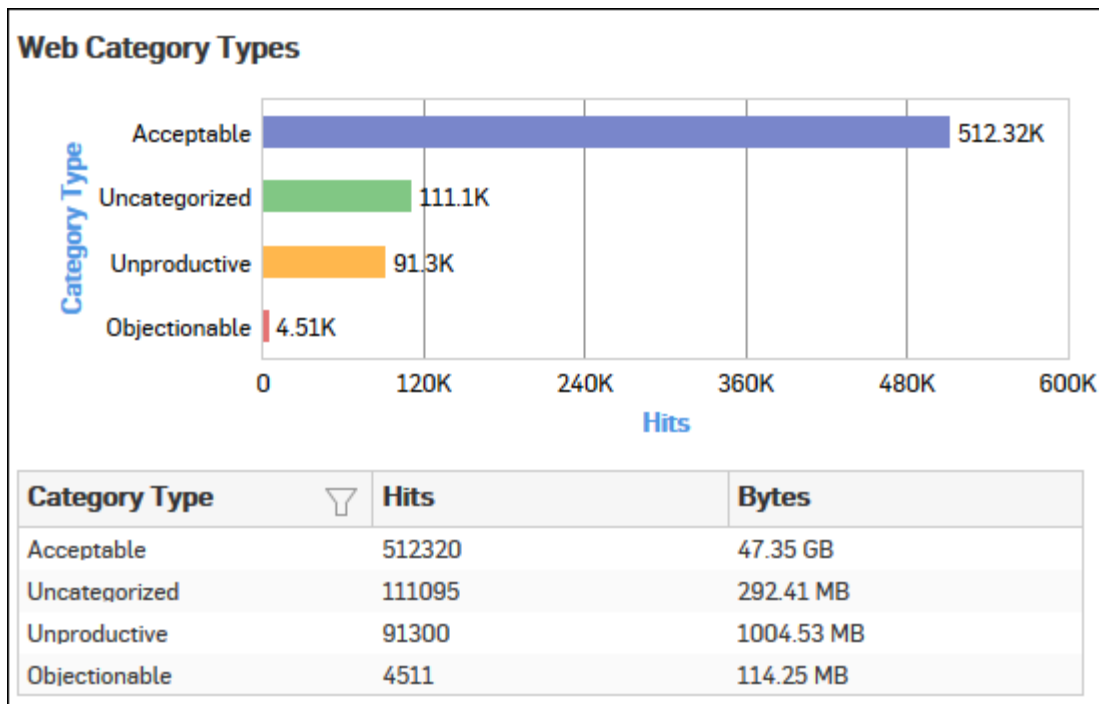


Figure 94: Web Category Types

Click the Category Type hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Users

This Report displays a list of Web Users, the group under which they are defined and number of hits & amount of data transferred per user.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Users**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per user while the tabular report contains the following information:

- User: Username of the user as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Hits: Number of hits to the user.
- Bytes: Amount of data transferred.

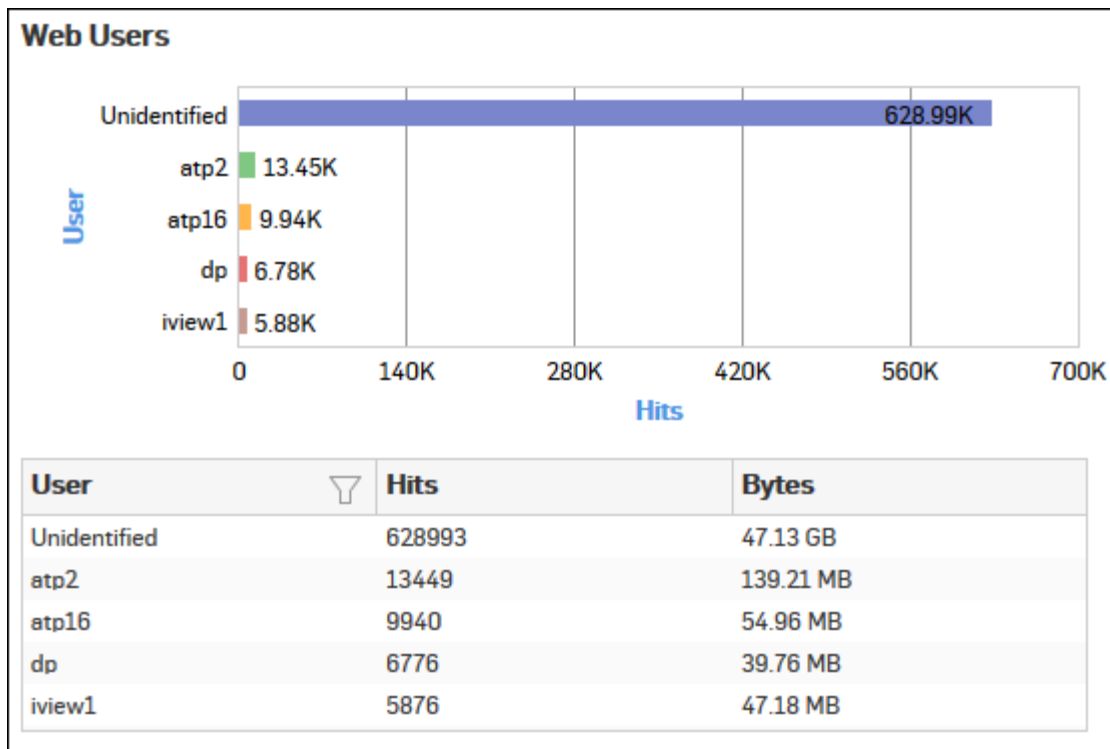


Figure 95: Web Users

Click the User hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).


Web User Groups (Primary Group)

This Report displays a list of Web User groups along with the number of hits and amount of data transferred per user group.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web User Groups (Primary Group)**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per user group while the tabular report contains the following information:

- User Group: User Group name as defined in the Device. If the User Group is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user group.
 -  **Note:** For users who are part of multiple user groups, the group shown here is the one that is at top of Objects > Identity > Groups page.
- Hits: Number of hits to the user group.
- Bytes: Amount of data transferred.

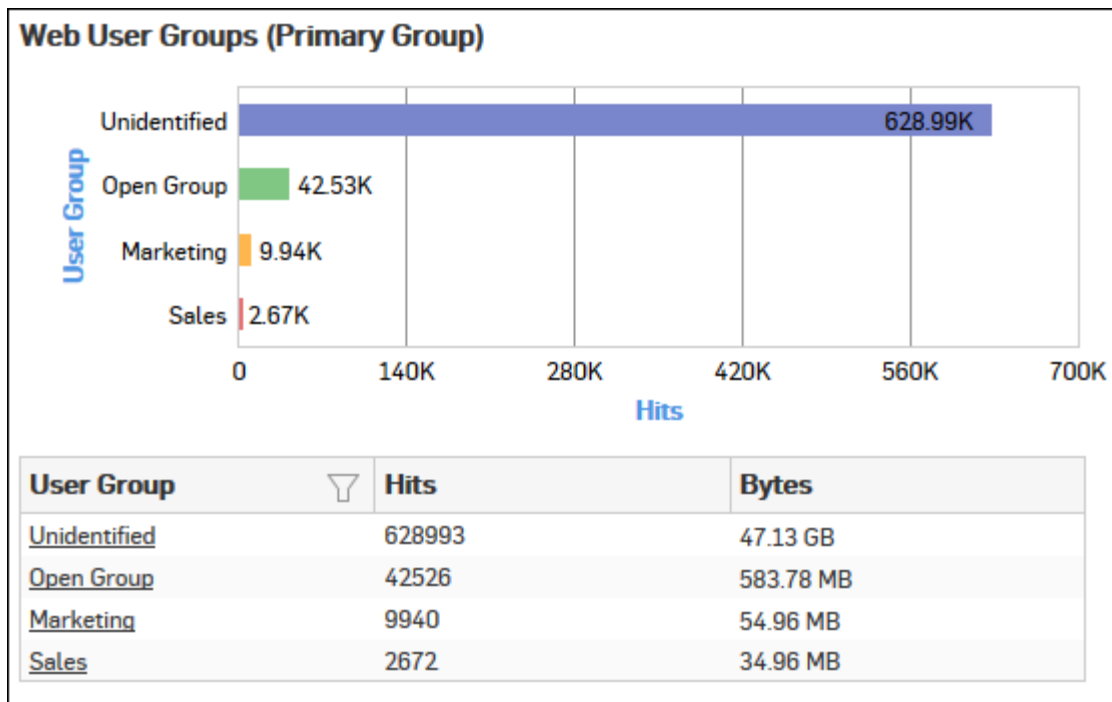


Figure 96: Web User Groups (Primary Group)

Click the User Group hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Activity

This Report displays a list of Web activities, the group under which web categories are defined along with the number of hits & amount of data transferred per activity.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Activity**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per web activity while the tabular report contains the following information:

- Activity: Displays name of the activity as defined in the Device.
- Hits: Number of hits per activity.
- Bytes: Amount of data transferred.

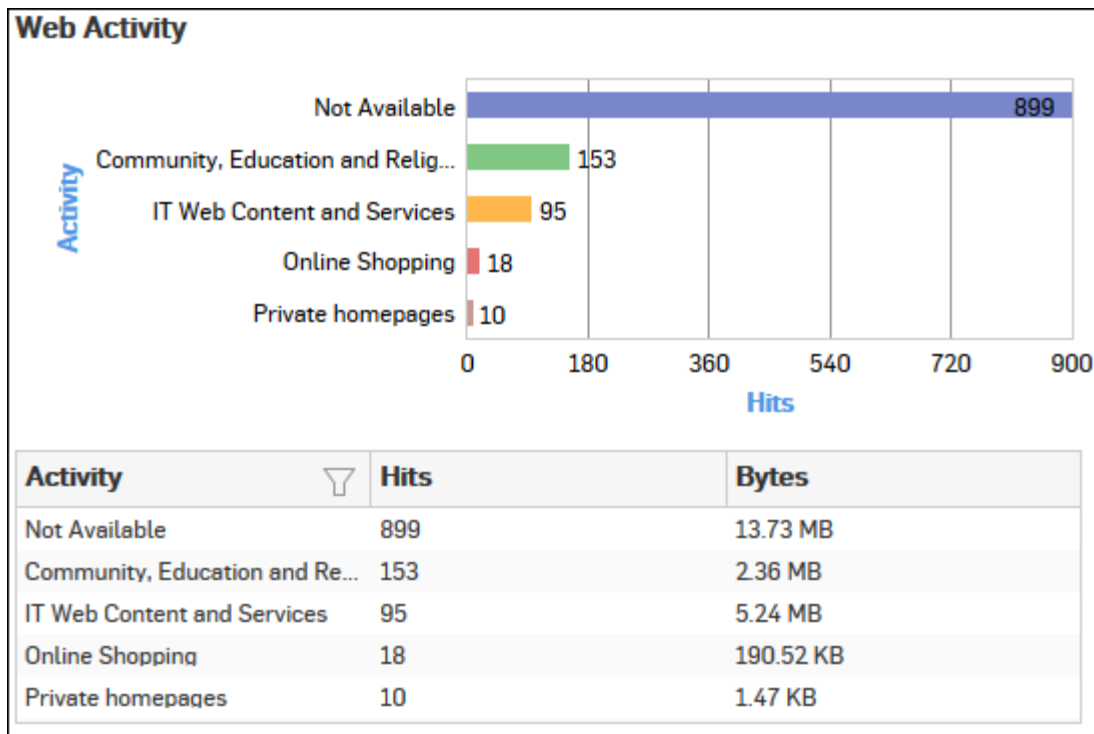


Figure 97: Web Activity

Click the Activity hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Objectionable Web Categories

This Report displays a list of Objectionable web categories accessed over the selected time period along with domain count per Objectionable category, number of hits and amount of data transferred through the category.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Categories**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Categories** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category while the tabular report contains the following information:

- Category: Displays name of the web category categorized as Objectionable in the Device.
- Domain Count: Number of domains accessed per Objectionable web category.
- Hits: Number of hits to the category.
- Bytes: Amount of data transferred.

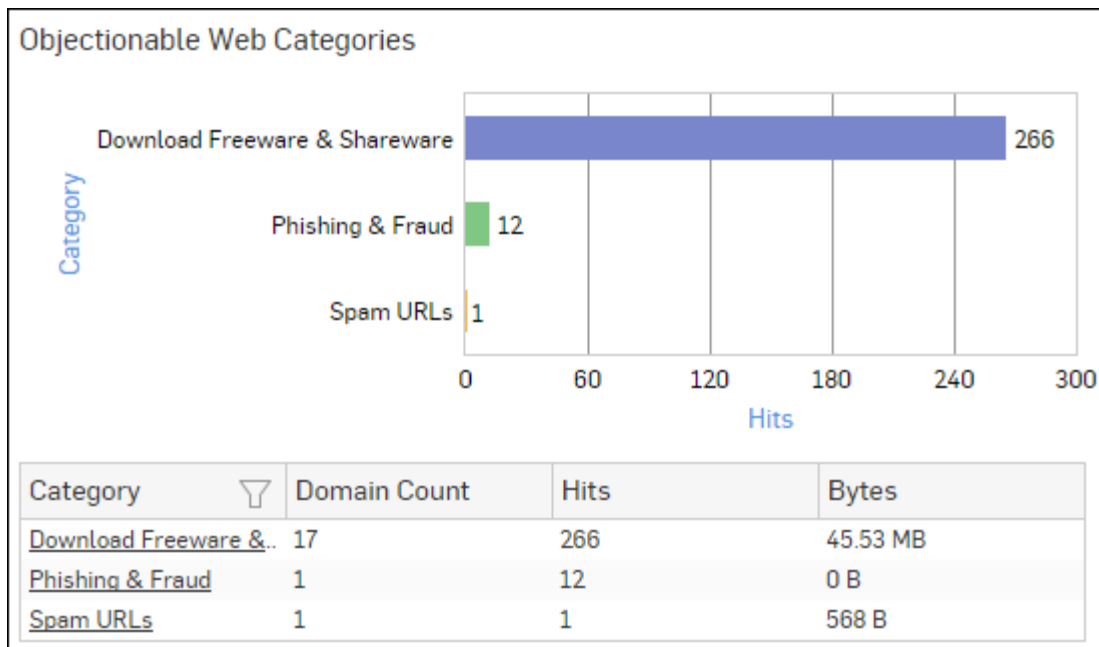


Figure 98: Objectionable Web Categories

Click the Category hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Objectionable Web Domains

This Report displays the list of Domains categorized under a Objectionable web category, along with number of hits and amount of data transferred through the domain.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Domains** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per domain while the tabular report contains the following information:

- Domain: Domain name or IP Address of the domain.
- Category: Name of the objectionable web category, under which the domain is categorized.
- Hits: Number of hits to the domain.
- Bytes: Amount of data transferred.

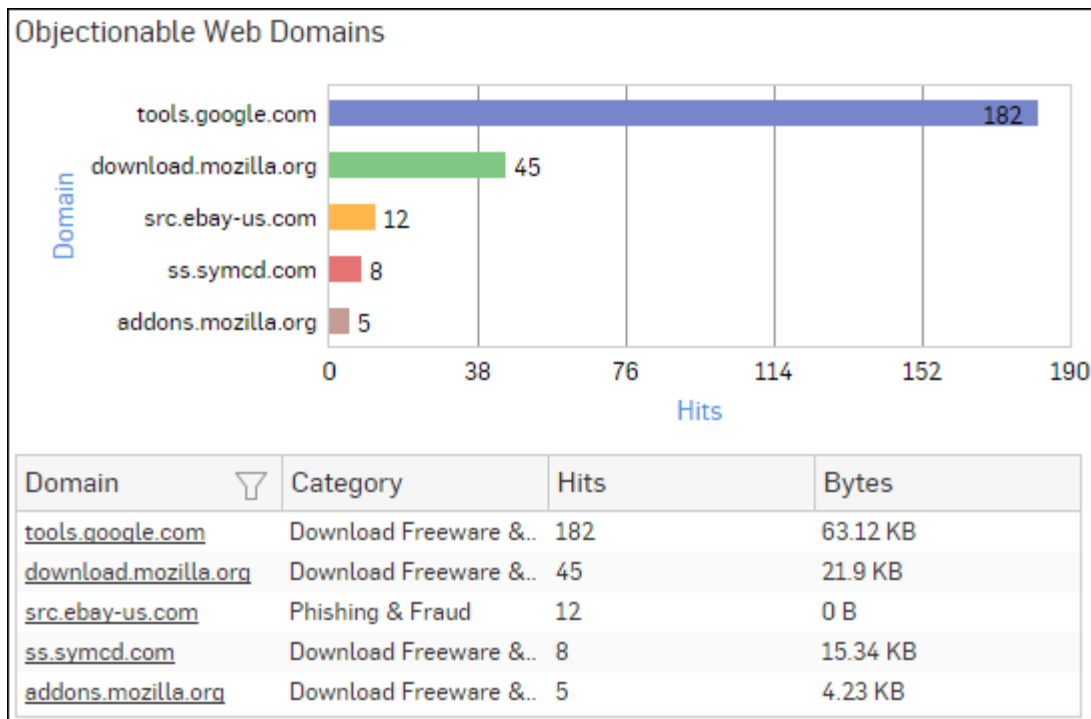


Figure 99: Objectionable Web Domains

Click the Domain hyperlink in table or graph to view the [Filtered Web Risks & Usage Reports](#).

Objectionable Web Users

This Report displays a list of Users accessing Objectionable web sites / categories along with number of times the Objectionable web site and web category was accessed and amount of data transferred per user.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Objectionable Web Users**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Objectionable Web Users** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per user, while the tabular report contains the following information:

- Username: Username of the user as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Category Count: Number of times a Objectionable web category was accessed per user.
- Domain Count: Number of times a Objectionable domain was accessed per user.
- Hits: Total number of hits to Objectionable web site and web categories.
- Bytes: Amount of data transferred per user.

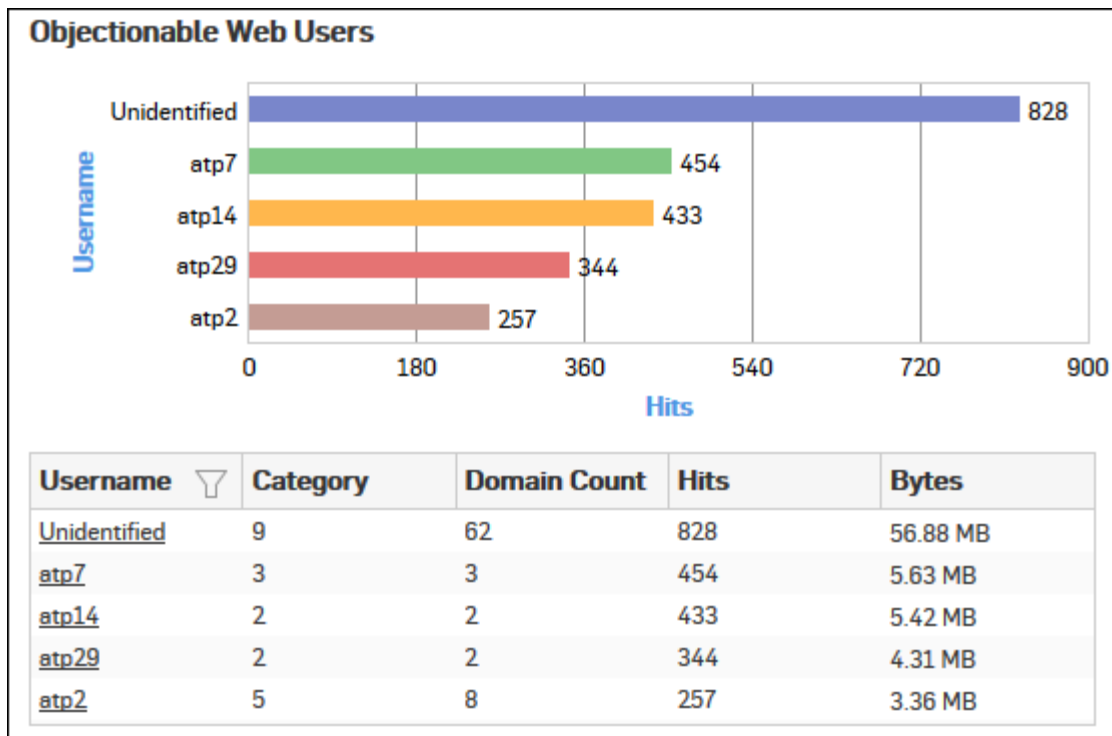


Figure 100: Objectionable Web Users

Click the Username hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Content

This Report displays the list of web content accessed over the selected time period along with number of hits and amount of data transferred per web content.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Content**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per web content while the tabular report contains the following information:

- Content: Type of the web content e.g. text, audio, video etc.
- Hits: Number of hits to the web content.
- Bytes: Amount of data transferred.

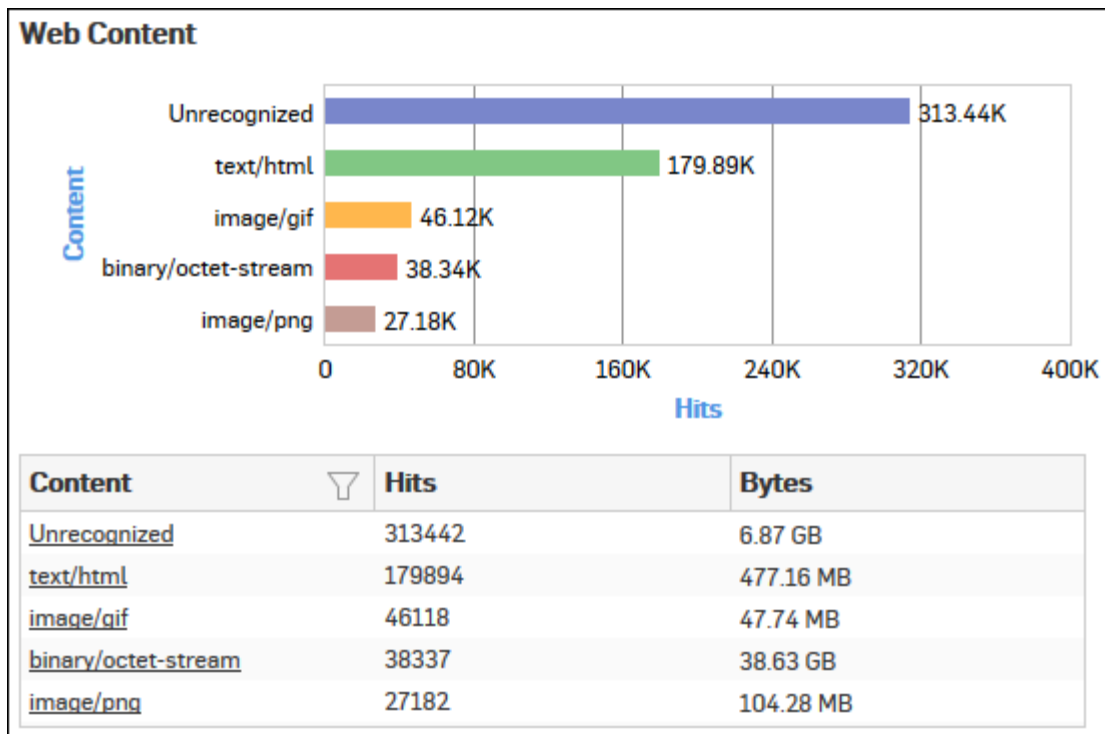


Figure 101: Web Content

Click the Content hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Web Hosts

This Report displays the list of Web Hosts along with the number of hits and amount of data transferred per host.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Web Hosts**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per web host while the tabular report contains the following information:

- Host: IP Address of the web host.
- Hits: Number of hits to the host.
- Bytes: Amount of data transferred.

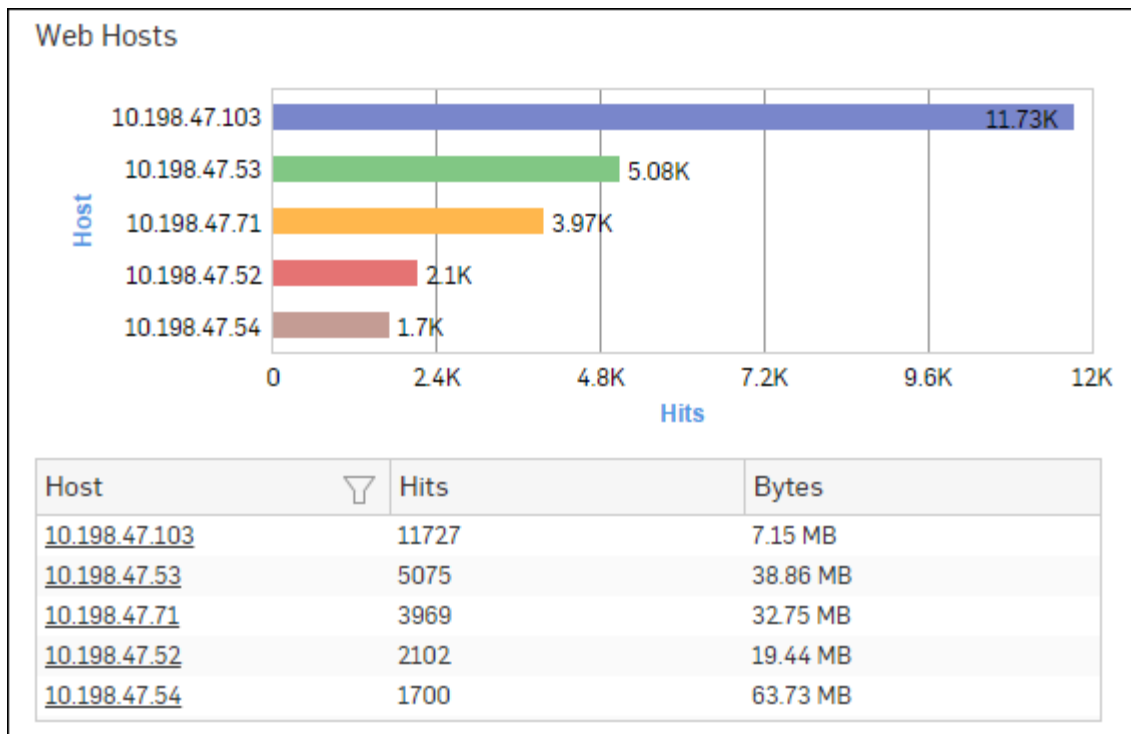


Figure 102: Web Hosts

Click the Host hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#).

Allowed Policies

This report displays a list of firewall rule ID(s) along with the number of hits per firewall rule and the total amount of data transfer through the firewall rule.

View the report from User App Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Allowed Policies**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of the firewall rule IDs along with the number of hits while the tabular report contains the following information:

- Policy Rule: Number displaying firewall rule ID.
- Hits: Number of hits per firewall rule.
- Bytes: Amount of data transfer through the firewall rule, in bytes.

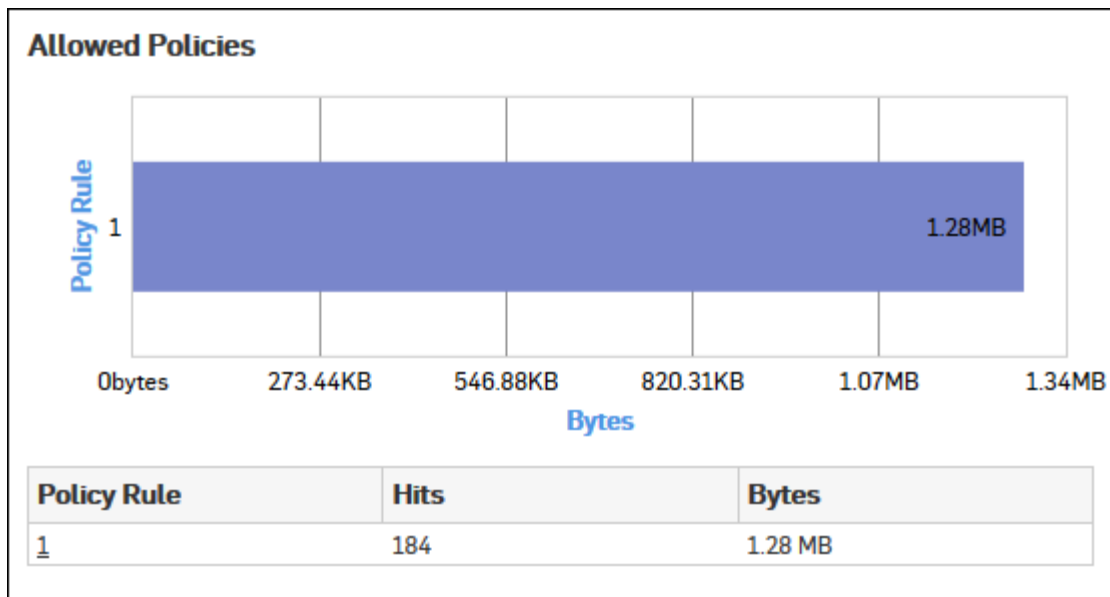


Figure 103: Allowed Policies

Click the Policy Rule hyperlink in the table or graph to view the [Filtered Web Risks & Usage Reports](#) on page 121.

File Uploaded via Web

This Report displays the list of Files Uploaded via web along with date, user, domain name, size and source from which it was uploaded.

View the report from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > File Uploaded via Web**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > File Uploaded via Web** as well.

The report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Tabular report contains the following information:

- Date: Date of file upload.
- Users: Name of the user.
- Source IP: IP Address of the source.
- Domain: Name of the domain where file has been uploaded.
- File name: Name of the file.
- Size: Size of the file.

File Uploaded via Web					
Date	Users	Source IP	Domain	File Name	Size
2015-10-31 1...	unidentified	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	unidentified	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	unidentified	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	new1	10.198.47.103	update.cyber...	update.cyber...	1002 B
2015-10-31 1...	new1	10.198.47.103	update.cyber...	update.cyber...	1002 B

Figure 104: File Uploaded via Web

Trend - Web Usage

This Report provides an overview of web usage trend based on the Internet surfing pattern of the users in your network.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Trend - Web Usage**.

The report is displayed using a graph as well as in a tabular format.

The bar graph displays mapping of web usage events with time, while the tabular report contains the following information:

- Time: Time when event occurred.
- Event Type: Type of the event.
- Event: Number of hits per event type.

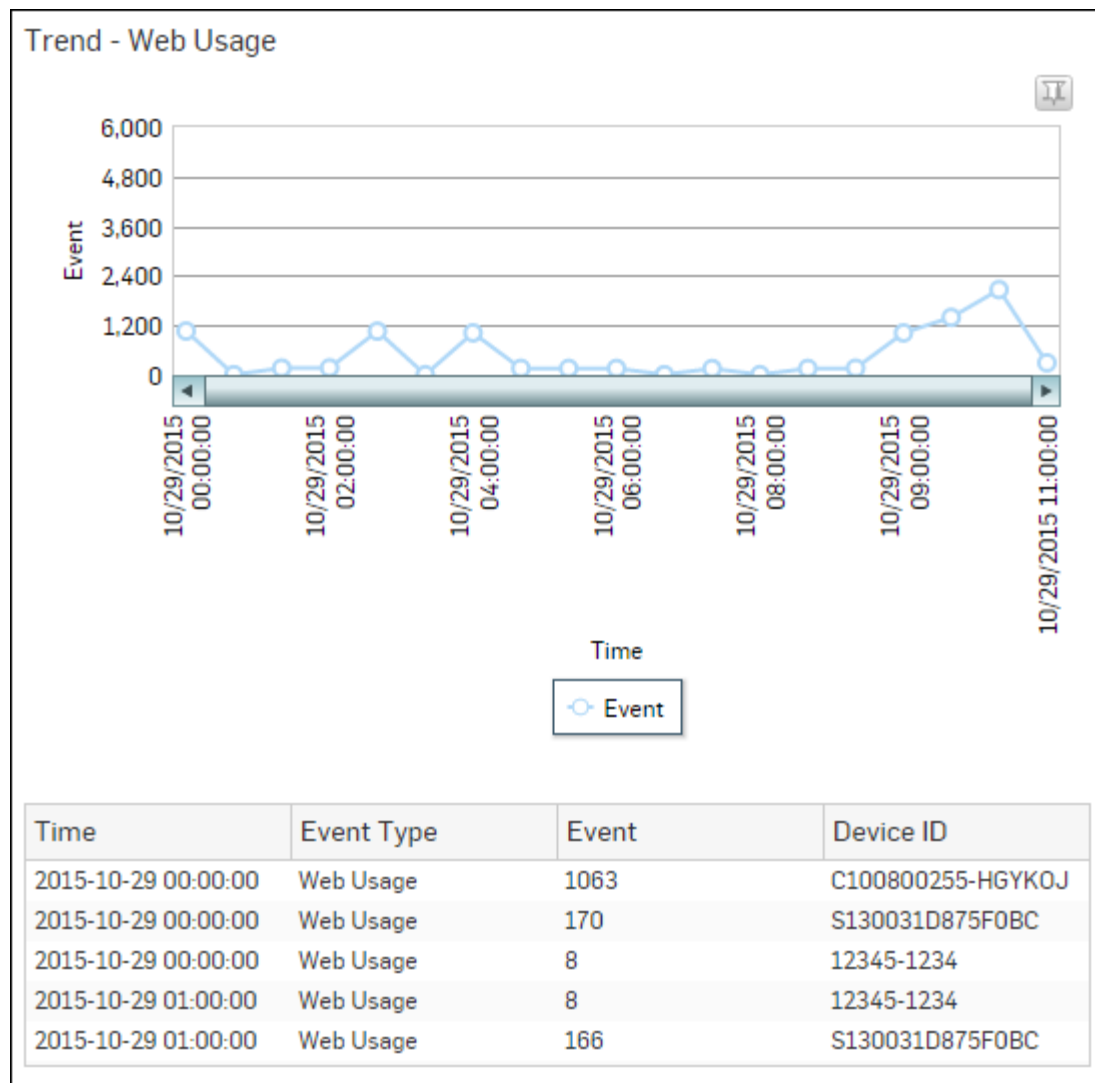


Figure 105: Trend - Web Usage

Warned Summary

This Report displays list of Traffic Types along with the number of domains and hits and amount of data transferred per traffic type.

View the reports from Web Risks & Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Risks & Usage > Warned Summary**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per traffic type while the tabular report contains the following information:

- Traffic Type: Displays type of the Traffic. By default there are three Traffic types defined in the Device:
 - Normal
 - Warned
 - Proceeded
- Domain Count: Number of domains accessed per Traffic Type.
- Hits: Number of hits to the Traffic type.
- Bytes: Amount of data transferred.

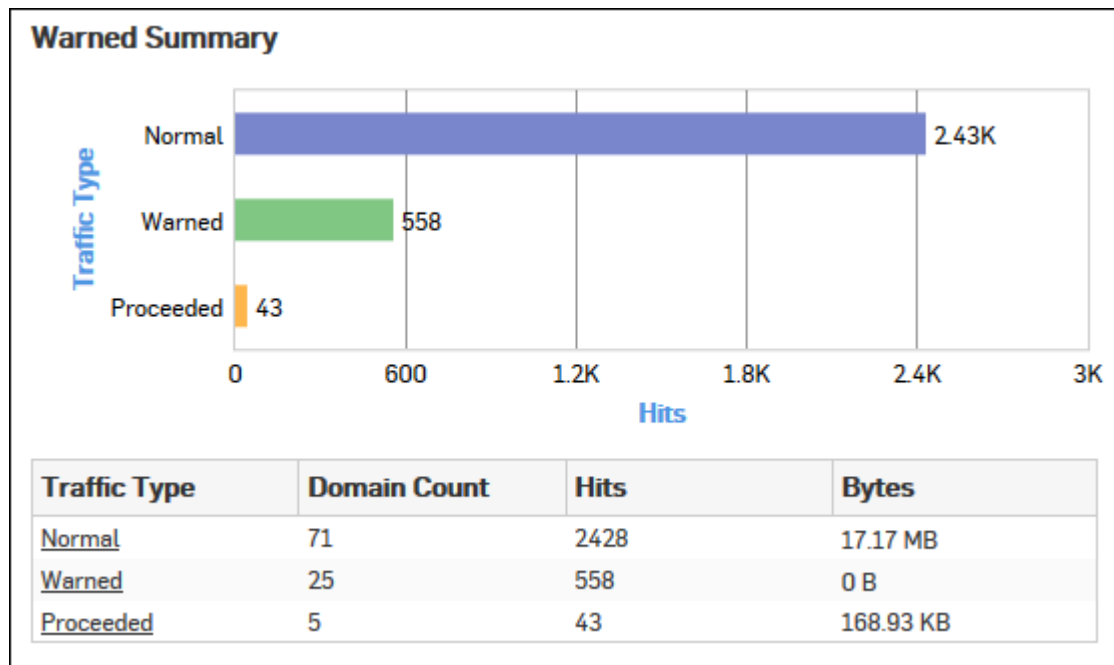


Figure 106: Warned Summary

Click the Traffic Type hyperlink in table or graph to view the [Filtered Web Risks & Usage Reports](#).

Filtered Web Risks & Usage Reports

Web Risks & Usage Reports can be filtered to get following set of reports.

- [Web Domains](#)
- [Web Categories](#)
- [Web Category Type](#)
- [Web Users](#)
- [Web User Groups \(Primary Group\)](#)
- [Web Activity](#)
- [Objectionable Web Categories](#)
- [Objectionable Web Domains](#)
- [Objectionable Web Users](#)
- [Web Content](#)
- [Web Hosts](#)
- [Web Applications](#)

To get filtered Web Risks & Usage reports, you need to choose one of the following filter criteria:

- Domain from [Web Domains](#) Report
- Category from [Web Categories](#) Report
- Category Type from [Web Category Types](#) Report
- User from [Web Users](#) Report
- User Group from [Web User Groups \(Primary Group\)](#) Report
- Activity from [Web Activity](#) Report
- Category from [Objectionable Web Categories](#) Report
- Domain from [Objectionable Web Domains](#) Report
- User from [Objectionable Web Users](#) Report
- Content from [Web Content](#) Report
- Host from [Web Hosts](#) Report

Based on the filter criterion, reports will be displayed in the following format:

- Summary - Reports in graphical format
- Details - Reports in tabular format

Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays report in a graph as well as in a tabular format which can again be filtered. Detailed Reports are displayed in a tabular format which can be filtered by clicking hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Web Domains widget

This widget Report displays the number of hits and the amount of data transferred per domain.



Note: This widget will not be displayed for filter criterion Domain.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per domain while the tabular report contains the following information:

- Domain: Domain name or IP Address of the domain.
- Hits: Number of hits to the domain.
- Bytes: Amount of data transferred.

Web Categories widget

This widget report displays the number of hits and the amount of data transferred per category.



Note: This widget will not be displayed for filter criterion Web Category.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category while the tabular report contains the following information:

- Category: Displays name of the category as defined in the Device. If category is not defined in the Device then this field will display 'Uncategorized' at place of category name.
- Category Type: Displays name of the category type as defined in the Device. If the category type is not defined in the Device then it will display 'Uncategorized' which means the traffic is generated by an uncategorized type. By default, there are four category types defined in the Device.
 - Productive
 - Unproductive

- Acceptable
- Objectionable
- Hits: Number of hits to the category.
- Bytes: Amount of data transferred.

Web Category Types widget

This widget Report displays the list of Web Category Types along with the number of hits that generate the most traffic.



Note: This widget will not be displayed for the filter criterion Web Category Type.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per web category type while the tabular report contains the following information:

- Category Type: Displays name of the category type as defined in the Device. If the category type is not defined in the Device then it will display 'Uncategorized' which means the traffic is generated by an uncategorized type. By default there are four category types defined in the Device.
 - Productive
 - Acceptable
 - Unproductive
 - Objectionable
- Hits: Number of hits to the Web category.
- Percentage: Amount of data transfer in percentage.

Web Users widget

This widget report displays the number of hits and amount of data transferred per Web user for the selected filter criterion.



Note: This widget will not be displayed for filter criterion User.

The bar graph displays number of hits per Web user group while the tabular report contains the following information:

- User: Username of the user as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Hits: Number of hits to the user.
- Bytes: Amount of data transferred.

Web User Groups (Primary Group) widget

This widget report displays the number of hits and the amount of data transferred per Web User Group.



Note: This widget will not be displayed for filter criterion User Group.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per Web user group while the tabular report contains the following information:

- User Group: User group name as defined in the Device.



Note: For users who are part of multiple user groups, the group shown here is the one that is at the top of **Objects > Identity > Groups** page.

- Hits: Number of hits to the category.

- Bytes: Amount of data transferred.

Web Activity widget

This widget report displays the number of hits and the amount of data transferred per activity.



Note: This widget will not be displayed for filter criterion Web Activity.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per web activity while the tabular report contains the following information:

- Activity: Displays name of the activity as defined in the Device. If activity is not defined in the Device then this field will display 'Not Available' at place of activity name.
- Hits: Number of hits per activity.
- Bytes: Amount of data transferred.

Objectionable Web Categories widget

This widget displays a list of Objectionable web categories accessed over the selected time period along with domain count per Objectionable category, number of hits and amount of data transferred through the category.



Note: This widget will not be displayed for filter criterion Category.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per category while the tabular report contains the following information:

- Category: Displays name of the web category categorized as Objectionable in the Device.
- Domain Count: Number of domains accessed per objectionable web category.
- Hits: Number of hits to the category.
- Bytes: Amount of data transferred.

Objectionable Web Domains widget

This widget displays the list of Domains categorized under a Objectionable web category, along with number of hits and amount of data transferred through the domain.



Note: This widget will not be displayed for filter criterion Domain.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per domain, while the tabular report contains the following information:

- Username: Username of the user as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Domain: Name of the domain falling under objectionable web category.
- Category: Name of the Objectionable web category.
- Hits: User-wise number of hits to the domains falling under Objectionable web category.
- Bytes: Amount of data transferred.

Objectionable Web Users widget

This widget displays a list of Users accessing Objectionable web sites / categories along with number of times the Objectionable web site and web category was accessed and amount of data transferred per user.



Note: This widget will not be displayed for filter criterion Category.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per user, while the tabular report contains the following information:

- Username: Username of the user as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Category: Name of the objectionable web category.
- Domain Count: User-wise number of domains accessed per objectionable web category.
- Hits: User-wise number of hits to the objectionable web category.
- Bytes: Amount of data transferred.

Web Content widget

This widget Report displays the Content Types along with number of bytes and the percentage of traffic.



Note: This widget will not be displayed for filter criterion Content.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per web content while the tabular report contains the following information:

- Content: Type of web content. Examples of possible content types are text, image, application etc.
- Hits: Number of hits to the web content.
- Bytes: Amount of data transferred.

Web Hosts widget

This widget displays the list of Web Hosts along with the number of hits and amount of data transferred per host.



Note: This widget will not be displayed for filter criterion Host.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of hits per web host, while the tabular report contains the following information:

- Host: IP Address of the host.
- Hits: Number of hits to the host.
- Bytes: Amount of data transferred.

Allowed Policies widget

This widget report displays a list of firewall rule IDs along with the rule-wise distribution of the total data transfer and the number of hits to those rules.



Note: This widget will not be displayed for filter criterion Rule ID.

The report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays various firewall Rule IDs and the amount of data transfer using that firewall rule while the tabular report contains the following information:

- Policy Rule: Displays firewall rule ID.
- Hits: Number of hits per firewall rule ID.
- Bytes: Amount of data transferred per firewall Rule ID.

Web Applications widget

This widget displays the list of web applications along with number of hits and amount of data transferred per application.

The bar graph displays web applications along with number of hits and amount of data transferred per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the web application.
- Hits: Number of hits per web application.
- Bytes: Amount of data transferred per application.

Blocked Web Attempts

Blocked Web Attempts reports dashboard provides an insight about the unsuccessful attempts made by users to access blocked sites.

View Blocked Web Attempts reports dashboard from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts**.

The Reports are displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Blocked Web Attempts reports dashboard enable to view traffic generated by:

- [Blocked Web Users](#)
- [Blocked Web Categories](#)
- [Blocked Web Domains](#)
- [Blocked Web Hosts](#)
- [Blocked Allowable Categories](#)
- [Blocked Allowable Domains](#)
- [Blocked Policies](#) on page 132
- [Blocked Web Activity](#)
- [Trend - Blocked Web Attempts](#)
- [Web Virus](#)
- [Domains - Web Virus](#)
- [Users - Web Virus](#)
- [Hosts - Web Virus](#)
- [Trend - Web Virus](#)

Blocked Web Users

This Report displays a list of Users who made the most attempts to access blocked sites.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Users**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Users** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of blocked users along with number of hits per user while the tabular report contains the following information:

- User: Name of the User as defined in the Device.
- Hits: Number of Hits.

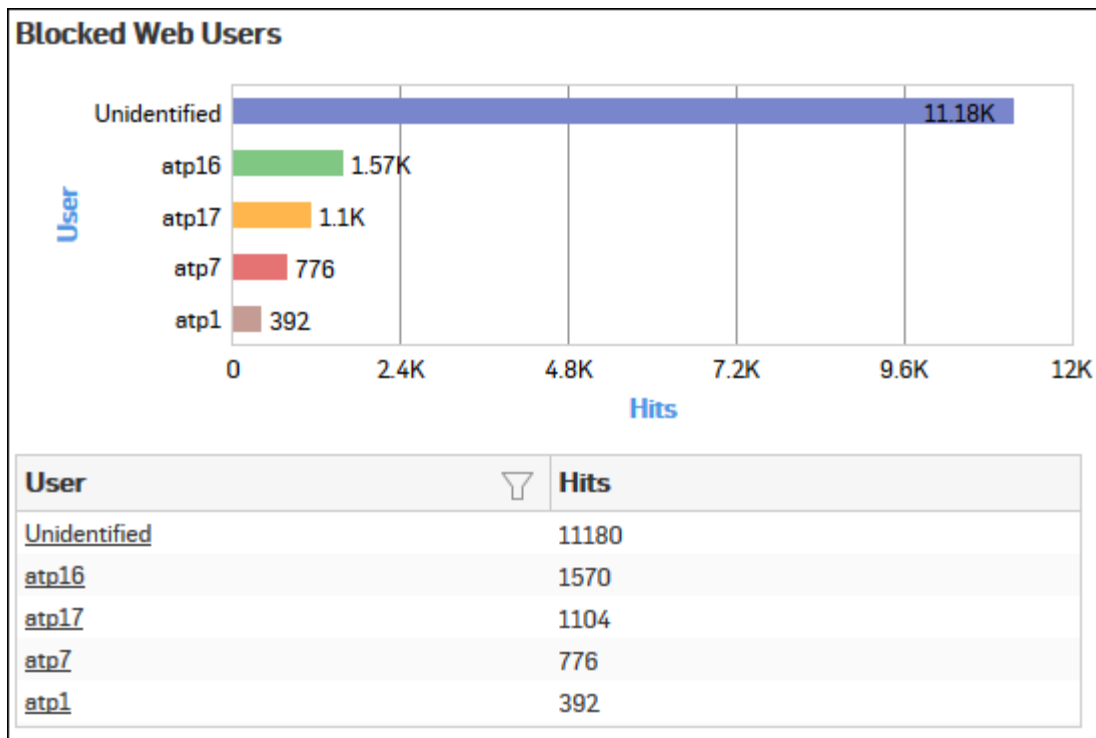


Figure 107: Blocked Web Users

Click the User hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Blocked Web Categories

This Report displays a list of blocked web categories that various users tried to access and the number of access attempts to each category.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Categories**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Categories** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of categories along with number of hits per category while the tabular report contains the following information:

- Category: Name of the category.
- Hits: Number of hits per category.

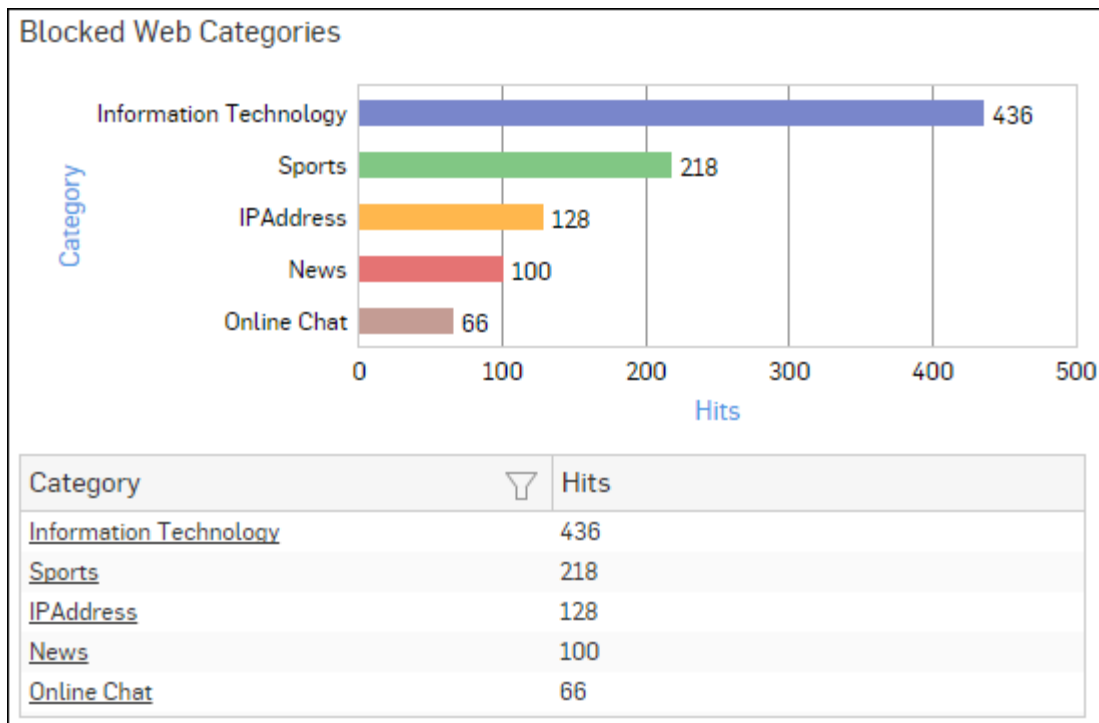


Figure 108: Blocked Web Categories

Click the Category hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Blocked Web Domains

This Report displays the list of blocked web domains that various users tried to access and the number of access attempts to each domain.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Domains** as well.

The Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of domains along with number of hits per domain while tabular report contains the following information:

- Domain: Name of the domain.
- Hits: Number of Hits.

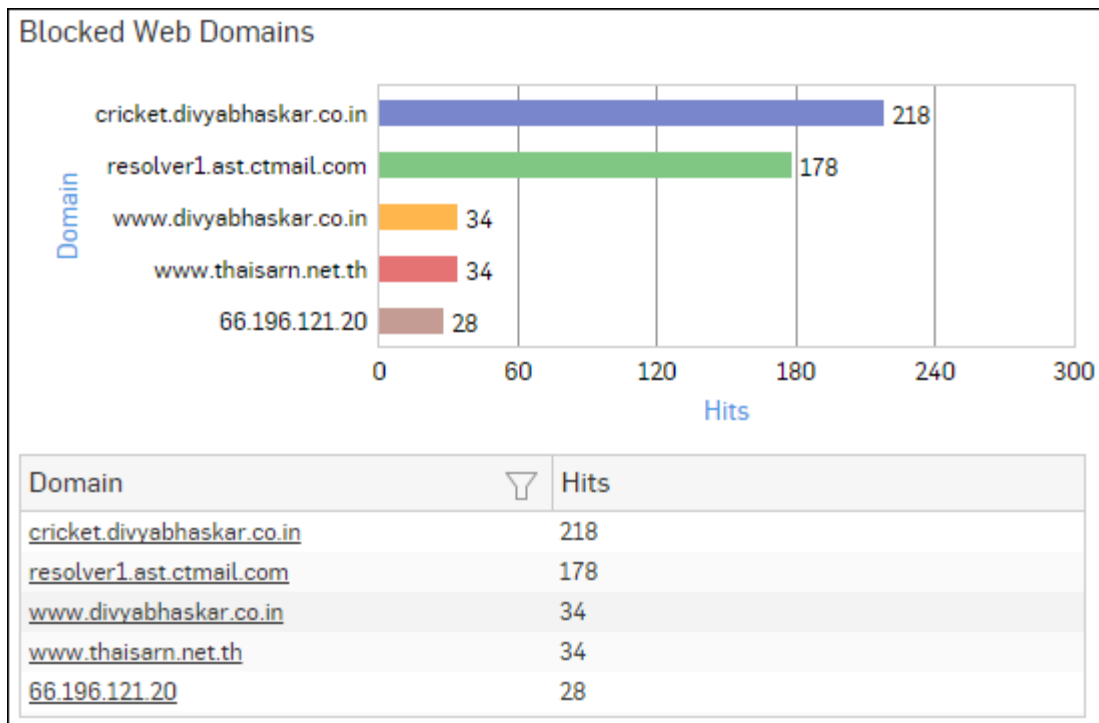


Figure 109: Blocked Web Domains

Click the Domain hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Blocked Web Hosts

This Report displays the list of blocked web hosts and the number of blocked sites users tried to access through that hosts.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Hosts**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of hosts along with number of hits per host while the tabular report contains the following information:

- Host: Name of the Host.
- Hits: Number of Hits.

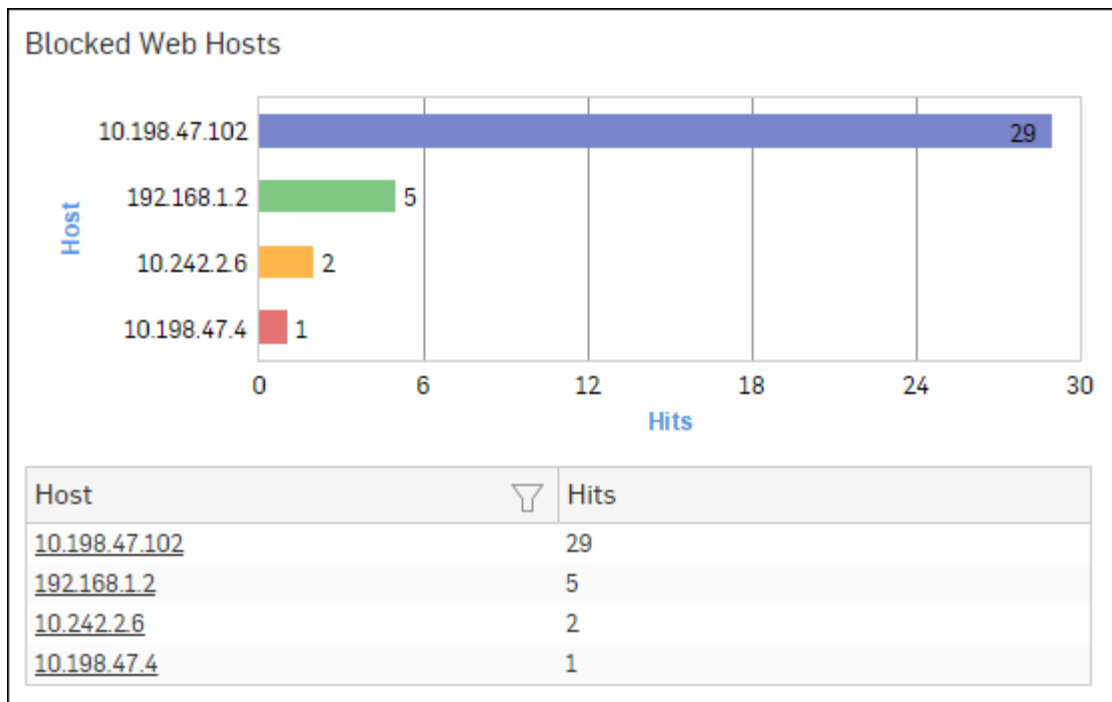


Figure 110: Blocked Web Hosts

Click the Host hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Blocked Allowable Categories

This Report displays a list of web categories falling under either Productive or Neutral category type and yet attempt to access the same by a user was denied.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Allowable Categories**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of categories along with number of hits per category while the tabular report contains the following information:

- Category: Name of the category.
- Category Type: Type of the acceptable category, as defined in the Device. Possible acceptable category types are:
 - Productive
 - Acceptable
- Domain Count: Number of blocked domains under each category.
- Hits: Number of hits per category.

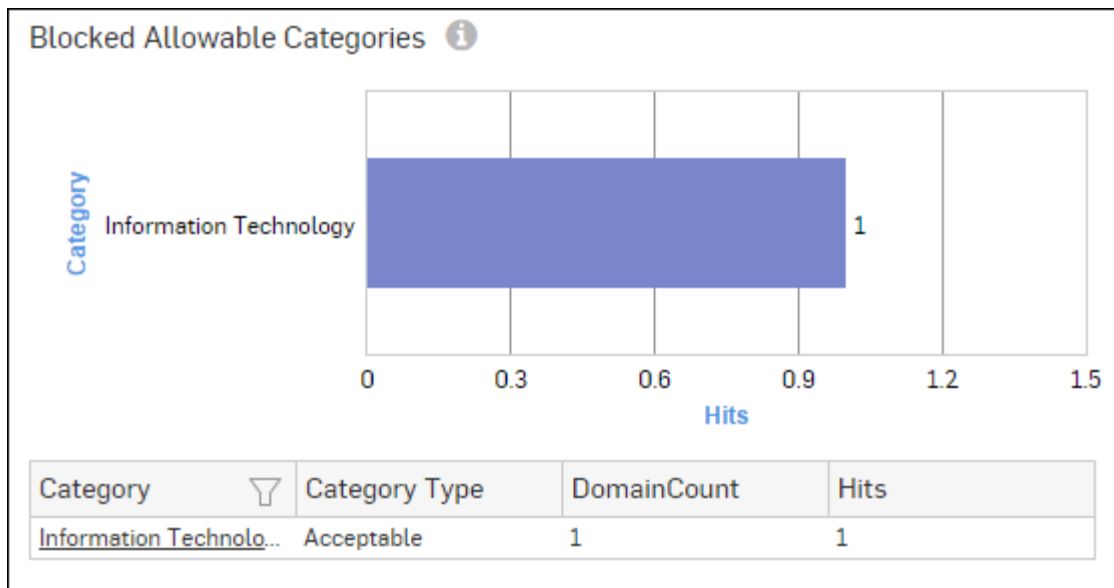


Figure 111: Blocked Allowable Categories

Click the Category hyperlink in table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Blocked Allowable Domains

This Report displays a list of Domains categorized under a category of type Productive or Acceptable and yet attempt to access the same by a user was denied.

View the report from Blocked Web Attempts reports dashboard or **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Allowable Domains**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of web domains along with number of hits per domain while the tabular report contains the following information:

- Domain: Name of the denied domain.
- Category: Name of the category, under which the domain is categorized in the Device.
- Category Type: Type of the acceptable category, as defined in the Device. Possible acceptable category types are:
 - Productive
 - Acceptable
- Hits: Number of hits per domain.

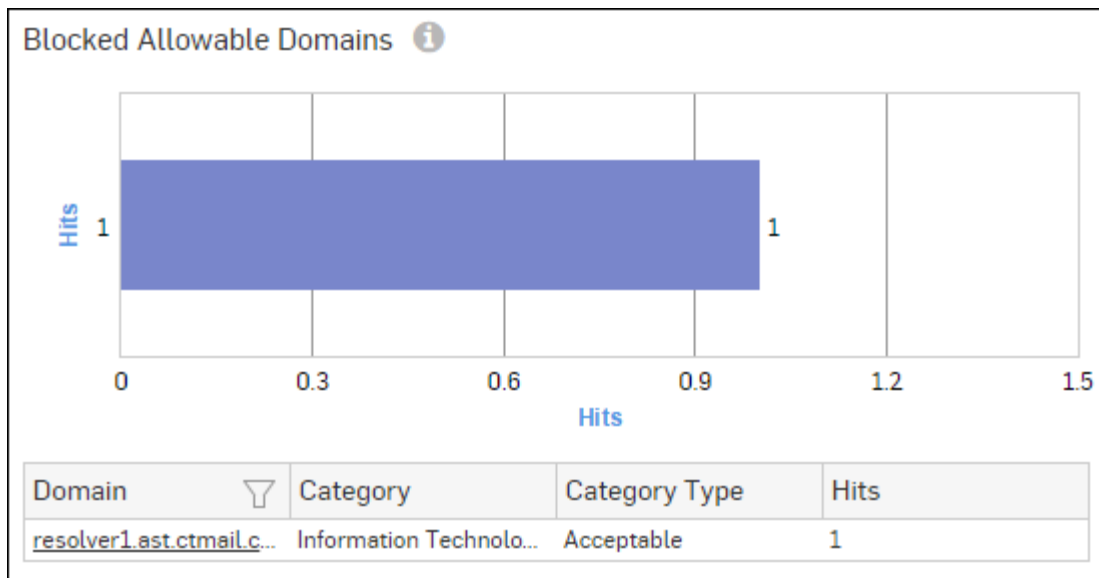


Figure 112: Blocked Allowable Domains

Click the Domain hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Blocked Policies

This Report displays a list of firewall rule ID along with number of hits per firewall rule.

View the reports from Blocked User Apps reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Policies**.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of firewall rule IDs along with number of hits while tabular report contains following information:

- Policy Rule: Number displaying firewall rule ID.
- Hits: Number of hits per firewall rule.

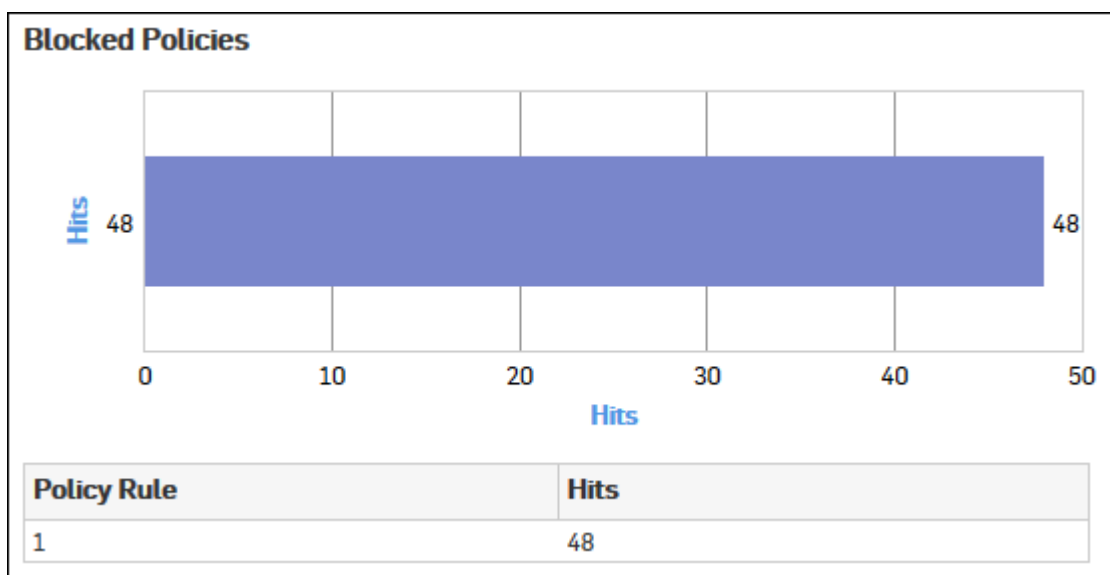


Figure 113: Blocked Policies

Click the Policy Rule hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#) on page 139.

Blocked Web Activity

This Report displays a list of blocked web activities that various users tried to access and the number of access attempts to each activity.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Blocked Web Activity**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of activities along with number of hits per activity while the tabular report contains the following information:

- Activity: Displays name of the activity as defined in the Device.
- Hits: Number of hits per activity.

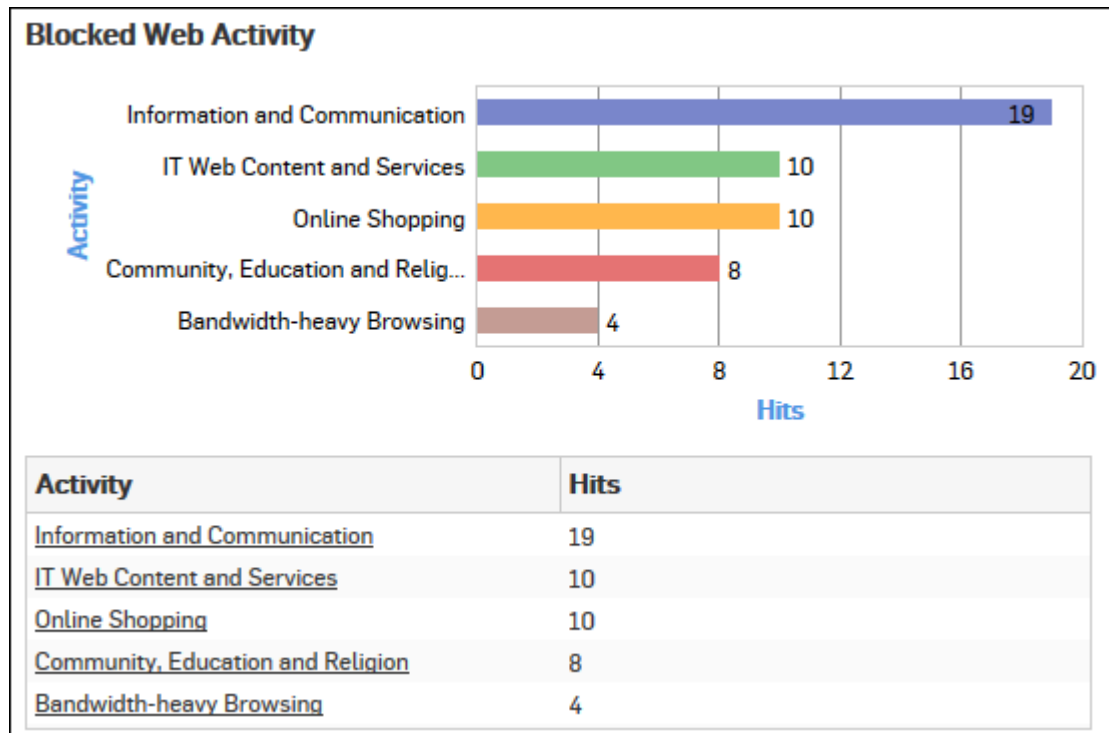


Figure 114: Blocked Web Activity

Click the Activity hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Web](#).

Trend - Blocked Web Attempts

This Report provides an overview of blocked web usage trend based on the Internet surfing pattern of the users in your network.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Trend - Blocked Web Attempts**.

This Report is displayed using a graph as well as in a tabular format.

The bar graph displays mapping of blocked web events with time, while the tabular report contains the following information:

- Time: Time when event occurred.

- Event Type: Type of the event.
- Event: Number of hits per event type.

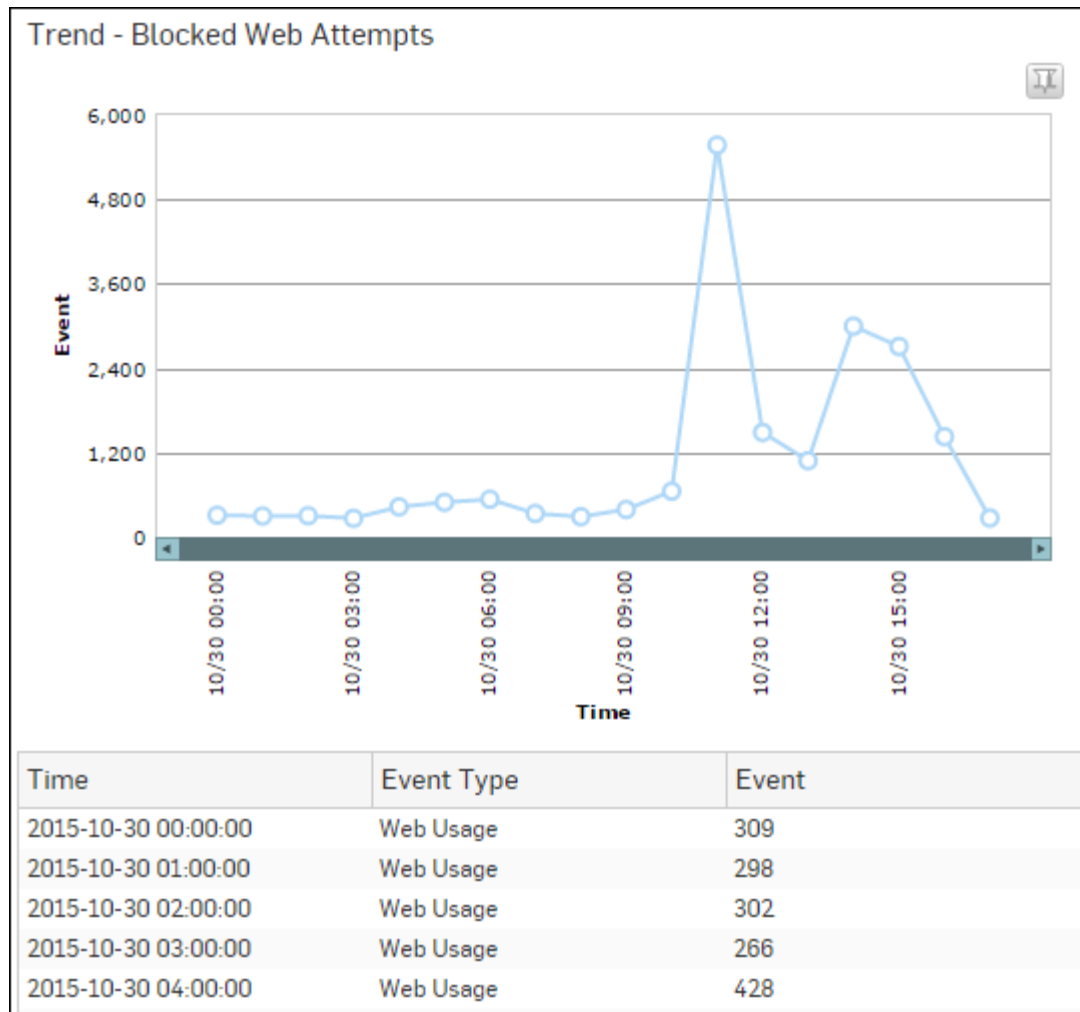


Figure 115: Trend - Blocked Web Attempts

Web Virus

This Report lists viruses blocked by the Device as well as number of occurrence per blocked virus.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked web viruses along with number of counts per virus while the tabular report contains the following information:

- Virus: Name of the blocked web virus.
- Count: Number of times a virus was blocked.

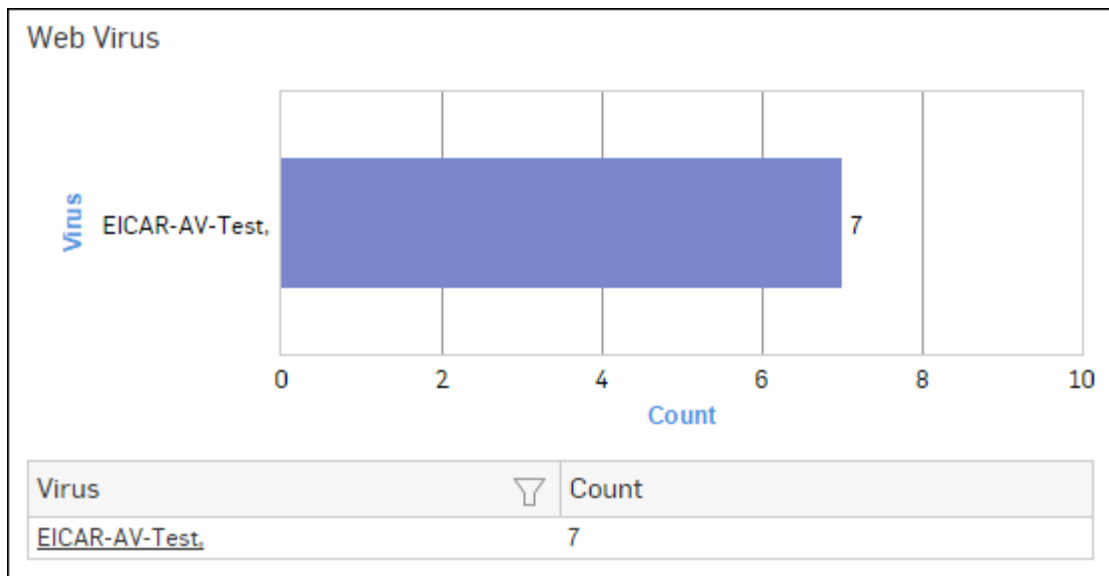


Figure 116: Web Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Domains - Web Virus

This Report lists web domains containing viruses and hence, blocked by the Device; as well as number of occurrence per blocked web domain.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Domains - Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked web domains along with number of counts per web domain while the tabular report contains the following information:

- Domain: Name of the blocked web domain.
- Count: Number of times a virus was blocked.

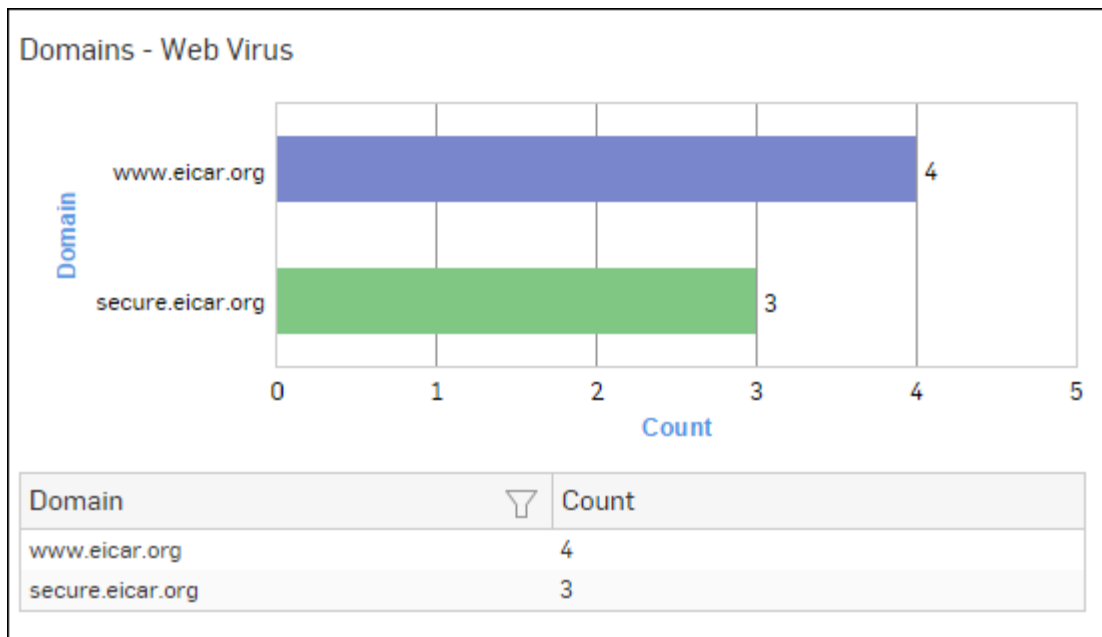


Figure 117: Domains - Web Virus

Click the Domain hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Users - Web Virus

This Report lists users containing machines infected with viruses and hence, blocked by the Device; as well as number of occurrence per blocked user.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Users - Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked users along with number of counts per user while the tabular report contains the following information:

- User: Name of the User as defined in the Device.
- Count: Number of times a user was blocked.

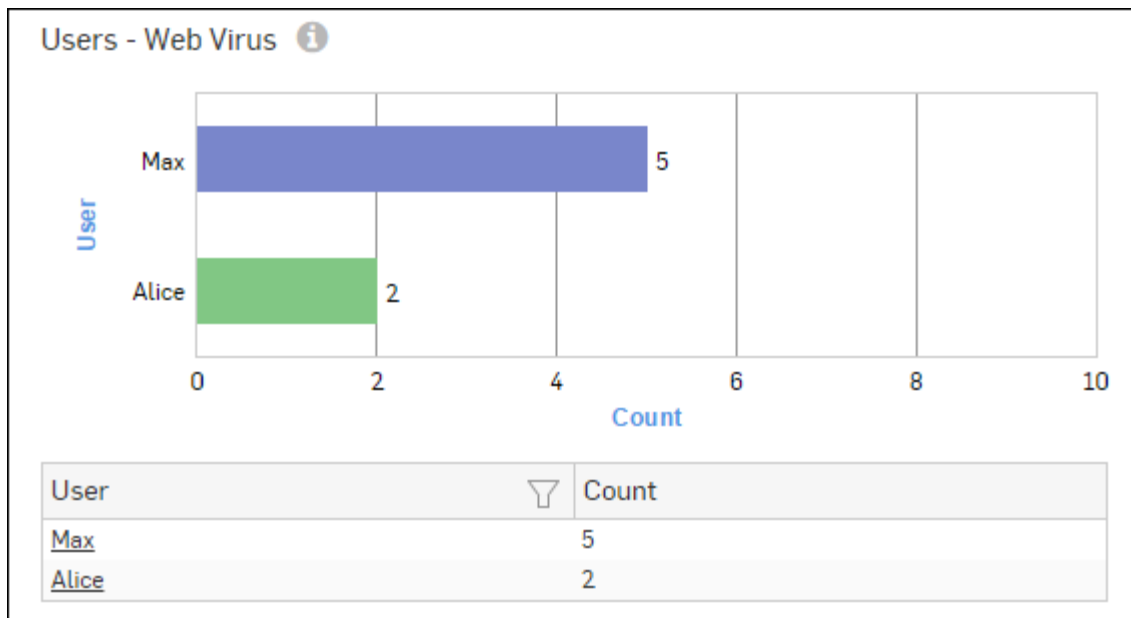


Figure 118: Users - Web Virus

Click the User hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Hosts - Web Virus

This Report lists hosts infected with viruses and hence, blocked by the Device; as well as number of occurrence per blocked host.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Hosts - Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked hosts along with number of counts per host while the tabular report contains the following information:

- Host: Name/IP Address of the host.
- Count: Number of times a host was blocked.

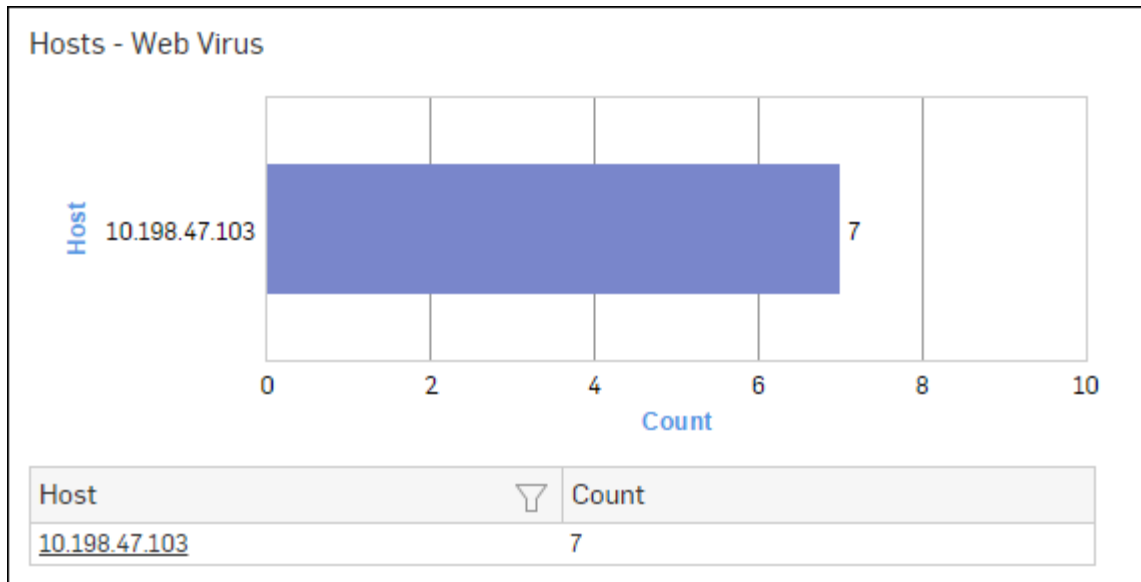


Figure 119: Hosts - Web Virus

Click the Host hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Trend - Web Virus

This Report provides an overview of blocked web virus trend based on the web viruses blocked over a period of time.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Trend - Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

The bar graph displays mapping of blocked web virus event with time, while the tabular report contains the following information:

- Time: Time when the event occurred.
- Event Type: Type of the event.
- Event: Number of hits per event type.

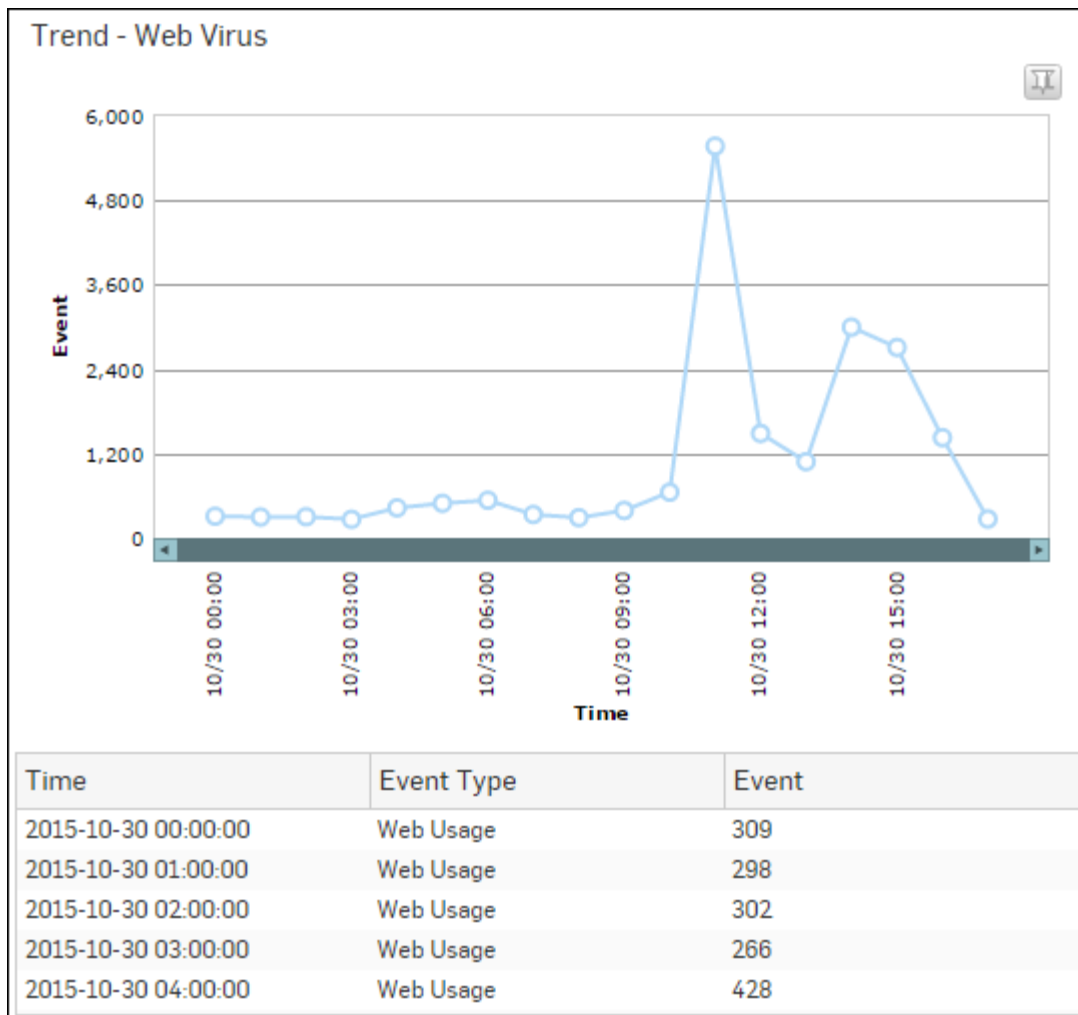


Figure 120: Trend - Web Virus

Filtered Blocked Web Attempts Reports - Web

The Blocked Web Attempts Reports can be filtered to get the following set of Blocked Web Attempts Reports:

- [Blocked Web Users](#)
- [Blocked Web Categories](#)
- [Blocked Web Domains](#)
- [Blocked Web Hosts](#)
- [Blocked Web Applications](#)
- [Blocked Allowable Categories](#)
- [Blocked Allowable Domains](#)
- [Blocked Policies](#)
- [Blocked Web Activity](#)

To get the Filtered Blocked Web Attempts reports, you need to choose one of the following filter criteria:

- User from [Blocked Web Users](#) Report
- Category from [Blocked Web Categories](#) Report
- Domain from [Blocked Web Domains](#) Report
- Host from [Blocked Web Hosts](#) Report
- Category from [Blocked Allowable Categories](#) Report
- Domain from [Blocked Allowable Domains](#) Report

- Rule ID from [Blocked Policies](#) on page 132 Report
- Activity from [Blocked Web Activity](#) Report

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format, which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Blocked Web Users widget

This widget displays the list of blocked web users along with the number of hits.



Note: This widget will not be displayed for filter criterion User.

The bar graph displays various users who tried to access sites under a denied category while the tabular report contains the following information:

- User: Displays the various denied users.
- Hits: Number of hits per user.

Blocked Web Categories widget

This widget displays a list of blocked web categories along with the number of hits per category.



Note: This widget will not be displayed for filter criterion Category.

The bar graph displays various denied categories which a user has tried to access while the tabular report contains the following information:

- Category: Web category name.
- Hits: Number of Hits.

Blocked Web Domains widget

This Widget displays the list of blocked web domains along with the number of hits per domain.



Note: This widget will not be displayed for filter criterion Domain.

The bar graph displays various denied domains and number of hits while the tabular report contains the following information:

- Domain: Name of denied domain.
- Hits: Number of Hits

Blocked Web Hosts widget

This widget displays the list of blocked web hosts through which a user has tried to access denied sites, along with the number of hits per host.



Note: This widget will not be displayed for filter criterion Host.

The bar graph displays various hosts and number of hits while the tabular report contains the following information:

- Host: Displays the host name.
- Hits: Number of hits per host.

Blocked Web Applications widget

This widget displays the list of blocked web applications along with the number of hits per blocked application.

The bar graph displays blocked web applications and number of hits per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the blocked web application.
- Hits: Number of hits per blocked web application.

Blocked Allowable Categories widget

This widget displays a list of web categories falling under either Productive or Acceptable category type and yet attempt to access the same by a user was denied



Note: This widget will not be displayed for filter criterion Category.

The bar graph displays list of categories along with number of hits per category while the tabular report contains the following information:

- Category: Name of the category.
- Category Type: Type of the acceptable category, as defined in the Device. Possible acceptable category types are:
 - Productive
 - Acceptable
- Domain Count: Number of blocked domains under each category.
- Hits: Number of hits per category.

Blocked Allowable Domains widget

This widget displays a list of Domains categorized under a category of type Productive or Acceptable and yet attempt to access the same by a user was denied



Note: This widget will not be displayed for filter criterion Domain.

The bar graph displays list of web domains along with number of hits per domain while the tabular report contains the following information:

- Domain: Name of the denied domain.
- Category: Name of the category, under which the domain is categorized in the Device.
- Category Type: Type of the acceptable category, as defined in the Device. Possible acceptable category types are:
 - Productive
 - Acceptable
- Hits: Number of hits per domain.

Blocked Policies widget

This widget report displays a list of firewall rule ID along with number of hits per firewall rule.



Note: This widget will not be displayed for filter criterion Rule ID.

The Report is displayed in the form of a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

Bar graph displays list of firewall rule IDs along with number of hits while tabular report contains following information:

- Policy Rule: Number displaying firewall rule ID.
- Hits: Number of hits per firewall rule.

Blocked Web Activity widget

This widget displays a list of blocked web activities along with the number of hits per activity.



Note: This widget will not be displayed for filter criterion Activity.

The bar graph displays various denied activity which a user has tried to access while the tabular report contains the following information:

- Activity: Displays name of the activity as defined in the Device.
- Hits: Number of hits per activity.

Filtered Blocked Web Attempts Reports - Virus

The Blocked Web Attempts Reports can be filtered to get the following set of Blocked Web Attempts Reports:

- [Web Virus](#)
- [Domains - Web Virus](#)
- [Users - Web Virus](#)

- [Hosts - Web Virus](#)

To get the Filtered Blocked Web Attempts reports, you need to choose one of the following filter criteria:

- Virus from [Web Virus](#) Report
- Domain from [Domains - Web Virus](#) Report
- User from [Users - Web Virus](#) Report
- Host from [Hosts - Web Virus](#) Report

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format, which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Web Virus widget

This widget lists viruses blocked by the Device as well as number of occurrence per blocked virus.



Note: This widget will not be displayed for filter criterion Virus.

The bar graph displays blocked web viruses along with number of hits per virus while the tabular report contains the following information:

- Virus: Name of the blocked web virus.
- Count: Number of times a virus was blocked.

Domains - Web Virus widget

This widget lists web domains containing viruses and hence, blocked by the Device; as well as number of occurrence per blocked web domain.



Note: This widget will not be displayed for filter criterion Domain.

The bar graph displays blocked web domains along with number of hits per web domain while the tabular report contains the following information:

- Domain: Name of the blocked web domain.
- Count: Number of times a virus was blocked.

Users - Web Virus widget

This widget lists users containing machines infected with viruses and hence, blocked by the Device; as well as number of occurrence per blocked user.



Note: This widget will not be displayed for filter criterion User.

The bar graph displays blocked users along with number of hits per user while the tabular report contains the following information:

- User: Name of the User as defined in the Device.
- Count: Number of times a user was blocked.

Hosts - Web Virus widget

This widget lists hosts infected with viruses and hence, blocked by the Device; as well as number of occurrence per blocked host.



Note: This widget will not be displayed for filter criterion Host.

The bar graph displays blocked hosts along with number of hits per host while the tabular report contains the following information:

- Host: Name/IP Address of the host.
- Count: Number of times a host was blocked.

Search Engine

Search Engine reports dashboard provide a snapshot of the search patterns of the users.

The reports help identify the Internet behavior of the users. It provides search statistics based on Google, Yahoo, Bing, Wikipedia, Rediff and eBay search engines.

These reports can help determining users' orientations and Internet behavior.

View Search Engine reports dashboard from **Monitor & Analyze > Reports > Applications & Web > Search Engine**

The Search Engine reports dashboard enables to view search request details for the following search engines:

- [Google Search](#)
- [Yahoo Search](#)
- [Bing Search](#)
- [Wikipedia Search](#)
- [Rediff Search](#)
- [eBay Search](#)
- [Yandex Search](#)

Google Search

This Report displays a list of search keywords used to perform Google Search, along with the user and time of search.

View the report from Search Engine reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Search Engine > Google Search**.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Time: Date and time of the search request. Precision of time will be in milliseconds.
- User Name: Name of the user who performed the search.
- Source IP: IP Address of the machine from which the search query was performed.
- Search Key: Search keyword.

Google Search			
Time	User Name	Source IP	Search Key
2015-11-03 15:39:59	Unidentified	10.198.47.9	Vadilal Enterprises L...
2015-11-03 15:39:59	Unidentified	10.198.47.9	vadilal enterprise
2015-11-02 13:00:00	Unidentified	10.198.47.9	dvi diwali thali decor...
2015-10-14 10:46:00	iview1	10.198.47.52	rediff search
2015-10-14 10:46:00	iview1	10.198.47.52	rediff search

Figure 121: Google Search

Yahoo Search

This Report displays a list of keywords used to perform Yahoo Search along with the user and time of search.

View the report from Search Engine reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Search Engine > Yahoo Search**.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains following information:

- Time: Date and time of the search request. Precision of time will be in milliseconds.
- User Name: Name of the user who performed the search.
- Source IP: IP Address of the machine from which the search query was performed.
- Search Key: Search keyword.

Yahoo Search			
Time	User Name	Source IP	Search Key
2015-10-30 16:50:00	dp	10.198.47.102	google translate

Figure 122: Yahoo Search

Bing Search

This Report displays a list of keywords used to perform Bing Search along with the user name, source IP address and time of search.

View the report from Search Engine reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Search Engine > Bing Search**.

By default, the report is displayed for the current date and all the devices. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Time: Date and time of the search request. Precision of time is in milliseconds.
- User Name: Name of the user who performed the search.
- Source IP: IP Address of the machine from which the search query was performed.
- Search Key: Search keyword.

Bing Search			
Time	User Name	Source IP	Search Key
2015-10-30 16:10:00	Unidentified	10.198.47.4	digit it
2015-10-30 15:35:00	Unidentified	10.198.47.4	Hello
2015-10-30 15:35:00	Unidentified	10.198.47.4	search engin
2015-10-30 15:35:00	Unidentified	10.198.47.4	search engineer
2015-10-30 15:10:01	Unidentified	10.198.47.4	digit it

Figure 123: Bing Search

Wikipedia Search

This Report displays a list of keywords used to perform Wikipedia Search along with the user name, source IP address and time of search.

View the report from Search Engine reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Search Engine > Wikipedia Search**.

By default, the report is displayed for the current date and all the devices. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Time: Date and time of the search request. Precision of time is in milliseconds.
- User Name: Name of the user who performed the search.
- Source IP: IP Address of the machine from which the search query was performed.
- Search Key: Search keyword.

Wikipedia Search			
Time	User Name	Source IP	Search Key
2015-10-14 10:36:00	dp	10.198.47.52	3D
2015-10-14 10:36:00	dp	10.198.47.52	Cisco Router
2015-10-14 10:36:00	dp	10.198.47.52	Computer Network
2015-10-14 10:36:00	dp	10.198.47.52	Motorola
2015-10-14 10:36:00	dp	10.198.47.52	Nokia

Figure 124: Wikipedia Search

Rediff Search

This Report displays a list of keywords used to perform Rediff Search along with the user name, source IP Address and time of search.

View the report from Search Engine reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Search Engine > Rediff Search**.

By default, the report is displayed for the current date and all the devices. The report date or devices can be changed from the top most row of the page.

The tabular report contains the following information:

- Time: Date and time of the search request. Precision of time is in milliseconds.
- User Name: Name of the user who performed the search.
- Source IP: IP Address of the machine from which the search query was performed.
- Search Key: Search keyword.

Rediff Search			
Time	User Name	Source IP	Search Key
2015-10-14 10:46:00	iview1	10.198.47.52	Bags
2015-10-14 10:46:00	iview1	10.198.47.52	Books
2015-10-14 10:46:00	iview1	10.198.47.52	Lady gaga
2015-10-14 10:46:00	iview1	10.198.47.52	Laptop
2015-10-14 10:46:00	iview1	10.198.47.52	Laptops

Figure 125: Rediff Search

eBay Search

This Report displays a list of keywords used to perform eBay Search along with the user name, source IP address and time of search.

View the report from Search Engine reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Search Engine > eBay Search**.

By default, the report is displayed for the current date and all the devices. The report date or devices can be changed from the top most row of the page.

The tabular report contains the following information:

- Time: Date and time of the search request. Precision of time is in milliseconds.
- User Name: Name of the user who performed the search.
- Source IP: IP Address of the machine from which the search query was performed.
- Search Key: Search keyword.




eBay Search			
Time	User Name 	Source IP 	Search Key 
2015-12-08 15:07:01	atp10	10.198.47.102	mobile
2015-10-14 09:15:59	dp	10.198.47.52	furniture
2015-10-14 09:15:59	dp	10.198.47.52	bike
2015-10-14 09:15:59	dp	10.198.47.52	LED TV
2015-10-14 09:15:59	dp	10.198.47.52	dslr camera

Figure 126: eBay Search

Yandex Search

This Report displays a list of keywords used to perform Yandex Search along with the user name, source IP address and time of search.

View the report from Search Engine reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Search Engine > Yandex Search**.

By default, the report is displayed for the current date and all the devices. The report date or devices can be changed from the top most row of the page.

The tabular report contains the following information:

- Time: Date and time of the search request. Precision of time is in milliseconds.
- User Name: Name of the user who performed the search.
- Source IP: IP Address of the machine from which the search query was performed.
- Search Key: Search keyword.




Yandex Search			
Time	User Name 	Source IP 	Search Key 
2015-10-14 10:21:00	dp	10.198.47.52	5G
2015-10-14 10:21:00	dp	10.198.47.52	Apple
2015-10-14 10:21:00	dp	10.198.47.52	Dominoz
2015-10-14 10:21:00	dp	10.198.47.52	Election
2015-10-14 10:21:00	dp	10.198.47.52	Facebook

Figure 127: Yandex Search

Web Server Usage

Web Server Usage reports dashboard provides statistics about your hosted web servers in terms of bandwidth consumed, users and domains.

View the reports dashboard from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage**.

Web Server Usage reports dashboard provide visibility of:

- [Web Server Domains](#)
- [Web Server Users](#)
- [Web Server Client IP](#)



Note: The bandwidth usage information displayed in reports may vary from that shown in Policies page as the Policies page shows the amount of data processed by the Sophos Firewall at the network layer while the reports display the amount processed at the application layer.

Web Server Domains

This Report displays a list of frequently accessed web server domains according to the utilization of bandwidth, along with the number of requests per web server.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Traffic Dashboard > Web Server Domains** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of web servers along with the number of bytes while the tabular report contains the following information:

- Web Server Domain: Displays name of the web server domain.
- Bytes: Bandwidth used per web server domain.
- Requests: Number of requests per web server domain.

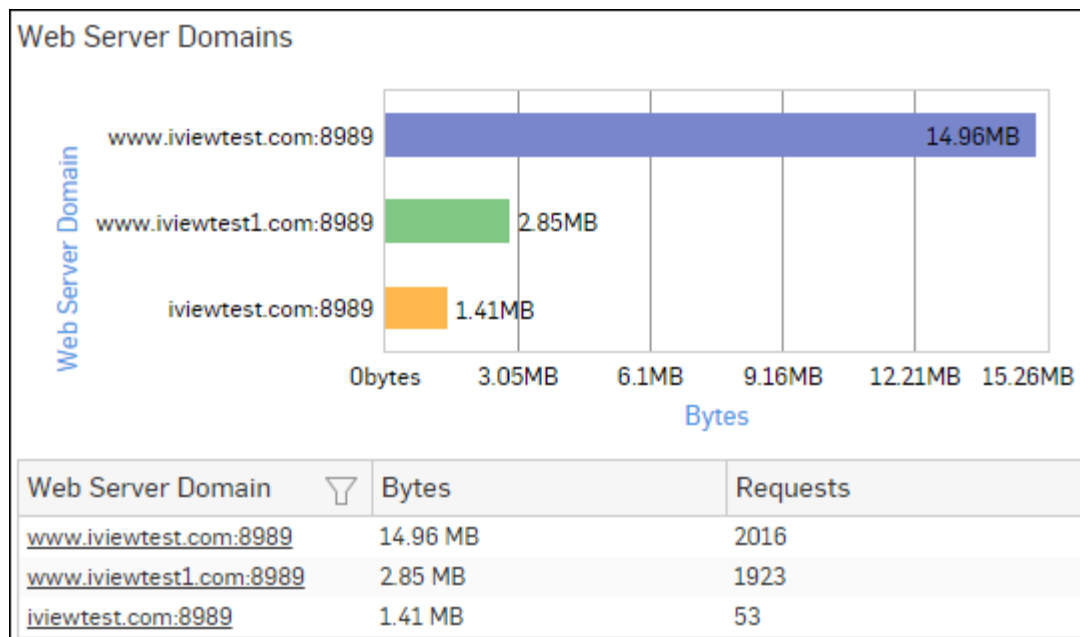


Figure 128: Web Server Domains

Click the Web Server Domain hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Web Server Users

This Report displays web server usage in terms of bandwidth utilization by users.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of domains along with bytes while the tabular report contains the following information:

- User: Username of the user, as defined in the Device.
- Bytes: Bandwidth used per user.
- Hits: Number of hits per user.

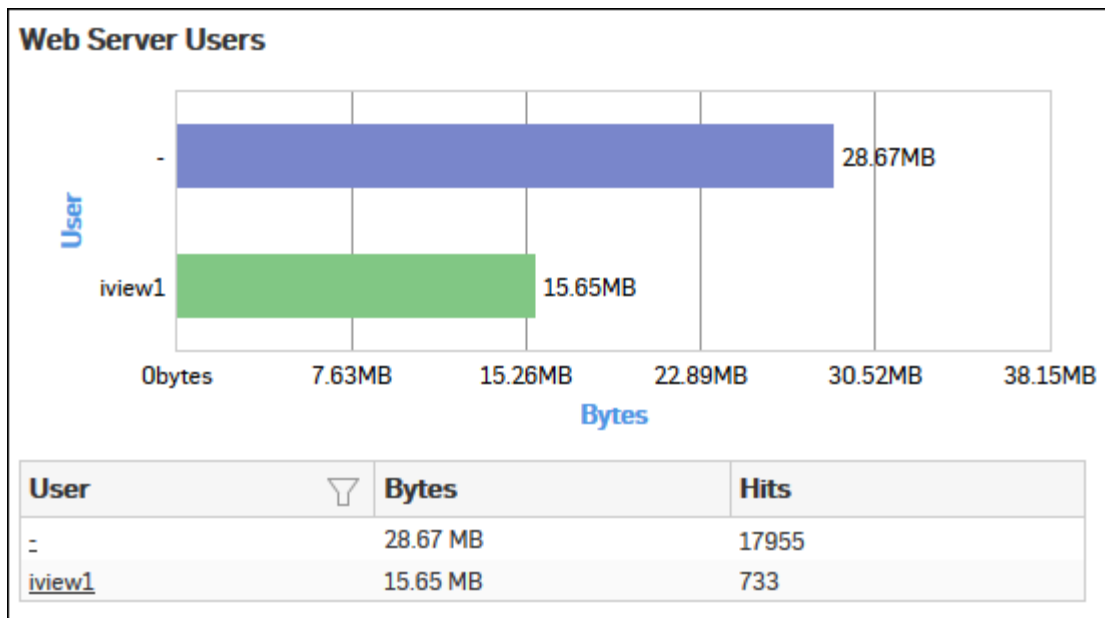


Figure 129: Web Server Users

Click the User hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Web Server Client IP

This Report displays number of requests sent to a web server per client IP Address along with amount of data transferred.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Client IP**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of client IP Addresses along with the bytes while the tabular report contains the following information:

- Client IP: IP Address of the machine, sending request to the web server.
- Bytes: Bandwidth used per Client IP.
- Hits: Number of hits per Client IP.

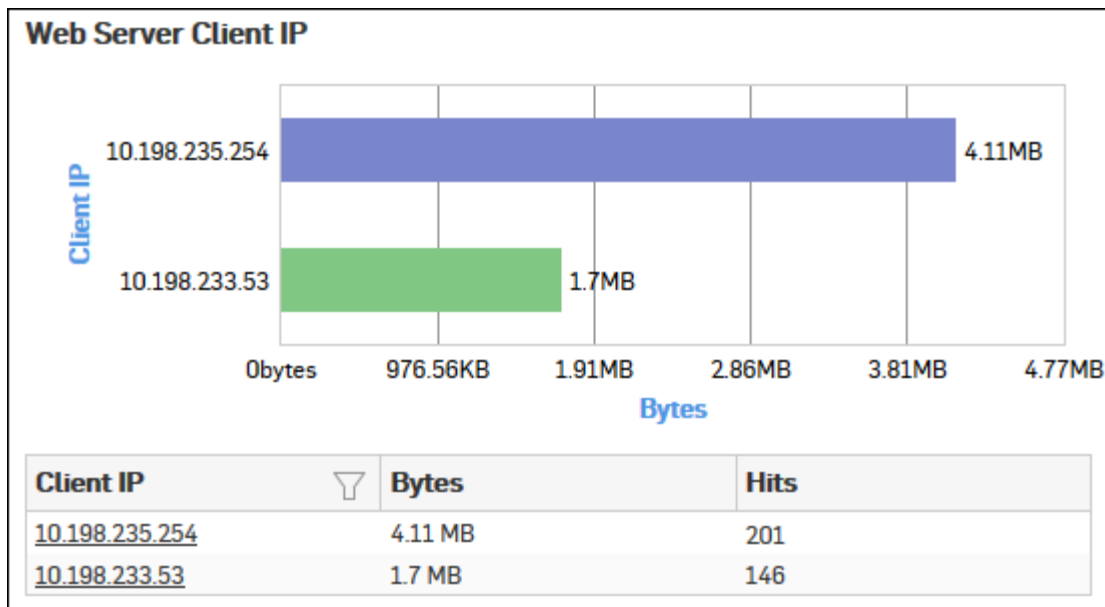


Figure 130: Web Server Client IP

Click the Client IP hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Filtered Web Server Usage Reports

Web Server Usage reports can be filtered to get following set of reports:

- [Web Server Domains](#)
- [Web Server Users](#)
- [Web Server Client IP](#)

To get Filtered Web Server Usage reports, you need to choose one of the following filter criteria:

- Web Server from [Web Server Domains](#) Report
- Web User from [Web Server Users](#) Report
- Client IP from [Web Server Client IP](#) Report

Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Web Server Domains widget

This widget displays a list of frequently accessed web servers according to the utilization of bandwidth, along with the number of hits per web server.



Note: This widget will not be displayed for filter criterion Web Server.

The bar graph displays the list of web servers along with the number of hits while the tabular report contains the following information:

- Web Server Domain: Displays name of the web server.
- Bytes: Bandwidth used per web server.
- Requests: Number of requests per web server.

Web Server Users widget

This widget displays web server usage in terms of bandwidth utilization by users.



Note: This widget will not be displayed for filter criterion User.

The bar graph displays a list of domains along with the number of hits while the tabular report contains the following information:

- User: Username of the user, as defined in the Device.
- Bytes: Bandwidth used per user.
- Hits: Number of hits per user.

Web Server Client IP widget

This Report displays number of requests sent to a web server per client IP Address along with amount of data transferred.



Note: This widget will not be displayed for filter criterion Client IP.

The bar graph displays a list of client IP Addresses along with the bytes while the tabular report contains the following information:

- Client IP: IP Address of the machine, sending request to the web server.
- Bytes: Bandwidth used per Client IP.
- Hits: Number of hits per Client IP.

Web Server Protection

Web Server Protection reports dashboard provide security status about your hosted web servers in terms of attacked web servers and attacks, users, sources blocked by the Device .

View the Web Server Protection reports dashboard from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection**.

Web Server Protection reports dashboard provide visibility of:

- [Attacked Web Server Domains](#)
- [Web Server Attacks](#)
- [Web Server Attackers](#)
- [Web Server Virus](#)

Attacked Web Server Domains

This Report displays a list of attacked web servers along with the number of hits per server.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Attacked Web Server Domains**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Attacked Web Server Domains** as well.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of web servers along with the number of hits while the tabular report contains the following information:

- Web Server Domain: Displays name or IP Address of the attacked web server.
- Hits: Number of hits per web server.

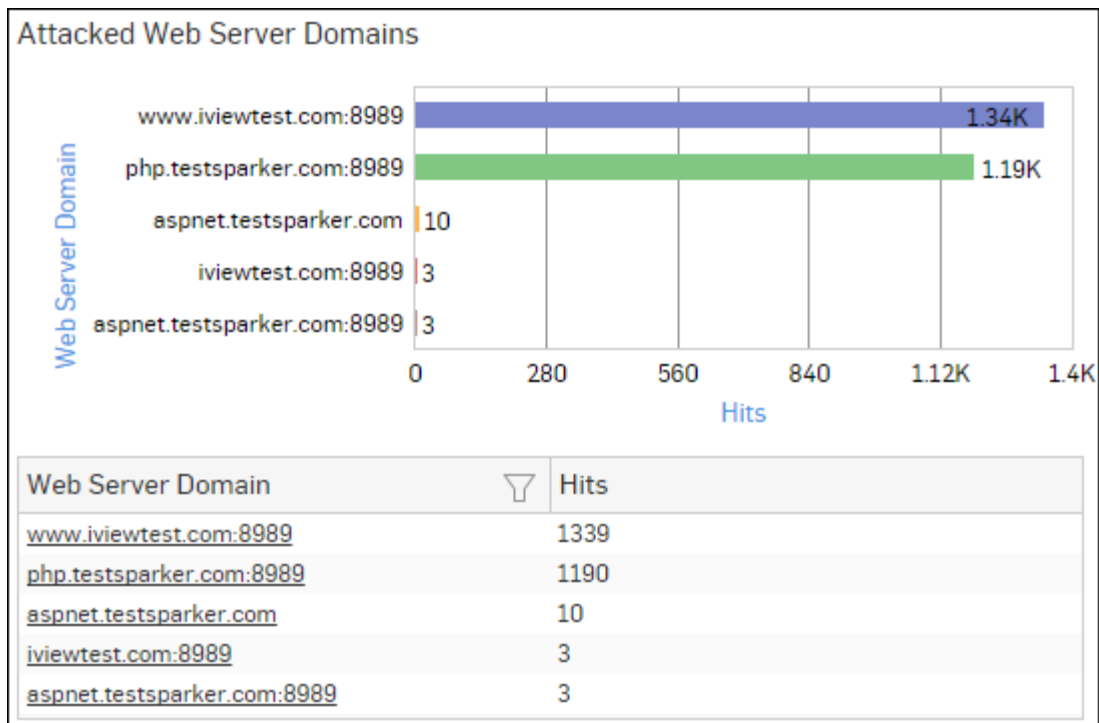


Figure 131: Attacked Web Server Domains

Click the Web Server Domain hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Blocked Web Server Requests

This Report displays a list of reasons of attacks blocked by the Device, along with the number of hits per attack.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Blocked Web Server Requests**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Server Requests** as well.

The bar graph displays the list of blocked reasons along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

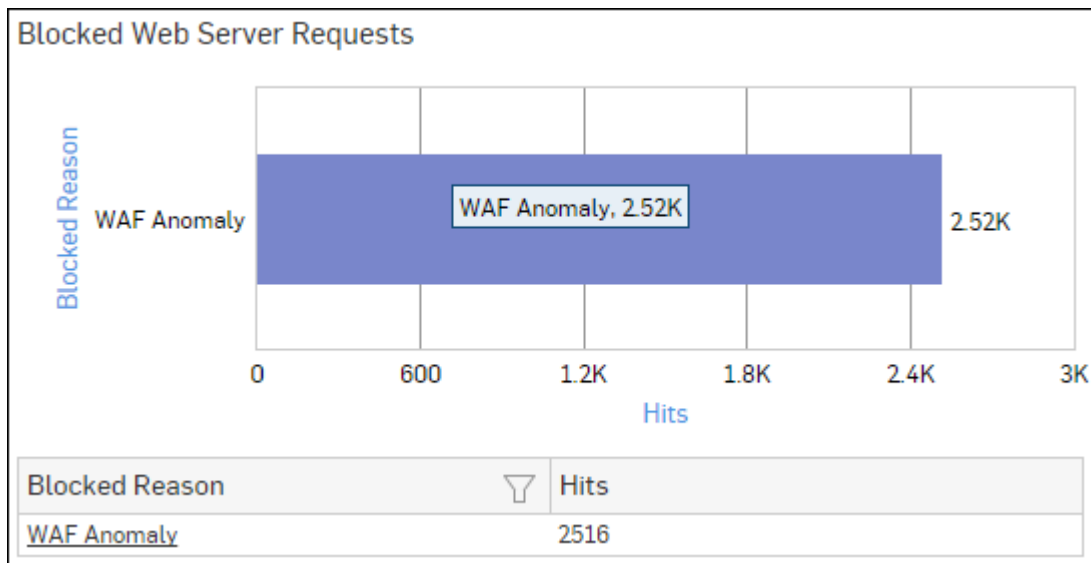


Figure 132: Blocked Web Server Requests

Click the Blocked Reason hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Web Server Attack Source

This report displays a list of source IP Addresses used to launch an attack on your web server, along with the number of hits per source IP Address.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Web Server Attack Source**.

The bar graph displays the list of the source IP Addresses and the number of hits while the tabular report contains the following information:

- Source IP: IP Address of the source(s) which are used to launch the attack.
- User: Name of the user, as defined in the Device. In case the user is unauthenticated, Unidentified is displayed.
- Hits: Number of hits to the source IP Address.

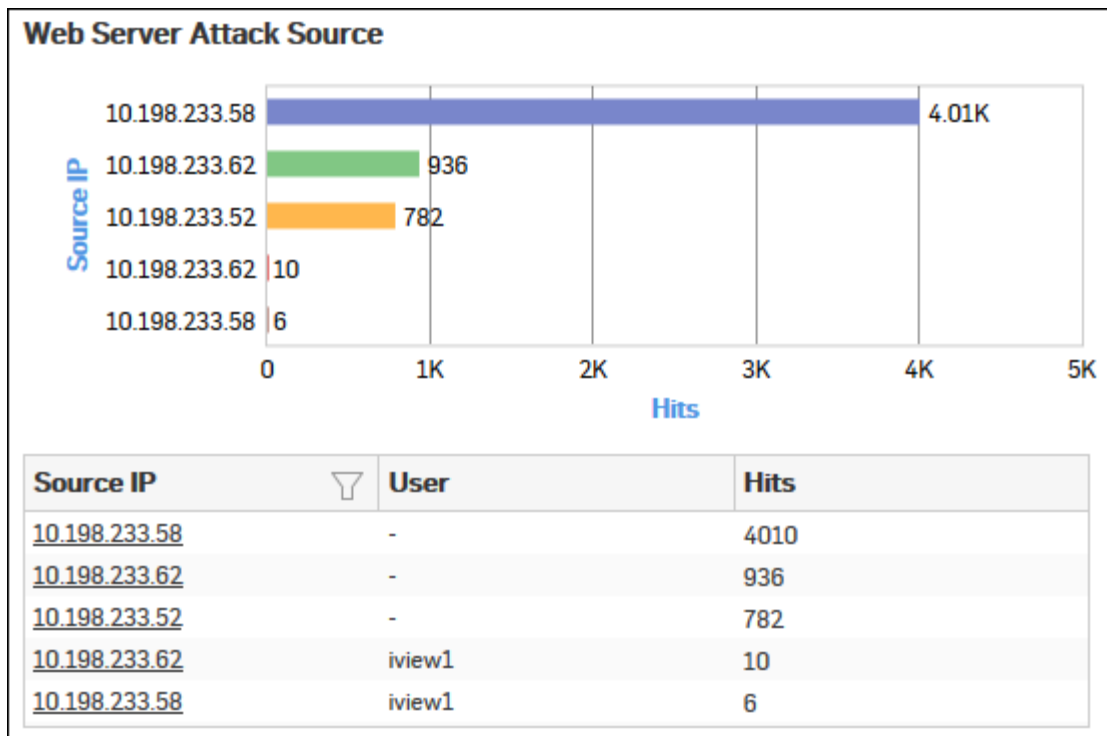


Figure 133: Web Server Attack Source

Click the Source IP hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Web Server Virus

This report displays a list of blocked viruses along with number of hits per virus.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Web Server Virus**.

The bar graph displays the list of viruses and number of hits while the tabular report contains the following information:

- Virus: Name of the Virus blocked by the Device.
- Hits: Number of hits per blocked virus.

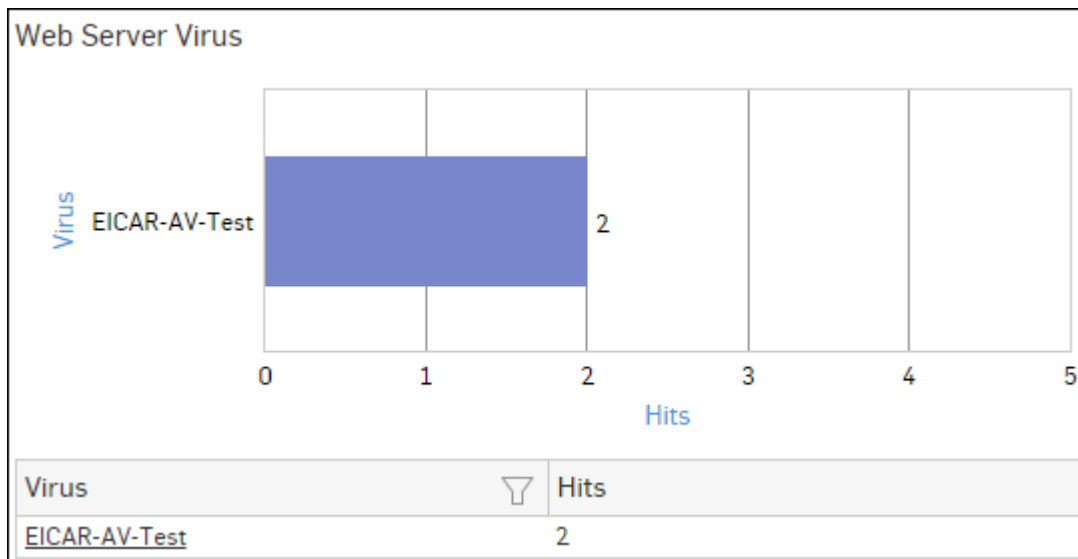


Figure 134: Web Server Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Filtered Web Server Protection Reports

Web Server Protection reports can be filtered to get following set of reports:

- [Attacked Web Servers](#)
- [Blocked Web Server Requests](#)
- [Web Server Attackers](#)
- [Web Server Virus](#)

To get Filtered Web Server Protection reports, you need to choose one of the following filter criteria:

- Web Server from [Attacked Web Servers Report](#)
- Attack from [Web Server Attacks Report](#)
- Attacker from [Web Server Attackers Report](#)
- Virus from [Web Server Virus Report](#)

Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays report in a graph as well as in a tabular format which can again be filtered. Detailed Reports are displayed in a tabular format which can be filtered by clicking hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Attacked Web Server Domains widget

This Report displays a list of attacked web servers along with the number of hits per server.



Note: This widget will not be displayed for filter criterion Web Server.

The bar graph displays the list of web servers along with the number of hits while the tabular report contains the following information:

- Web Server Domain: Displays name or IP Address of the attacked web server.
- Hits: Number of hits per web server.

Blocked Web Server Requests widget

This Report displays a list of reason of attacks blocked by the Device, along with the number of hits per attack.



Note: This widget will not be displayed for filter criterion Blocked Reason.

The bar graph displays the list of blocked attacks along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

Web Server Attack Source widget

This widget displays a list of source IP Addresses used to launch an attack on your web server, along with the number of hits per source IP Address.



Note: This widget will not be displayed for filter criterion Source IP.

The bar graph displays the list of the source IP Addresses and the number of hits while the tabular report contains the following information:

- Source IP: IP Address of the source(s) which are used to launch the attack.
- User: Name of the user, as defined in the Device. In case the user is unauthenticated unidentified is displayed.
- Hits: Number of hits to the source IP Address.

Web Server Virus widget

This widget displays a list of blocked viruses along with number of hits per virus.



Note: This widget will not be displayed for filter criterion Virus.

The bar graph displays the list of viruses and number of hits while the tabular report contains the following information:

- Virus: Name of the Virus blocked by the Device.
- Hits: Number of hits per blocked virus.

User Data Transfer Report

The User Data Transfer reports dashboard provide a snapshot of the User traffic in terms of data transfer through your network.



Note: If the option to exclude data accounting from the Firewall Rule is enabled, then the User Data Transfer for the specific user is not be accounted for.



Note: The Data Transfer information, including the amount of uploaded/downloaded data, displayed in a report is accounted only when a user logs out of the Sophos Firewall device. In other words, data transfer usage for a user currently logged into the device is not be accounted for.

The data displayed here is accounted only when the user logs out of the Sophos Firewall device.

View the reports from **Monitor & Analyze > Reports > Applications & Web > User Data Transfer Report**.

The User Data Transfer reports dashboard enables to view the following reports:

- [User Groups](#)
- [Users](#)
- [Date-wise Usage Report](#)
- [Client Types](#)

User Groups

This Report displays the a list of the User Groups along with the amount of data transferred and time used for data transfer.

View the reports from the User Data Transfer reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User Data Transfer Report > User Groups**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of the user groups along with the amount of data transfer while the tabular report contains the following information:

- User Group: Name of the user group as defined in the Device.
- Data Transfer: Total amount of data transferred (Upload + Download) by the user group.
- Uploaded: Amount of uploaded data.
- Downloaded: Amount of downloaded data.
- Used Time: Time used for data transfer.

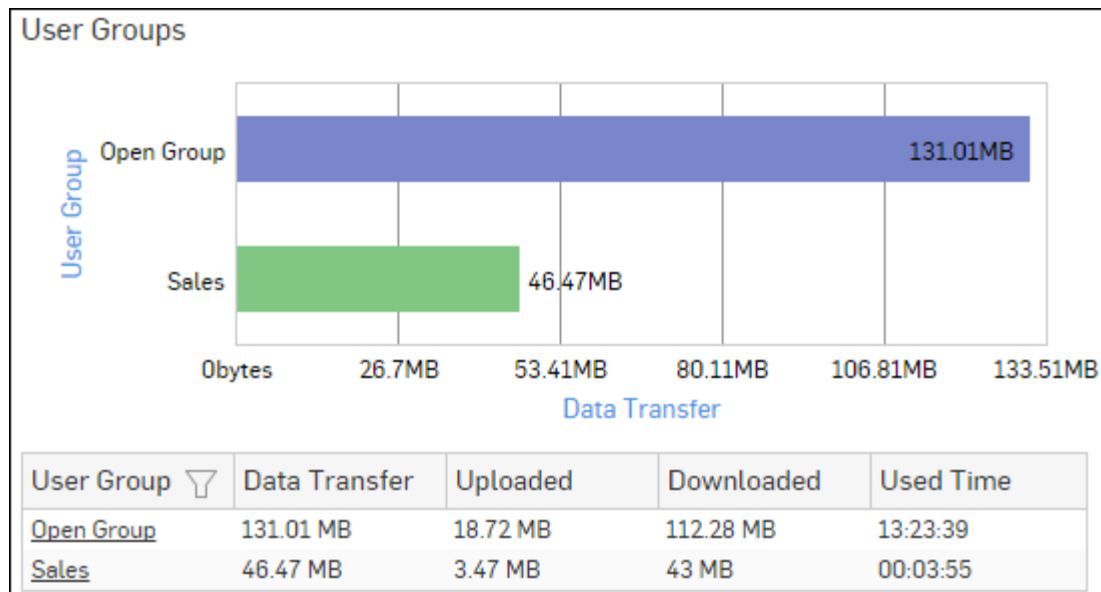


Figure 135: User Groups

Click the User Group hyperlink in table or graph to view the [Filtered User Data Transfer Reports](#).

Users

This Report displays a list of the Users along with the amount of data transferred and time used for data transfer.

View the reports from the User Data Transfer reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User Data Transfer Report > Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with amount of data transfer while the tabular report contains the following information:

- User: Name of the user as defined in the Device.
- Client Type: Type of client used for data transfer.
- Data: Total amount of data transferred (Upload + Download) by the user.
- Uploaded: Amount of uploaded data.
- Downloaded: Amount of downloaded data.
- Used Time: Time used for data transfer.

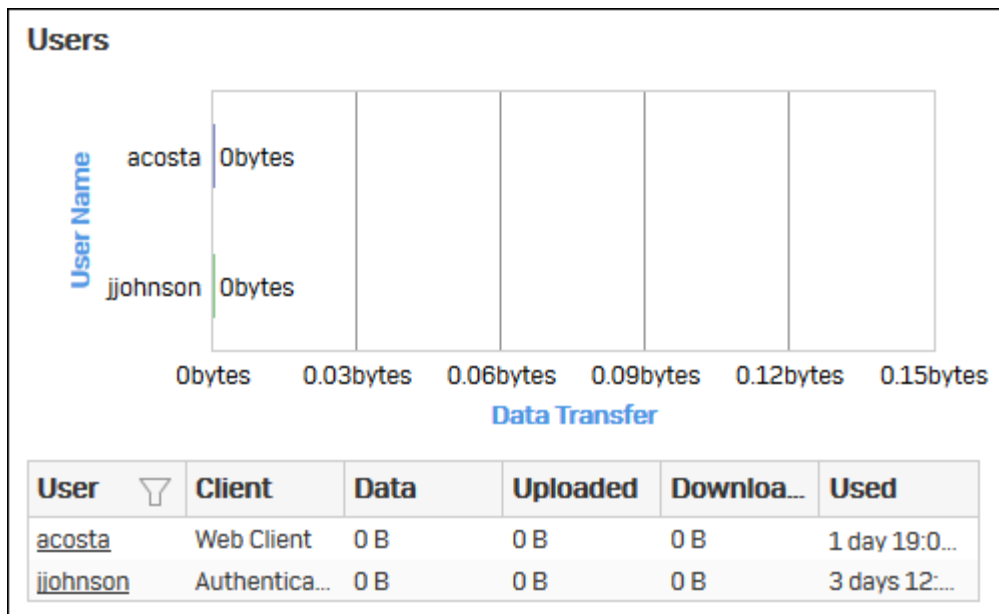


Figure 136: Users

Click the User hyperlink in the table or graph to view the [Filtered User Data Transfer Reports](#).

Date-wise Usage Report

This Report displays the list of Dates along with the amount of data transferred and time used for data transfer.

View the reports from the User Data Transfer reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User Data Transfer Report > Date-wise Usage Report**.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Tabular Report contains the following information:

- Date: Date when then data transfer has taken place.
- Client Type: Type of client used for data transfer.
- Used Time: Time used for data transfer.
- Data Transfer: Total amount of data transfer (Upload + Download).

Date-wise Usage Report			
Date	Client Type	Used Time	Data Transfer
2016-09-30	Web Client	1 day 19:04:20	0 B
2016-10-09	Authentication Ag...	3 days 12:02:48	0 B

Figure 137: Date-wise Usage Report

Click the Date hyperlink in the table or graph to view the [Filtered User Data Transfer Reports](#).

Client Types

This Report displays the list of clients along with amount of data transferred and time used for data transfer.

View the reports from the User Data Transfer reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > User Data Transfer Report > Client Types**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of clients along with amount of data transfer while the tabular report contains the following information:

- Client Type: Type of client used for data transfer.
- Data Transfer: Total amount of data transfer (Upload + Download).
- Uploaded: Amount of uploaded data.
- Downloaded: Amount of downloaded data.
- Used Time: Time used for data transfer.

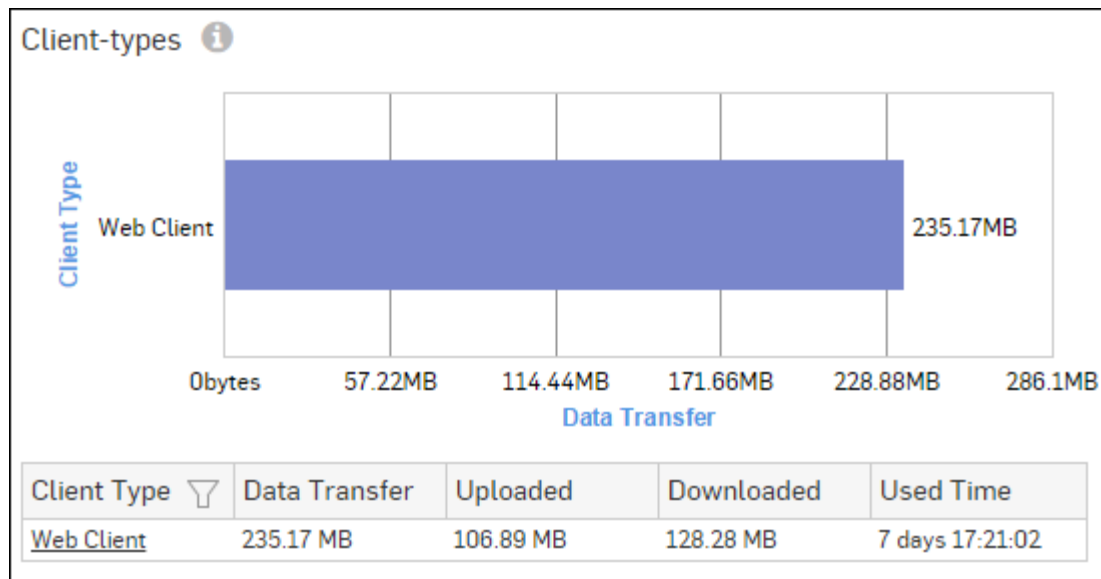


Figure 138: Client Types

Click the Client Type hyperlink in the table or graph to view the [Filtered User Data Transfer Reports](#).

Filtered User Data Transfer Reports

The User Data Transfer Reports can be filtered to get the following set of User Data Transfer reports.

- [User Groups](#)
- [Users](#)
- [Date-wise Usage Report](#)
- [Client Types](#)

To get filtered User Data Transfer reports, you need to choose one of the following filter criteria:

- User Group from [User Groups Report](#)
- User from [Users Report](#)
- Date from [Date-wise Usage Report](#)
- Client Type from [Client Types Report](#)

Based on the filter criterion, reports will be displayed in following formats.

- Summary- Reports in graphical format
- Details- Reports in tabular format

The Filtered Summary Reports consist of multiple report widgets except those in the filter criterion. Each widget displays report in a graph as well as in a tabular format which can again be filtered. The Detailed Reports are displayed in tabular format which can be filtered by clicking the hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

User Groups widget

This widget report displays a list of the User Groups along with the total amount of data transferred and time.



Note: This widget will not be displayed for the filter criterion User Group.

The bar graph displays various user groups with the total amount of data transfer while the tabular report contains the following information:

- User Group: Name of the user group as defined in the Device.
- Data Transfer: Total amount of data transferred (Upload + Download) by the user group.
- Uploaded: Amount of uploaded data.
- Downloaded: Amount of downloaded data.
- Used Time: Time used for data transfer.

Users widget

This widget report displays a list of the users along with the amount of data transferred.



Note: This widget will not be displayed for the filter criterion User.

The bar graph displays user wise data transfer while the tabular report contains the following information:

- User Name: Name of the user as defined in the Device.
- Client Type: Type of client used for data transfer.
- Data Transfer: Total amount of data transfer (Upload + Download) by the user.
- Uploaded: Amount of uploaded data.
- Downloaded: Amount of downloaded data.
- Used Time: Time used for data transfer.

Date-wise Usage Report widget

This widget report displays a list of the Dates along with the amount of data transfer.



Note: This widget will not be displayed for the filter criterion Date.

The bar graph displays the date wise data transfer while the tabular report contains the following information:

- Date: Date when then data transfer has taken place.
- Client Type: Type of client used for data transfer.
- Data Transfer: Total amount of data transfer (Upload + Download).
- Used Time: Time used for data transfer.

Client Types widget

This Widget report displays a list of the clients along with the amount of data transferred.

This widget will not be displayed for the filter criterion Client Type.

The bar graph displays client type wise data transfer while the tabular report contains the following information:

- Client Type: Type of client used for data transfer.
- Data Transfer: Total amount of data transfer (Upload + Download).
- Uploaded: Amount of uploaded data.
- Downloaded: Amount of downloaded data.
- Used Time: Time used for data transfer.

FTP Usage

The FTP Usage reports dashboard give an insight about the FTP activity - uploads and downloads; thus giving a clear picture of the FTP traffic volume over the selected time period.

The reports dashboard provide statistics based on the traffic generated by various hosts, users and servers.

View FTP Usage reports dashboard from **Monitor & Analyze > Reports > Applications & Web > FTP Usage**

The FTP Usage reports dashboard enables to view the FTP traffic generated by:

- [Files Uploaded via FTP](#)
- [Files Downloaded via FTP](#)
- [FTP Users \(Upload\)](#)
- [FTP Users \(Download\)](#)
- [FTP Hosts \(Upload\)](#)
- [FTP Hosts \(Download\)](#)
- [FTP Servers](#)

Files Uploaded via FTP

This Report displays a list of the Files uploaded along with the amount of data transferred.

View the report from FTP Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Usage > Files Uploaded via FTP**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of the files uploaded along with the amount of data transferred while the tabular report contains the following information:

- File: Name of the uploaded file.
- File Count: Number of files uploaded.
- Bytes: The amount of data transferred.

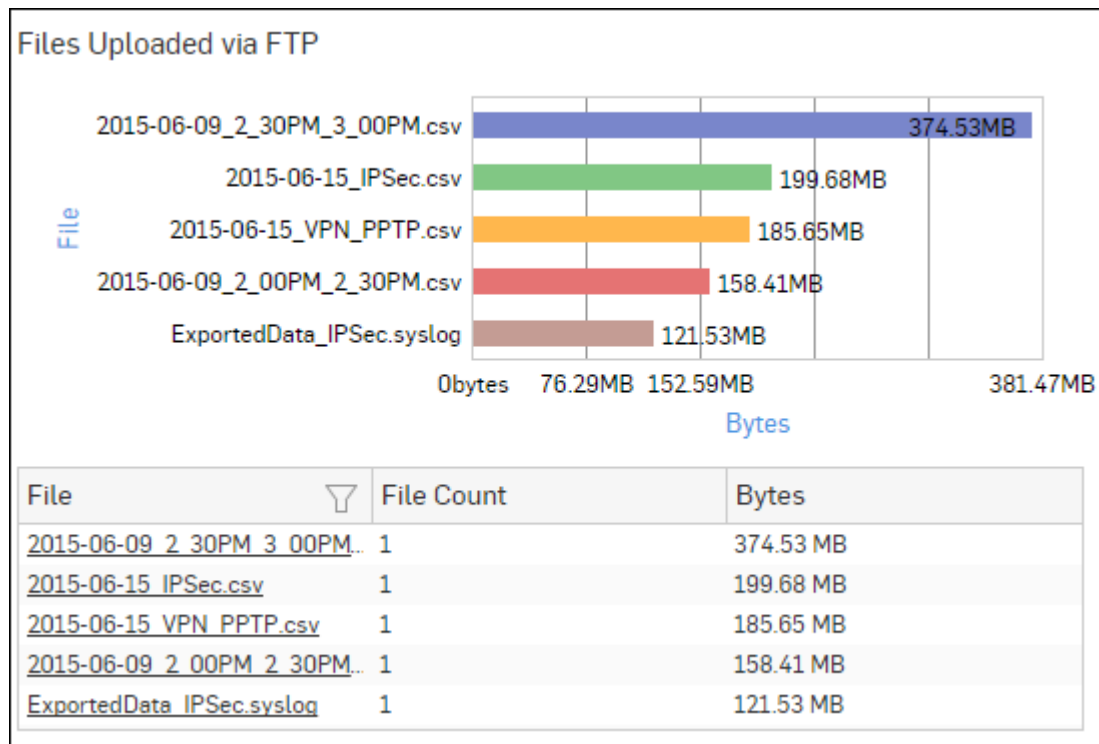


Figure 139: Files Uploaded via FTP

Click the File hyperlink in the table or graph to view the [Filtered FTP Usage Reports](#).

Files Downloaded via FTP

This Report displays a list of the top files downloaded along with the amount of data transfer.

View the report from FTP Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Usage > Files Downloaded via FTP**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays list of downloaded files along with the amount of data transferred while the tabular report contains the following information:

- File: Name of the file which has been downloaded.
- File Count: Number of files downloaded.
- Bytes: The amount of data transferred.

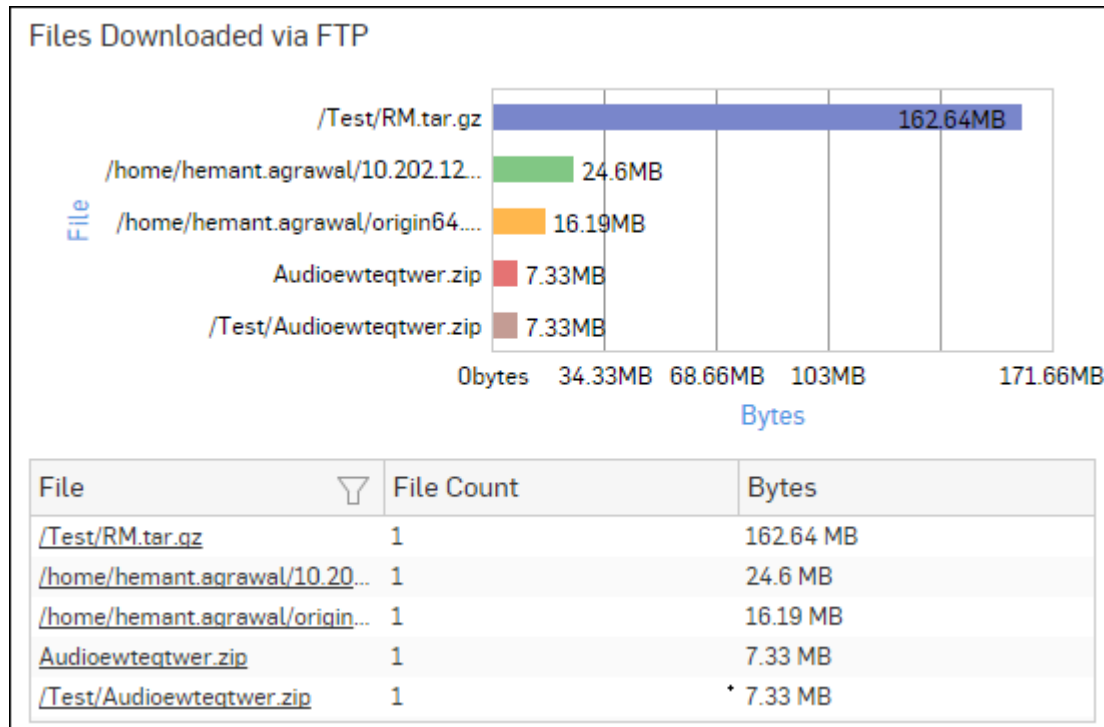


Figure 140: Files Downloaded via FTP

Click the File hyperlink in the table or graph to view the [Filtered FTP Usage Reports](#).

FTP Users (Upload)

This Report displays the list of Users who have generated the maximum traffic by uploading data through the FTP with the number of files and the amount of data transferred.

View the report from FTP Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Usage > FTP Users (Upload)**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data uploaded by each user while the tabular report contains the following information:

- User: Name of the user who uploaded the file. If the User is unauthenticated, then it will display 'Unidentified'. If more than one such user exists, then the traffic details of all the users will be grouped and displayed under unidentified.
- File Count: Number of files uploaded per user.

- Bytes: The amount of data transferred.

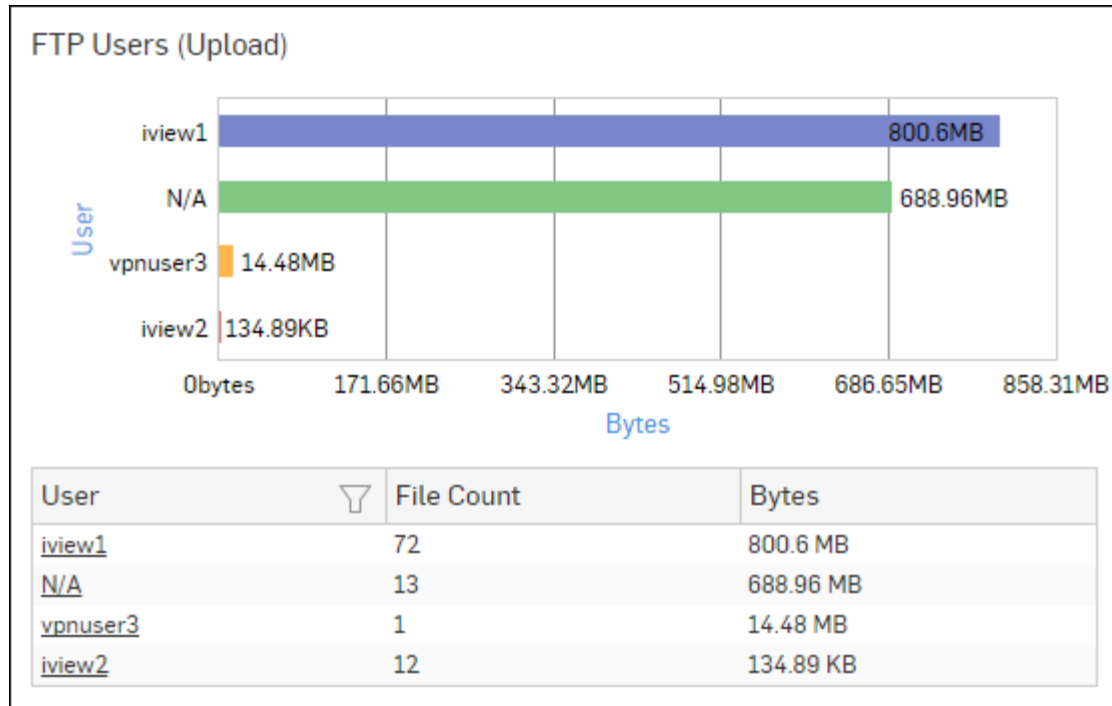


Figure 141: FTP Users(Upload)

Click the User hyperlink in the table or graph to view the [Filtered FTP Usage Reports](#).

FTP Users (Download)

This Report displays a list of Users who have generated the maximum traffic by downloading data through the FTP with the number of files and the amount of data transferred.

View the report from FTP Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Usage > FTP Users (Download)**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data downloaded by each user while the tabular report contains the following information:

- User: Name of the user who has downloaded the files. If the User is unauthenticated, then it will display 'Unidentified'. If more than one such user exists, then the traffic details of all such users will be grouped and displayed under unidentified.
- File Count: Number of files downloaded per user.
- Bytes: Amount of data transferred.

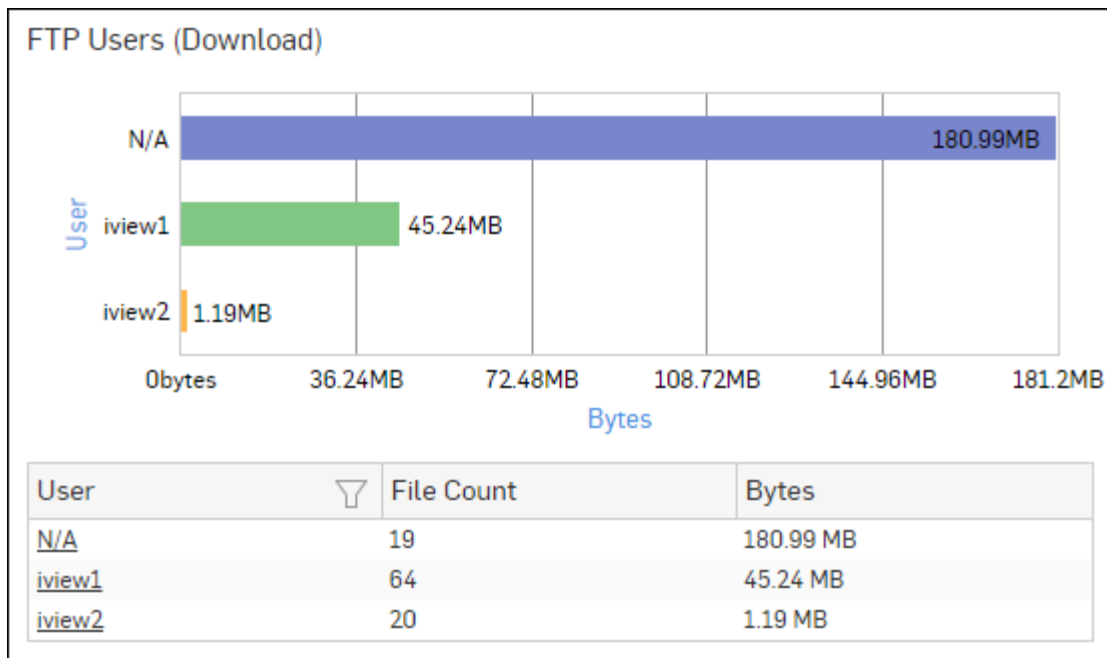


Figure 142: FTP Users(Download)

Click the User hyperlink in the table or graph to view the [Filtered FTP Usage Reports](#).

FTP Hosts (Upload)

This Report displays a list of the Hosts through which the maximum FTP uploaded traffic is generated with the number of files established to upload the data and the amount of data transferred.

View the report from FTP Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Usage > FTP Hosts (Upload)**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data uploaded by each host while the tabular report contains the following information:

- Host: Host IP Address through which the file is uploaded.
- File Count: Number of files uploaded per host.
- Bytes: Amount of data transferred.

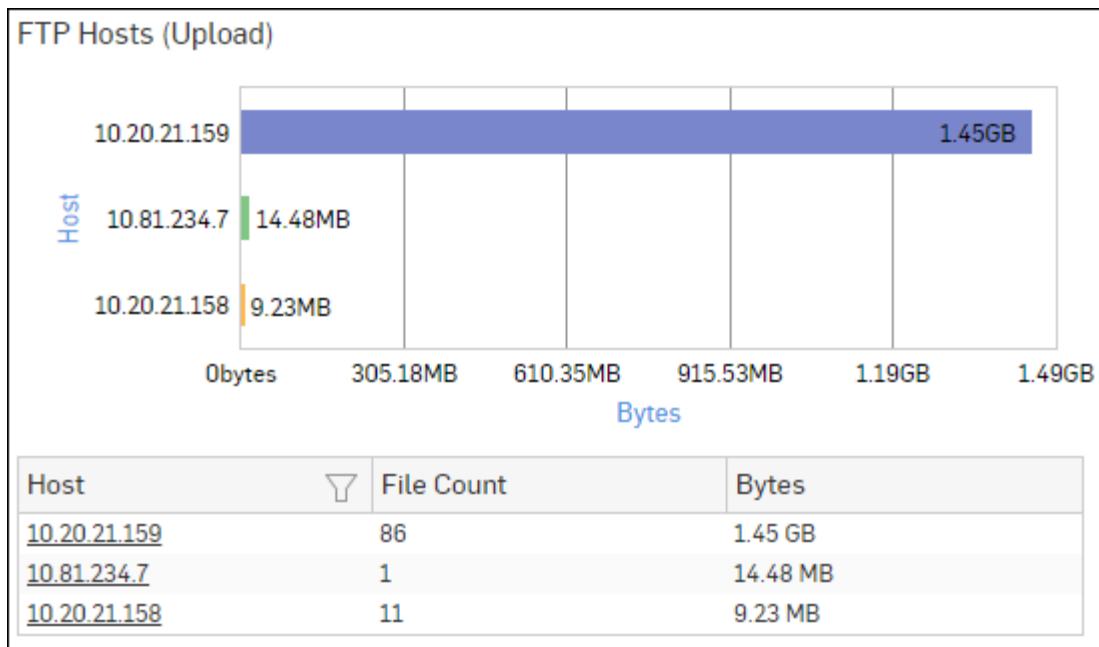


Figure 143: FTP Hosts(Upload)

Click the Host hyperlink in the table or graph to view the [Filtered FTP Usage Reports](#).

FTP Hosts (Download)

This Report displays the list of Hosts through which the maximum traffic is generated by downloading data through the FTP and the amount of data transferred.

View the report from FTP Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Usage > FTP Hosts (Download)**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data downloaded by each host while the tabular report contains the following information:

- Host: Host IP Address through which data is download.
- File Count: Number of files downloaded per host.
- Bytes: The amount of data transferred.

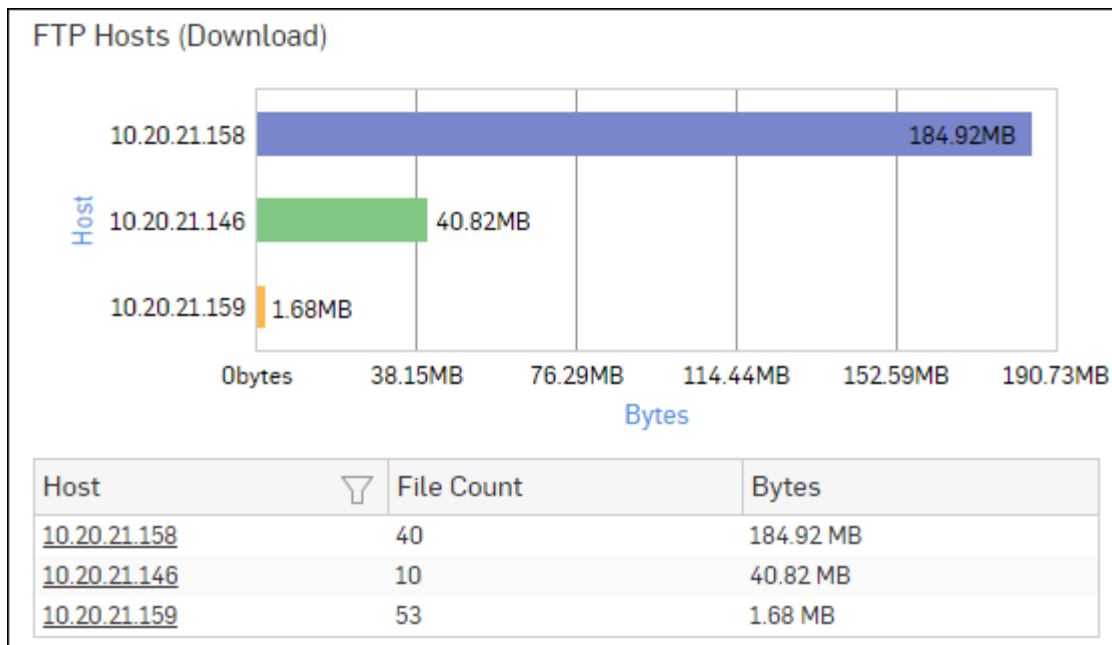


Figure 144: FTP Hosts(Download)

Click the Host hyperlink in the table or graph to view the [Filtered FTP Usage Reports](#).

FTP Servers

This Report displays the list of the Servers through which the most FTP traffic is generated along with the amount of data transferred.

View the report from FTP Usage reports dashboard or **Monitor & Analyze > Reports > Applications & Web > FTP Usage > FTP Servers**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred through each server while the tabular report contains the following information:

- Server: Server IP Address.
- File Count: Number of files uploaded to or downloaded from server.
- Bytes: The amount of data transferred.

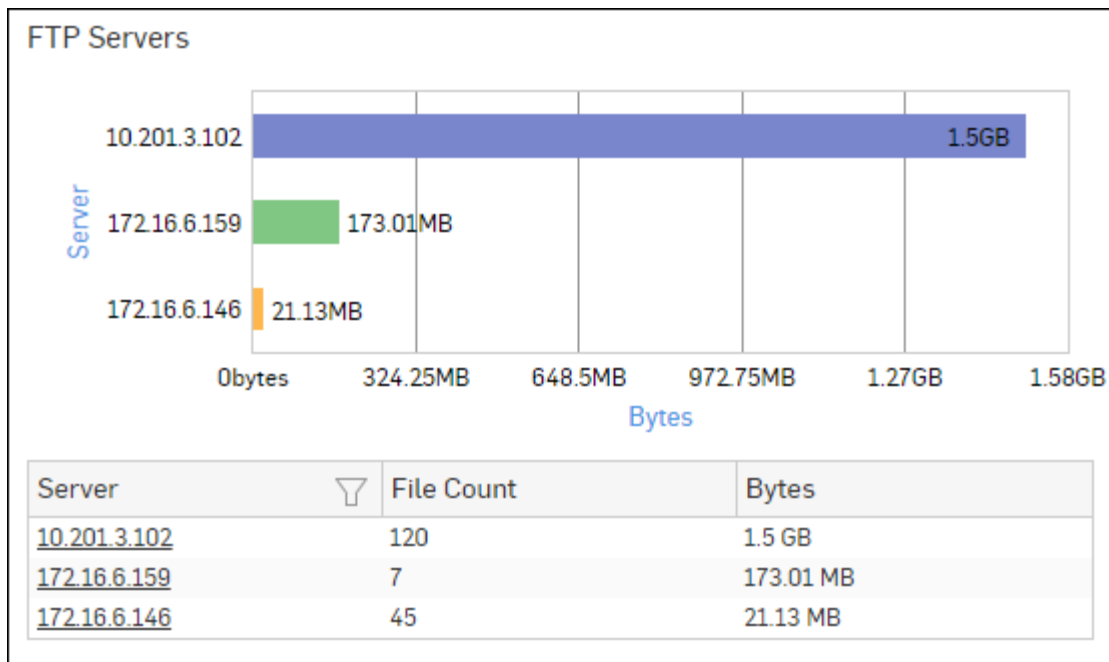


Figure 145: FTP Servers

Click the Server hyperlink in the table or graph to view the [Filtered FTP Usage Reports](#).

Filtered FTP Usage Reports

The FTP Usage Reports can be filtered to get the following set of FTP Usage reports.

- [Files Uploaded via FTP](#)
- [Files Downloaded via FTP](#)
- [FTP Users \(Upload\)](#)
- [FTP Users \(Download\)](#)
- [FTP Hosts \(Upload\)](#)
- [FTP Hosts \(Download\)](#)
- [FTP Servers](#)

To get filtered FTP Usage reports, you need to choose one of the following filter criteria:

- File from [Files Uploaded via FTP](#) Report
- File from [Files Downloaded via FTP](#) Report
- User from [FTP Users \(Upload\)](#) Report
- User from [FTP Users \(Download\)](#) Report
- Host from [FTP Hosts \(Upload\)](#) Report
- Host from [FTP Hosts \(Download\)](#) Report
- Server from [FTP Servers](#) Report

Based on the filter criterion, reports will be displayed in the following format.

- Summary - Reports in graphical format
- Details - Reports in tabular format

The Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered. Detailed Reports are displayed in a tabular format which can be filtered by clicking hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Files Uploaded via FTP widget

This Widget Report displays a list of Files Uploaded via the FTP along with the number of files and the amount of data uploaded for each file.



Note: This widget will not be displayed for filter criterion File (Upload).

The bar graph displays the amount of data uploaded per file while the tabular report contains the following information:

- File: Name of the uploaded file.
- File Count: Number of files uploaded.
- Bytes: The amount of data uploaded.

Files Downloaded via FTP widget

This Widget Report displays a list of Files Downloaded via the FTP along with the number of hits and the amount of data downloaded for each file.



Note: This widget will not be displayed for filter criterion File (Download).

The bar graph displays the amount of data downloaded per file while the tabular report contains the following information:

- File: Name of the downloaded file.
- File Count: Number of files downloaded.
- Bytes: Amount of data downloaded.

FTP Users (Upload) widget

This Widget Report displays a list of FTP users along with the amount of data uploaded by them.



Note: This widget will not be displayed for filter criterion User (Upload).

The bar graph displays the amount of data uploaded by the users while the tabular report contains the following information:

- Users: users who have uploaded the file.
- File Count: Number of files uploaded per user.
- Bytes: The amount of data uploaded.

FTP Users (Download) widget

This Widget Report displays a list of FTP users along with the amount of data downloaded by them.



Note: This widget will not be displayed for filter criterion User (Download).

The bar graph displays the amount of data downloaded by the users while the tabular report contains the following information:

- Users: Username of the users who have downloaded the file.
- File Count: Number of files downloaded per user.
- Bytes: Amount of data downloaded.

FTP Hosts (Upload) widget

This Widget Report displays the amount of data uploaded through each Host.



Note: This widget will not be displayed for filter criterion Host (Upload).

The bar graph displays the amount of data uploaded by each host while the tabular report contains the following information:

- Host: Hosts through which file is uploaded.
- File Count: Number of files uploaded per host.
- Bytes: Amount of data uploaded.

FTP Hosts (Download) widget

This Widget Report displays the amount of data uploaded through each Host.



Note: This widget will not be displayed for filter criterion ‘Host (Download)’.

The bar graph displays the amount of data downloaded by each host while the tabular report contains the following information:

- Host: Hosts through which file is downloaded.
- File Count: Number of files downloaded per host.
- Bytes: Amount of data downloaded.

FTP Servers widget

This Widget Report displays the amount of data transfer through each server.



Note: This widget will not be displayed for filter criterion Server.

The bar graph displays the amount of data transferred through server while the tabular report contains the following information:

- Server: IP Address of the FTP server.
- File Count: Number of files uploaded to or downloaded from server.
- Bytes: Amount of data downloaded.

FTP Protection

The FTP Protection reports dashboard consists of a collection of widgets displaying information regarding malicious FTP activities in your network.

View the report dashboard from **Monitor & Analyze > Reports > Applications & Web > FTP Protection**

The FTP Protection reports dashboard consists of following reports in widget form:

- [FTP Virus](#)
- [FTP Virus Directions](#)
- [Users - FTP Virus](#)
- [Servers - FTP Virus](#)
- [Hosts - FTP Virus](#)
- [Files- FTP Virus](#)

FTP Virus

This Report displays a list of the FTP viruses and number of counts per virus.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > FTP Virus**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per virus while the tabular report contains the following information:

- Virus: Name of the FTP virus.
- Count: Number of counts for the virus.

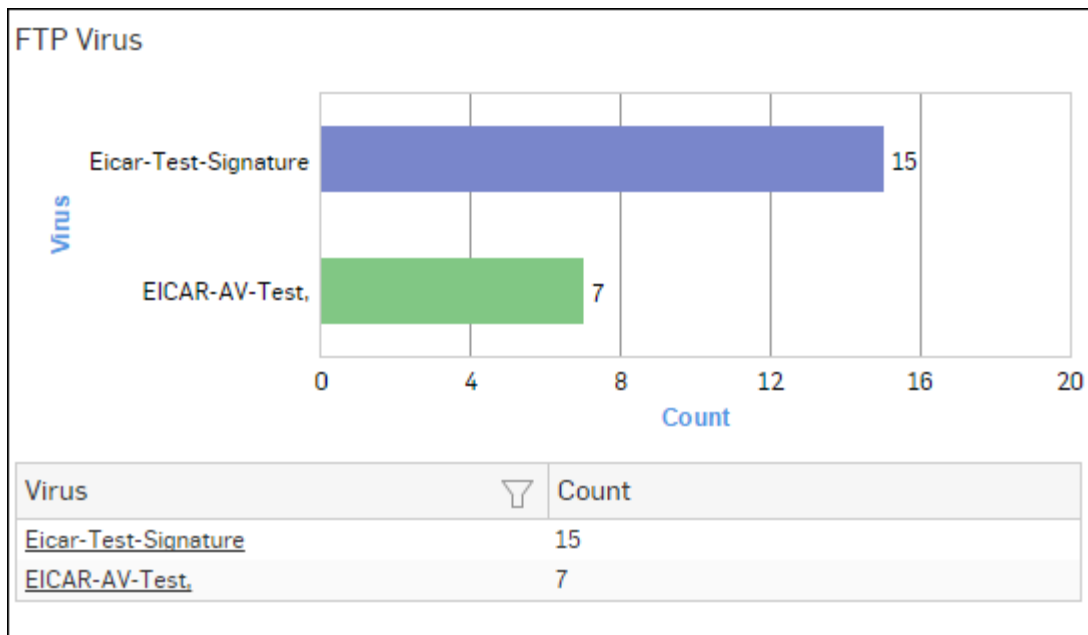


Figure 146: FTP Virus

Click the Virus hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

FTP Virus Directions

This Report displays the virus direction along with number of counts.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > FTP Virus Directions**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per direction while the tabular report contains the following information:

- Direction: Direction of the FTP traffic. Possible directions:
 - Upload
 - Download
- Count: Number of virus occurrence.

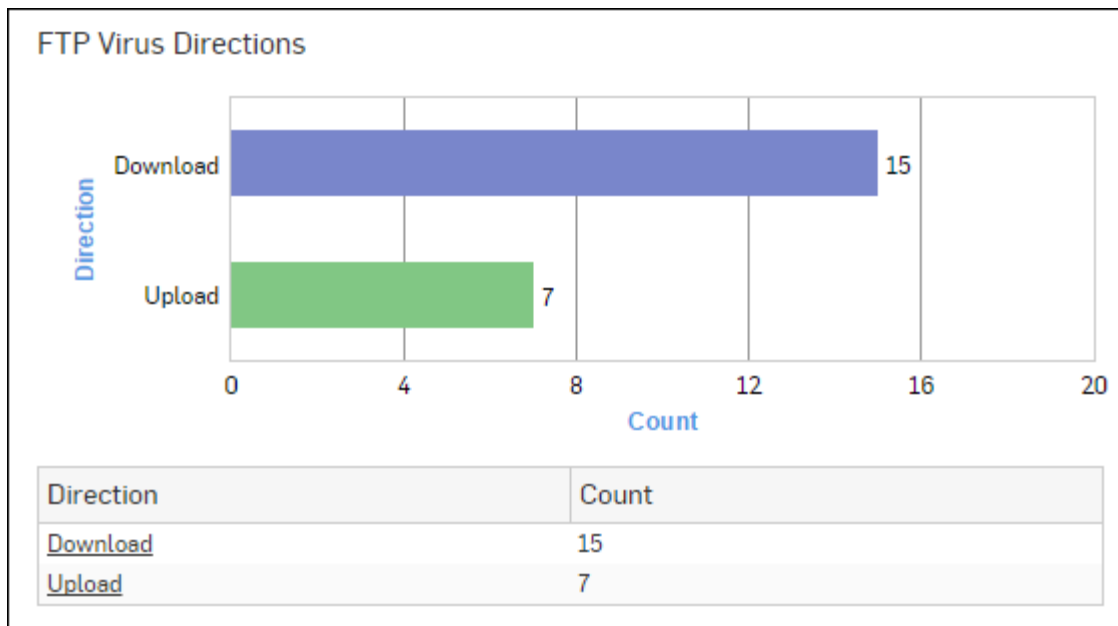


Figure 147: FTP Virus Directions

Click the Direction hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Users - FTP Virus

This Report displays a list of the FTP Users along with the number of virus counts.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > Users - FTP Virus**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per user while the tabular report contains the following information:

- User: Name of the user as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Count: Number of virus occurrence.

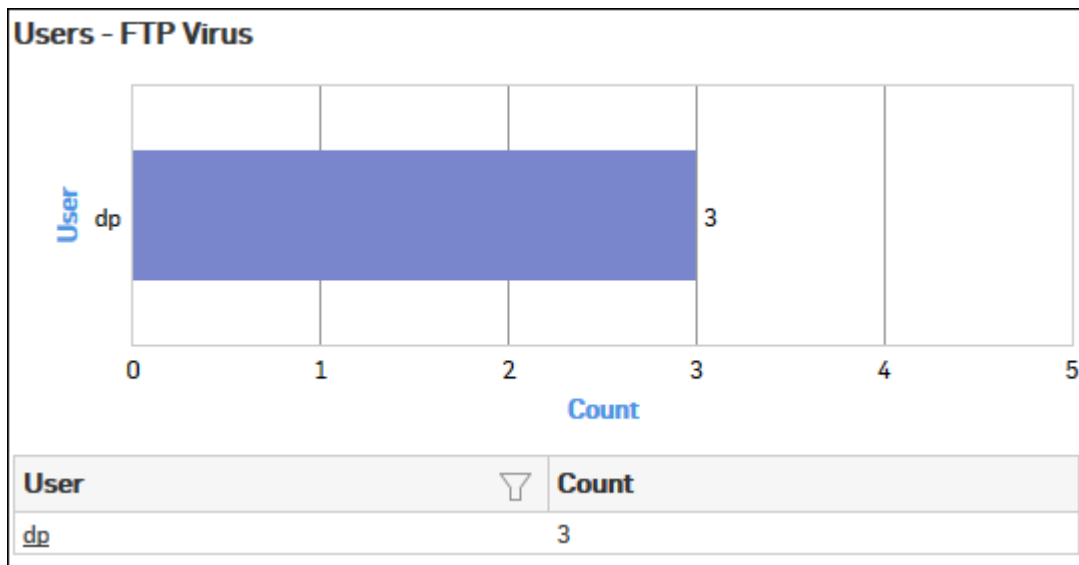


Figure 148: Users - FTP Virus

Click the User hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Servers - FTP Virus

This Report displays a list of FTP servers infected with viruses along with the number of virus counts per server.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > Servers - FTP Virus**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per FTP server while the tabular report contains the following information:

- Server: Name of the FTP server.
- Count: Number of virus occurrence.

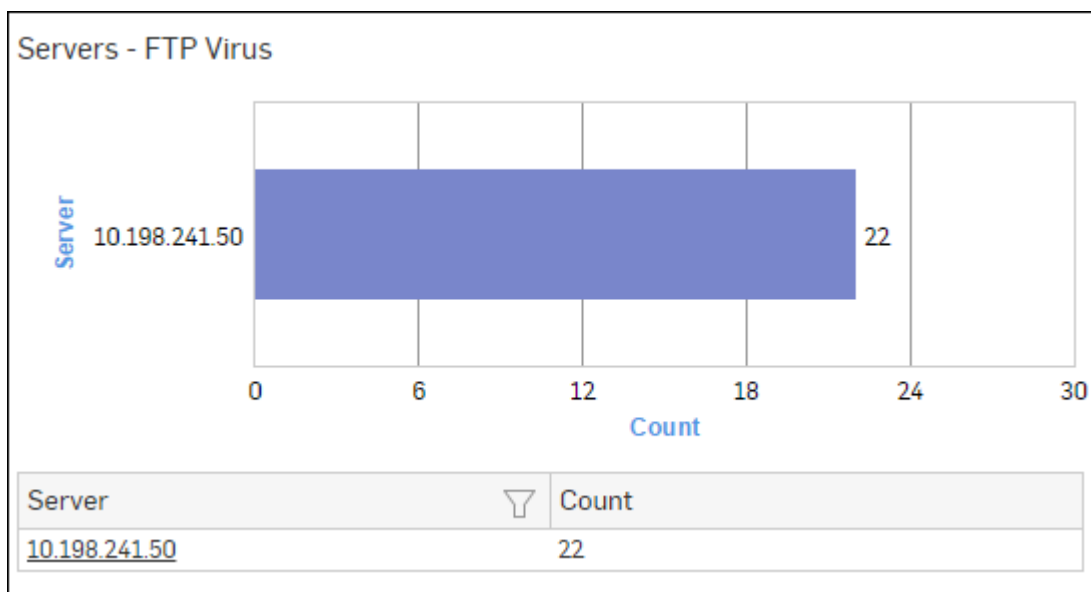


Figure 149: Servers - FTP Virus

Click the Server hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Hosts - FTP Virus

This Report displays a list of the FTP Hosts along with the number of virus counts per host.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > Hosts - FTP Virus**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per host while the tabular report contains the following information:

- Host: Name or IP Address of the host.
- Count: Number of virus occurrence.

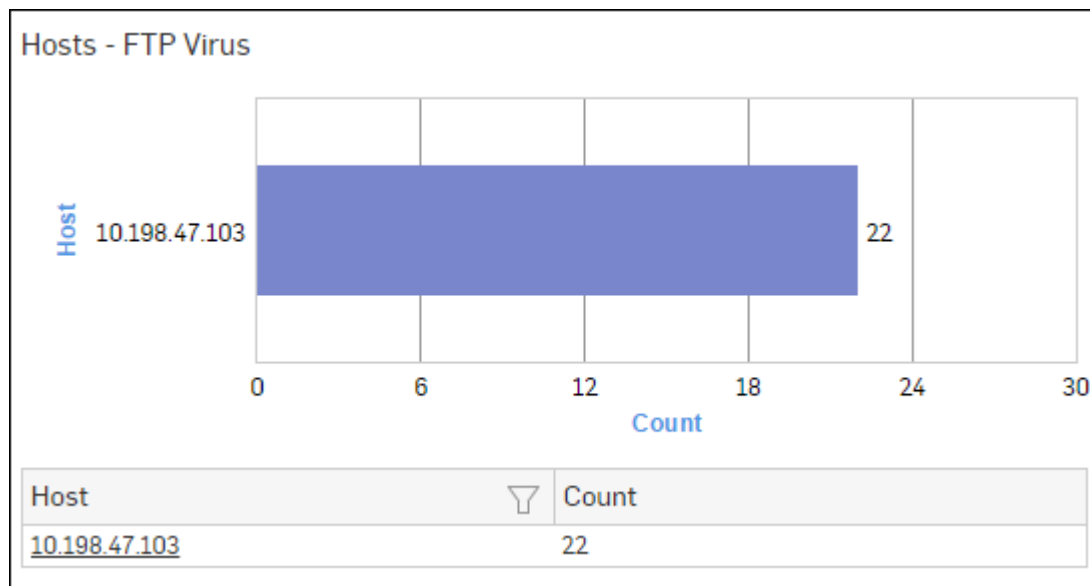


Figure 150: Hosts - FTP Virus

Click the Host hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Files- FTP Virus

This Report displays a list of virus infected files along with the number of counts per file

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > Files- FTP Virus**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per file while the tabular report contains the following information:

- File: Name of the virus infected file.
- Count: Number of virus occurrence.

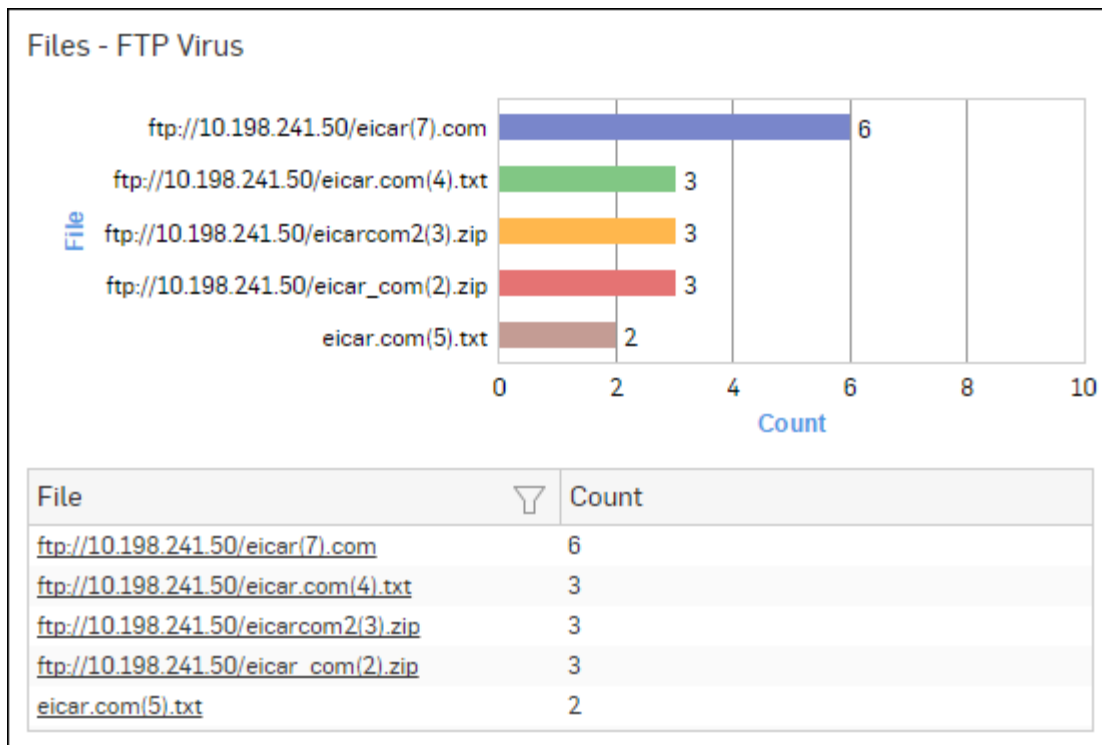


Figure 151: Files - FTP Virus

Click the File hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Filtered FTP Protection Reports

The FTP Protection Reports can be further filtered to get granular reports.

The FTP Protection Reports can be filtered to get the following set of reports:

- [FTP Virus](#)
- [FTP Virus Directions](#)
- [Servers - FTP Virus](#)
- [Hosts - FTP Virus](#)
- [Users - FTP Virus](#)
- [Files- FTP Virus](#)

To get filtered FTP Viruses reports, you need to choose one of the following filter criteria:

- FTP Virus from [FTP Virus Report](#)
- Direction from [FTP Virus Directions Report](#)
- Server from [Servers - FTP Virus Report](#)
- Host from [Hosts - FTP Virus Report](#)
- User from [Users - FTP Virus Report](#)
- File from [Files- FTP Virus Report](#)

Based on the filter criterion, reports will be displayed in following formats.

- Summary - Reports in graphical format
- Details - Reports in tabular format

Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays report in graph as well as in tabular format which can again be filtered, while Detailed Reports are displayed in tabular format which can be filtered by clicking hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

FTP Virus widget

This Widget report displays a list of the FTP viruses and the number of virus counts per virus.



Note: This widget will not be displayed for filter criterion FTP Virus.

The bar graph displays the number of virus counts per virus while the tabular report contains the following information:

- Virus: Name of the FTP virus.
- Count: Number of counts for the virus.

FTP Virus Directions widget

This Report displays the virus directions with number of counts.



Note: This widget will not be displayed for filter criterion Direction.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of counts per direction while the tabular report contains the following information:

- Direction: Direction of the FTP traffic. Possible directions:
 - Upload
 - Download
- Count: Number of virus occurrence.

Servers - FTP Virus widget

This Report displays a list of the top FTP servers along with the number of virus counts.



Note: This widget will not be displayed for filter criterion Server.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of virus counts per FTP server while the tabular report contains the following information:

- Server: Name of the FTP server.
- Count: Number of virus occurrence.

Hosts - FTP Virus widget

This Report displays a list of the top FTP hosts along with the number of virus counts.



Note: This widget will not be displayed for filter criterion Host.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of virus counts per host while the tabular report contains the following information:

- Host: Name or IP Address of the host.
- Count: Number of virus occurrence.

Users - FTP Virus widget

This Report displays a list of the FTP Users along with the number of virus counts.



Note: This widget will not be displayed for filter criterion User.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of virus counts per user while the tabular report contains the following information:

- User: Name of the user as defined in the Device. If the User is not defined then it will display 'unidentified' which means the traffic is generated by an unauthenticated or a clientless user.
- Count: Number of virus occurrence.

Files- FTP Virus widget

This Report displays a list of Files along with the number of virus counts.



Note: This widget will not be displayed for filter criterion File.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of virus counts per file while the tabular report contains the following information:

- File: Name of the infected file.
- Count: Number of virus occurrence.

Network & Threats

Network & Threats section provides an in-depth insight into Network usage and threats associated with your network.



Note: Network Protection subscription is required to view all the Network & Threats reports. Without a valid subscription, some reports do not show any data. The Network & Threats sub-sections can be accessed by selecting drop-down 1 given at the upper left corner of the page.

The section includes following reports:

- [Intrusion Attacks](#)
- [Advanced Threat Protection](#)
- [Wireless](#)
- [Security Heartbeat](#)
- [Sandstorm](#) on page 214

Intrusion Attacks

Intrusion Attacks reports dashboard provide an insight of the attack attempts in your network.

The reports provide complete statistics about the attacks and attackers with concise reports on victims and applications through which the attack was launched.

These reports can facilitate an administrator in determining the severity of the attack and thus provides the basis for fine tuning the intrusion prevention policies.

View the Attacks reports dashboard from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks**.

It enables to view the break up for various attacks as:

- [Attack Categories](#)
- [Attacked Platforms](#)
- [Attack Targets](#)
- [Severity wise Attacks](#)
- [Intrusion Attacks](#)
- [Attacks detected and allowed](#)
- [Intrusion Source](#)
- [Intrusion Destination](#)
- [Users](#)
- [Applications used for Attacks](#)
- [Source Countries](#)
- [Trend - Intrusion Attacks](#)

Attack Categories

The report enables to view the details of the Top Attack Categories along with number of hits per category.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Attack Categories**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits per attack category, while the tabular report contains the following information:

- Category: Name of the attack category as defined in the Device. If the attack category is not defined in the Device then this field displays 'Uncategorized' which means the blocked attack is uncategorized type.
- Hits: Number of hits for the attack category.

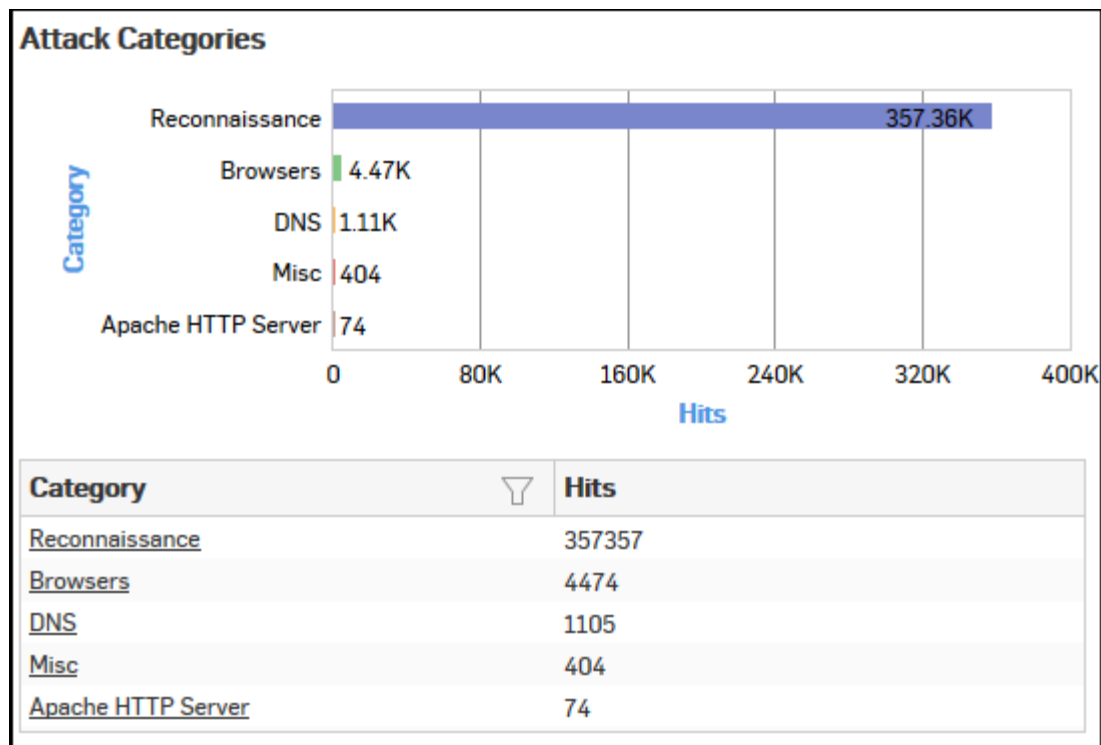


Figure 152: Attack Categories

Click the Category hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Attacked Platforms

The Report displays a list of the Attacked Platforms along with the number of hits to the platform.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Attacked Platforms**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the name of the attacked platform and number of hits while the tabular report contains the following information:

- Platform: Name of the attacked platform as defined in the Device. If the platform is not defined in the Device then this field displays 'Unknown' which means the platform of blocked attack is uncategorized.

Hits: Number of hits for the attack platform.

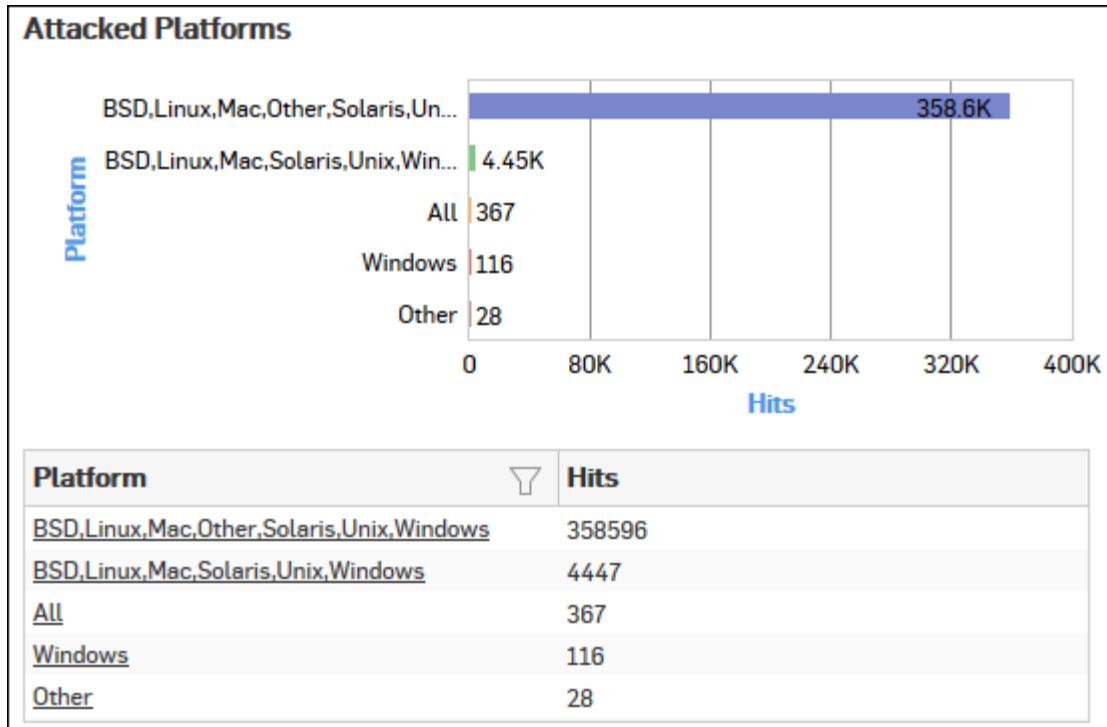


Figure 153: Attacked Platforms

Click Platform hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Attack Targets

The Report displays the list of Top Targets along with number of hits to the target.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Attack Targets**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the type of attack target and the number of hits while tabular report contains the following information:

- Target: Displays target type. Possible target types:
 - Client
 - Server
 - Client-Server
- Hits: Number of hits for target.

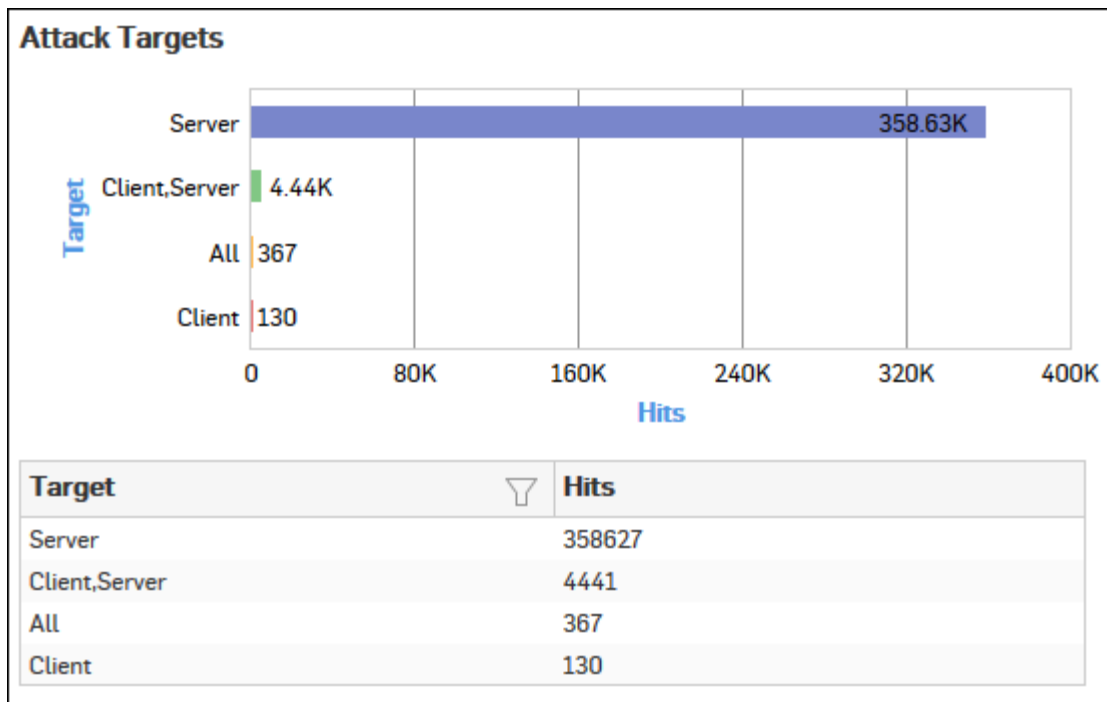


Figure 154: Attack Targets

Click the Target hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Severity wise Attacks

The Report enables to view the severity of the attack that has hit the system and gives a detailed disintegration of the attacks, attackers, victims and applications through individual reports under severity.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Severity wise Attacks**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each severity, while the tabular report contains the following information:

- Severity: Severity level of the attack attempt. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION – Informational
 - DEBUG - Debug level messages
- Hits: Number of hits under each severity.

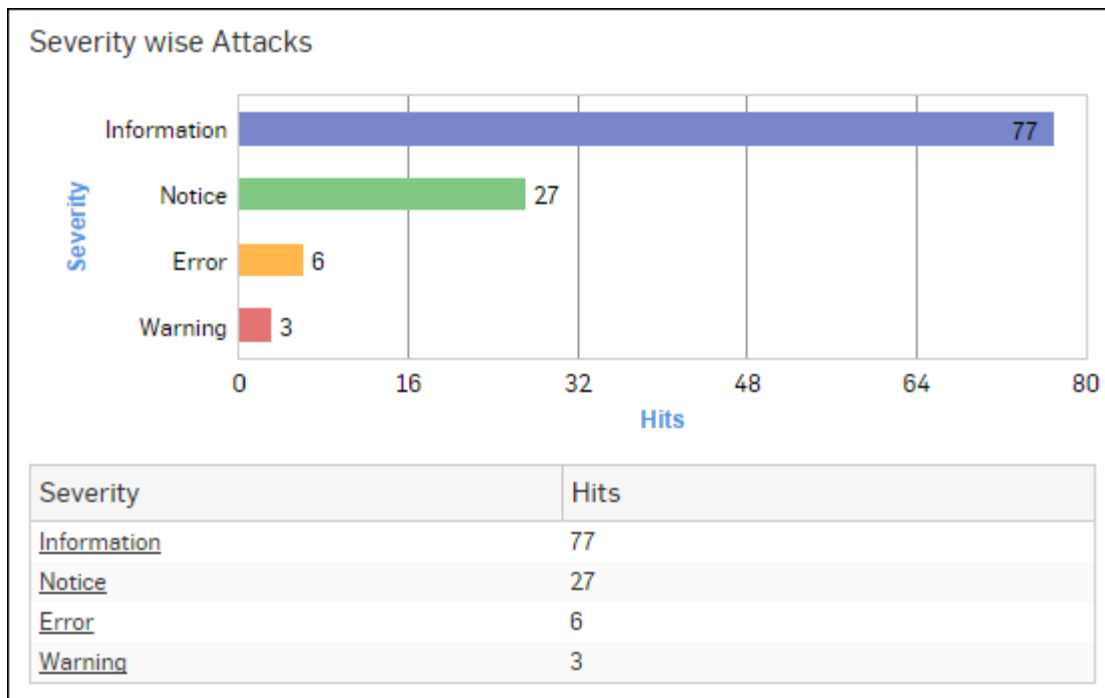


Figure 155: Severity wise Attacks

Click the Severity hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Attacks

The Report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Attacks**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Attacks** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each attack, while the tabular report contains the following information:

- Attack: Name of the attack launched.
- Hits: Number of hits for each attack.

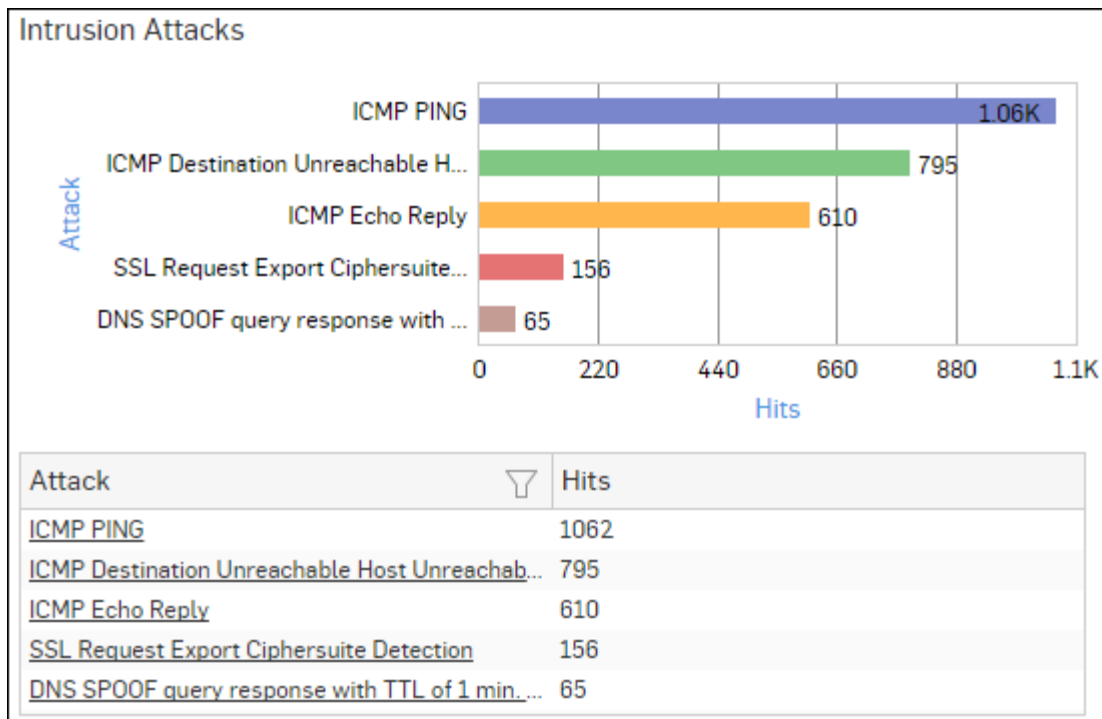


Figure 156: Intrusion Attacks

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Attacks detected and allowed

The Report lists the attacks identified by the Device and yet allowed to pass through the network.



Note: The prime reason why an attack packet is allowed to pass through the network is because action for the relevant IPS signature is set to Allow in the Device. To prevent the attack packet from passing through the network, change the action to Block.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Attacks detected and allowed**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each detected attack, while the tabular report contains the following information:

- Attack: Name of the attack identified and allowed by the Device.
- Hits: Number of hits for each attack.

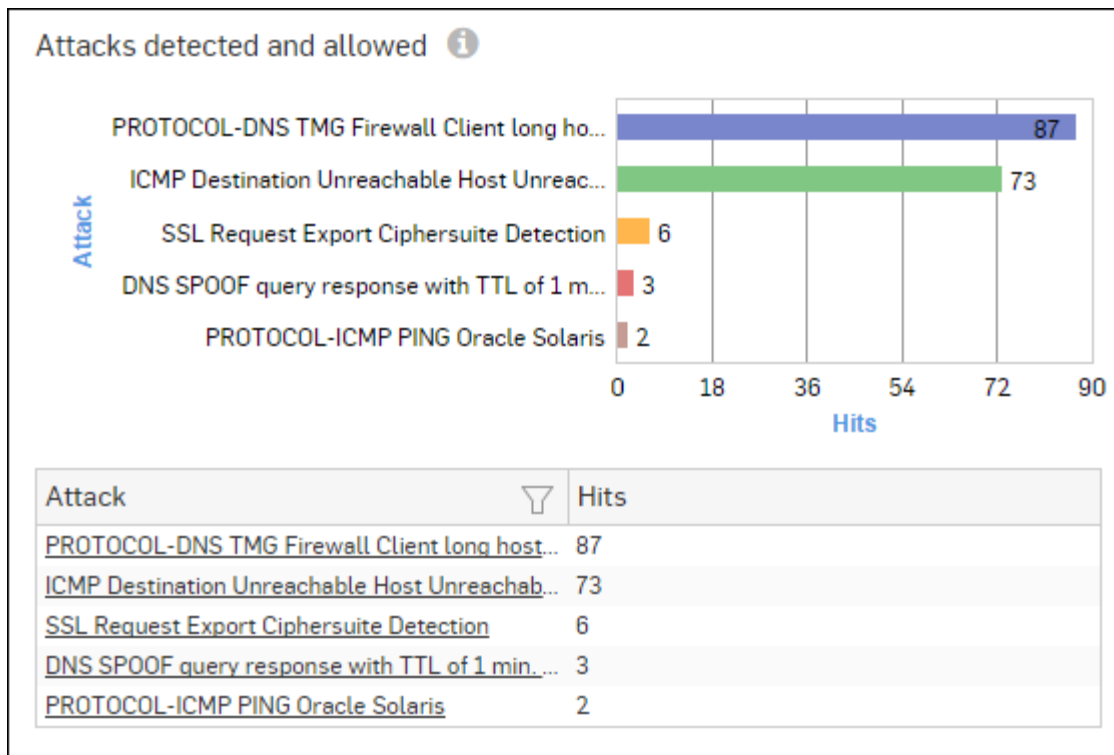


Figure 157: Attacks detected and allowed

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Source

The Report enables to view the details of the attacker(s) who have hit the system and gives the detailed disintegration of attacks, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Source**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Source** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each attacker, while the tabular report contains the following information:

- Attacker: IP Address of the attacker.
- Hits: Number of hits for each attacker.

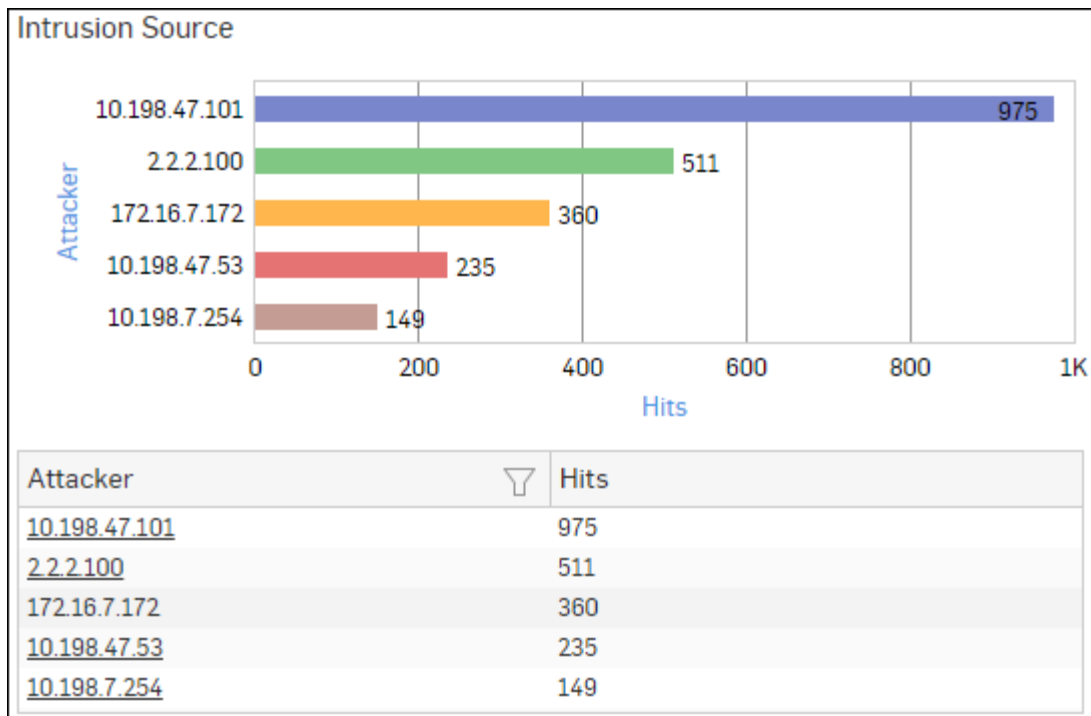


Figure 158: Intrusion Source

Click Attacker hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Destination

The Report enables to view the details of the victims who have hit the system unknowingly and gives the detailed disintegration of attacks, attackers and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Destination**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each victim, while the tabular report contains following information:

- Victim: IP Address of the victim.
- Hits: Number of hits for each victim.

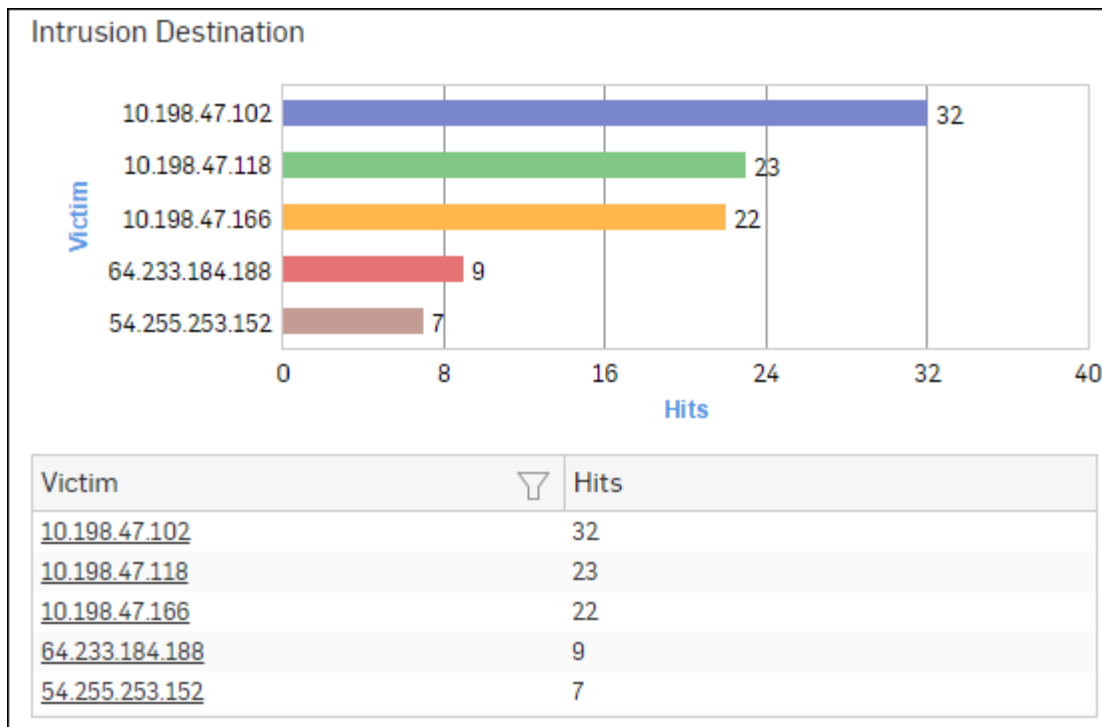


Figure 159: Intrusion Destination

Click Victim hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Users

The report enables to view the details of the users and gives the detailed disintegration of attacks, attackers and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Users**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits per user while tabular report contains following information:

- User: User name as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Hits: Number of hits for the user.

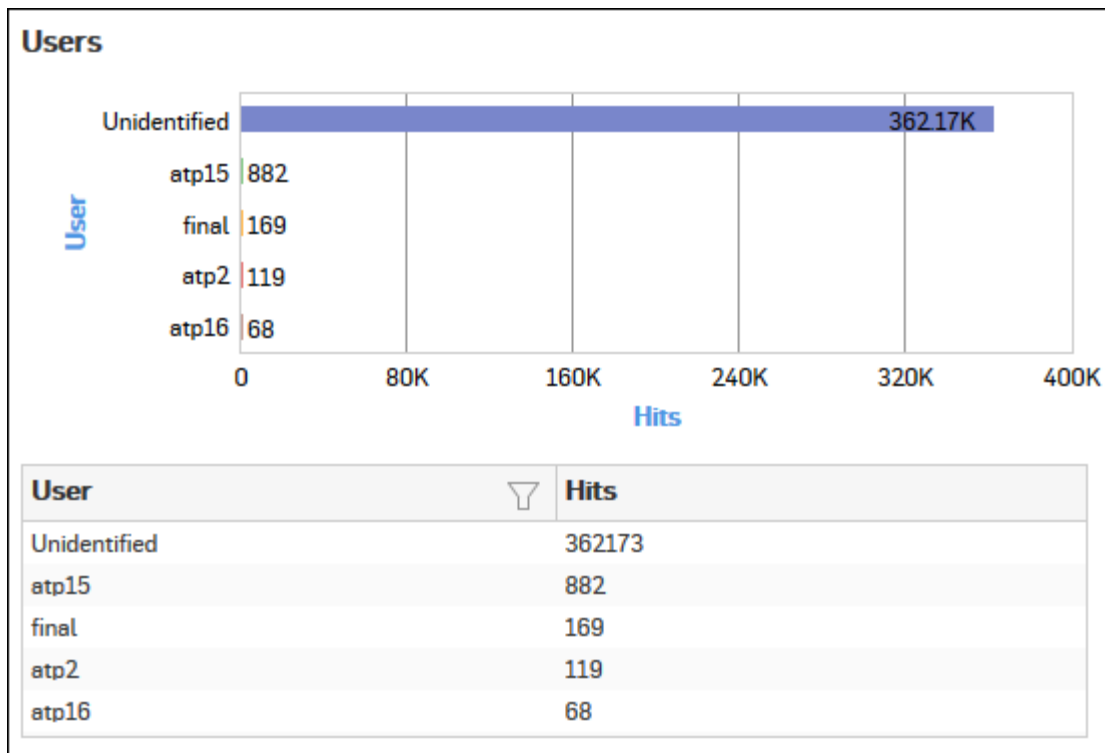


Figure 160: Users

Click the User hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Applications used for Attacks

The report enables to view details of the applications used for attacks that have hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Applications used for Attacks**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under for each application, while the tabular report contains the following information:

- Application/Proto:Port: Name of the application under attack.
- Hits: Number of hits for each application.

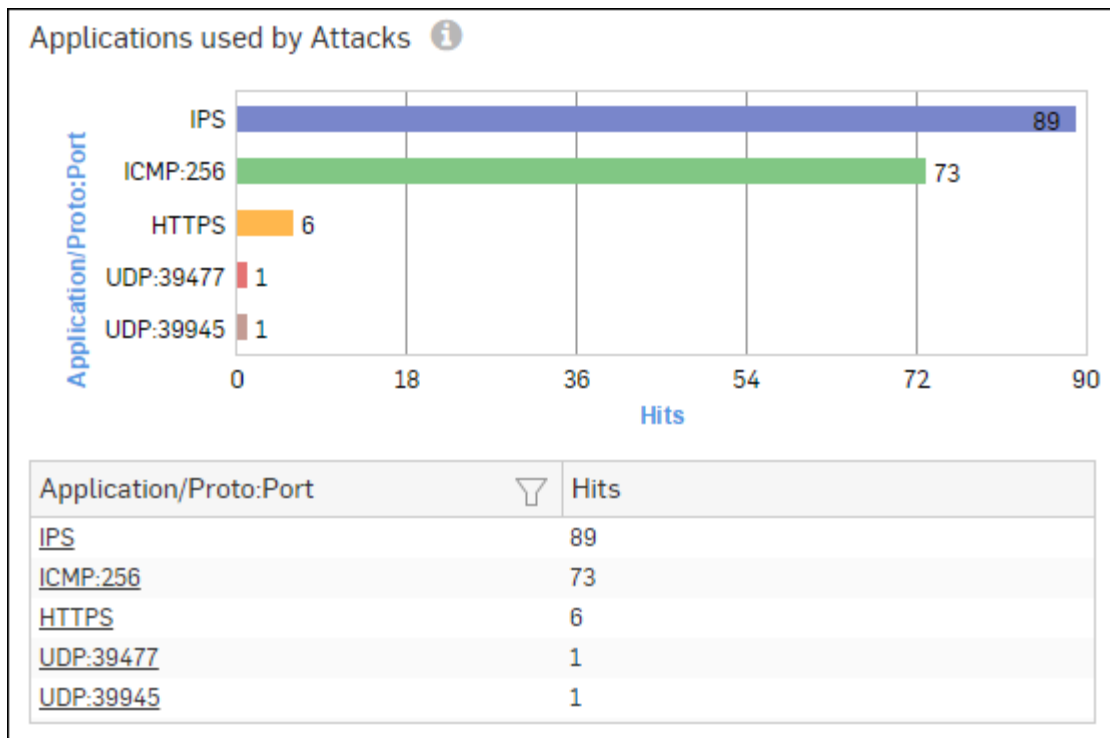


Figure 161: Applications used for Attacks

Click the Application hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Source Countries

This Report displays a list of countries from where the maximum number of intrusion attacks are generated along with number of hits per country.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Source Countries**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each country, while tabular report contains following information:

- Source Country: Name of the country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits for each country.

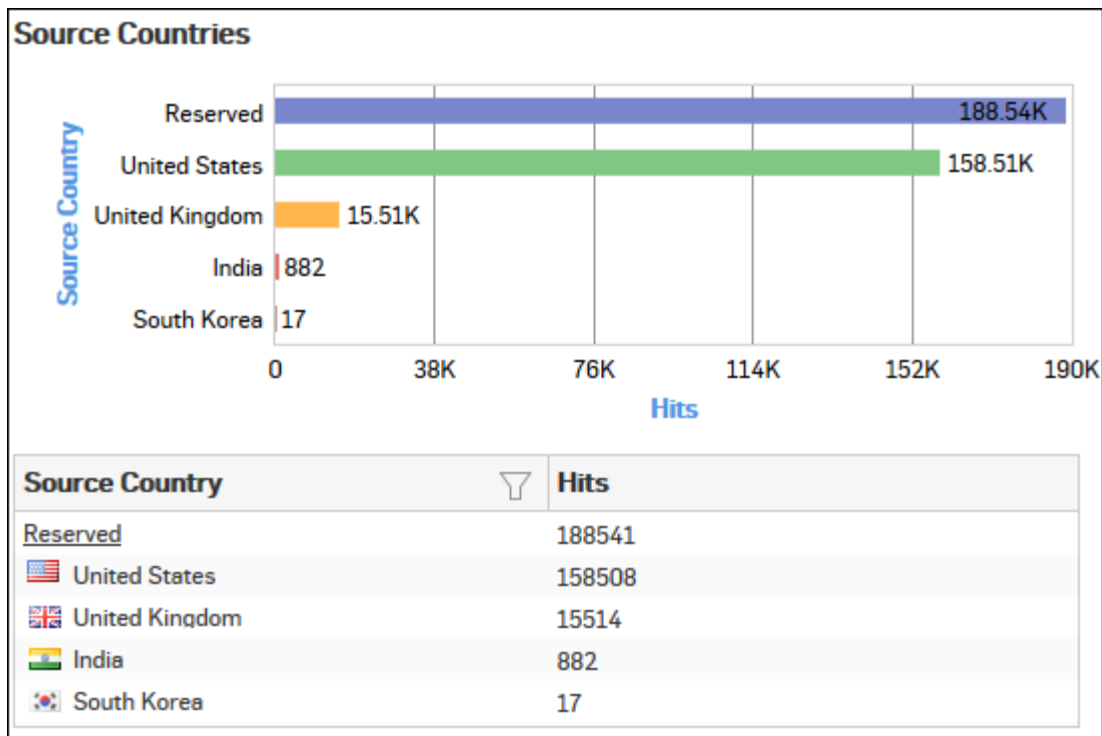


Figure 162: Source Countries

Click the Source Country hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Trend - Intrusion Attacks

The Report provides an overview of IPS trends observed in the network during the selected time period.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Trend - Intrusion Attacks**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of hits under each detected attack, while the tabular report contains the following information:

- Time: Time of the event in YYYY:MM:DD HH:MM:SS format.
- Event Type: Name of the event type.
- Event: Number of occurrence of the event per time period.

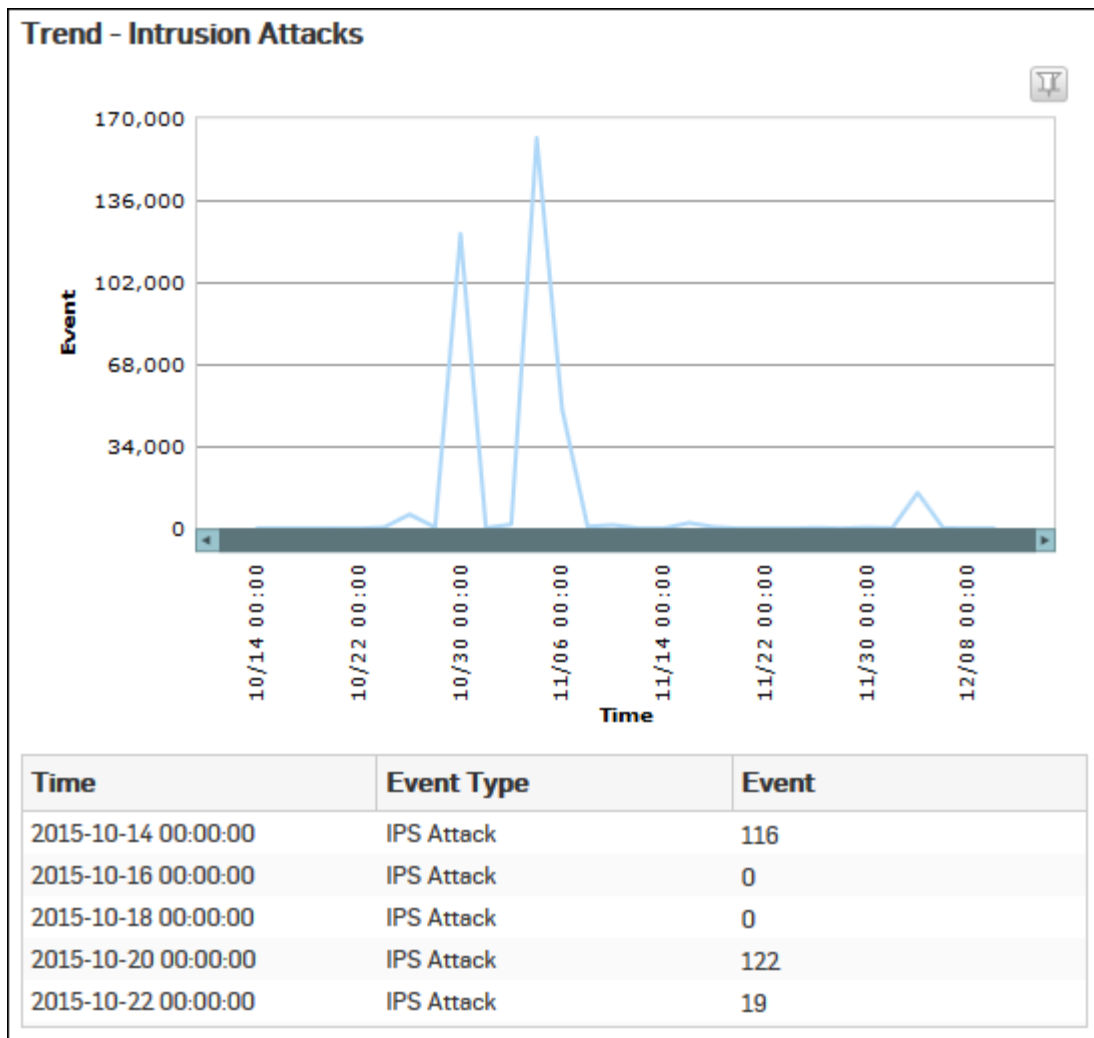


Figure 163: Trend - Intrusion Attacks

Filtered Intrusion Attacks Reports

The Intrusion Attacks Reports can be filtered to get the filtered Intrusion Attacks reports.

Filtered Intrusion Attacks Reports has following set of reports:

- [Attack Categories](#)
- [Attacked Platforms](#)
- [Attack Targets](#)
- [Severity wise Attacks](#)
- [Intrusion Attacks](#)
- [Attacks detected and allowed](#)
- [Intrusion Source](#)
- [Intrusion Destination](#)
- [Users](#)
- [Applications used for Attacks](#)
- [Source Countries](#)

To get the filtered Intrusion Attacks reports, you need to choose one of the following filter criteria:

- Category from [Attack Categories Report](#)
- Platform from [Attacked Platforms Report](#)

- Target from [Attack Targets Report](#)
- Severity from [Severity wise break-down Report](#)
- Attack from [Intrusion Attacks Report](#)
- Attack from [Attacks detected and allowed Report](#)
- Attacker from [Intrusion Sources Report](#)
- Victim from [Intrusion Destinations Report](#)
- User from [Users Report](#)
- Application from [Applications used for Attacks Report](#)
- Country from [Source Countries Report](#)

Filtered Reports consist of multiple report widgets. Each widget displays the report in graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Attack Categories widget

This Widget Report displays a list of Attack Categories along with number of hits to the category.



Note: This widget will not be displayed for the filter criterion Category.

The bar graph displays the name of attack category and number of hits while tabular report contains following information:

- Category: Name of the attack category as defined in the Device. If the attack category is not defined in the Device then this field displays 'Uncategorized' which means the blocked attack is uncategorized type.
- Hits: Number of hits for the attack category.

Attacked Platforms widget

This Widget Report displays a list of Attacked Platforms along with the number of hits to the platform.



Note: This widget will not be displayed for the filter criterion Platform.

The bar graph displays the name of the attack platform and the number of hits while the tabular report contains the following information:

- Platform: Name of the attack platform as defined in the Device. If the platform is not defined in the Device then this field displays 'Unknown' which means the platform of blocked attack is uncategorized.
- Hits: Number of hits for the attack category.

Attack Targets widget

This Widget Report displays target type wise number of hits.



Note: This widget will not be displayed for the filter criterion Target.

The bar graph displays the type of attack target and the number of hits while the tabular report contains the following information:

- Target: Displays target type. Possible target types:
 - Client
 - Server
 - Client-Server
- Hits: Number of hits for target.

Severity wise Attacks widget

The Severity wise break-down Report enables to view the severity level of the attack and the number of hits for the severity level.



Note: This widget will not be displayed for the filter criterion Severity.

The Report is displayed as a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each severity, while the tabular report contains the following information:

- Severity: Severity level of the attack attempt.
- Hits: Number of hits for each severity level.

Intrusion Attacks widget

This Widget Report displays the number of hits for every intrusion attack.



Note: This widget will not be displayed for the filter criterion Attack.

The bar graph displays the type of attack while the tabular report contains the following information:

- Attack: Name of the intrusion attack.
- Hits: Number of hits for the attack.

Attacks detected and allowed widget

The Report lists the attacks identified by the Device and yet allowed to pass through the network.



Note: This widget will not be displayed for the filter criterion Attack.



Note: The prime reason why an attack packet is allowed to pass through the network is because action for the relevant IPS signature is set to Allow in the Device. To prevent the attack packet from passing through the network, change the action to Block.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of hits under each detected attack, while the tabular report contains the following information:

- Attack: Name of the attack identified and allowed by the Device.
- Hits: Number of hits for each attack.

Intrusion Source widget

This Widget Report displays a list of the Attackers and the number of hits for every attacker.



Note: This widget will not be displayed for the filter criterion Attacker.

The bar graph displays the IP Address of the attacker, while the tabular report contains the following information:

- Attacker: IP Address of the attacker.
- Hits: Number of hits by the attacker.

Intrusion Destination widget

This Widget Report displays a list of victims and the number of hits for every victim.



Note: This widget will not be displayed for the filter criterion Victim.

The bar graph displays the IP Address of the victim, while the tabular report the contains following information:

- Victim: IP Address of the victim.
- Hits: Number of hits per victim.

Users widget

This Report displays a list of the Top Users along with the number of hits to the user.



Note: This widget will not be displayed for the filter criterion User.

The Report is displayed as graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits per user while the tabular report contains the following information:

- User: User name as defined in the Device. If the User is not defined in the Device then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Hits: Number of hits for the user.

Applications used for Attacks widget

This Widget report displays a list of the Top Applications and number of hits for every application.



Note: This widget will not be displayed for the filter criterion Application.

The bar graph displays the name of the application under attack, while the tabular report contains the following information:

- Application/Proto:Port: Name of the application as defined in the Device.
- Hits: Number of hits for the application.

Source Countries widget

This widget displays a list of countries from where the maximum number of intrusion attacks are generated along with number of hits per country.



Note: This widget will not be displayed for the filter criterion Source Country.

This Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits per country while the tabular report contains the following information:

- Source Country: Name of attacker country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Hits: Number of hits for the country.

Advanced Threat Protection

Advanced Threat Protection (ATP) reports dashboard provide a snapshot of advanced threats in your network. It helps to identify clients/hosts within your network that are infected or part of botnet.

ATP analyzes network traffic, e.g., DNS requests, HTTP requests, or data packets in general, coming from and going to all networks for possible threats. The database used to identify threats is updated constantly by a CnC/Botnet data feed from Sophos Labs through signature updates.

Based on this data, the ATP reports can help administrators to quickly identify infected hosts and their communication with command-and-control (CnC) servers. This in turn, provides a basis for fine-tuning the configuration to efficiently control network traffic flow.

View the ATP reports dashboard from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection**.

ATP reports dashboard enable viewing of traffic generated by:

- [Hosts - ATP](#)
- [Advanced Threats](#)
- [Users - ATP](#)
- [Origins](#)
- [Trend - ATP Events](#)
- [Threat Destinations](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)
- [Suspicious Executable](#)

Hosts - ATP

This report displays a comprehensive summary of host wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Hosts-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Hosts-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of events per host while the tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Threat Count: Number of threats per source host.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

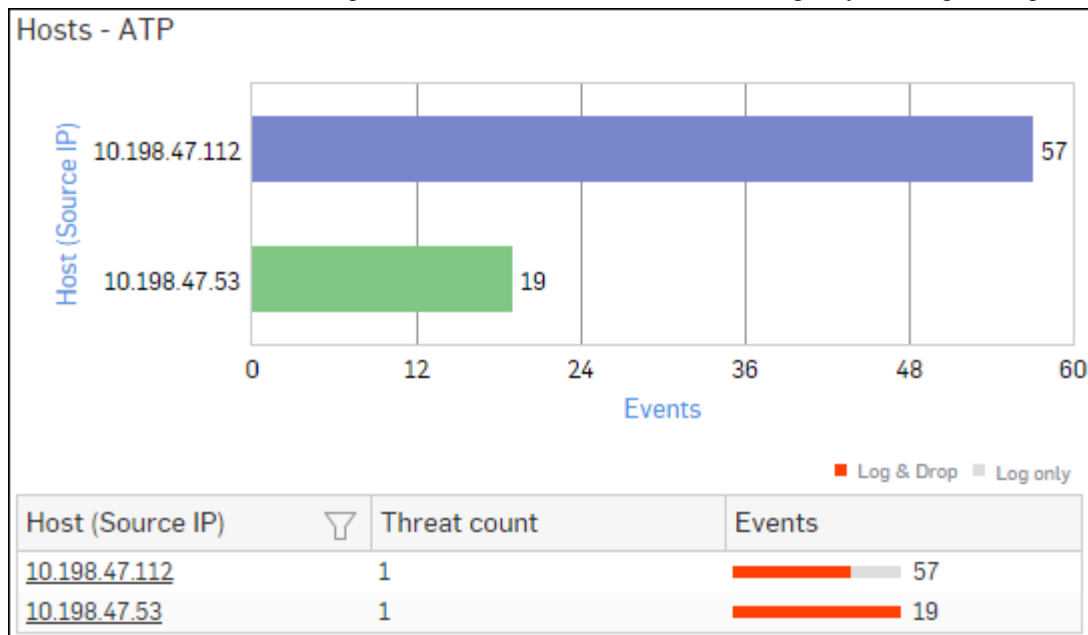


Figure 164: Hosts - ATP

Click Host hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Advanced Threats

This report displays a comprehensive summary of advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Advanced Threats**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Advanced Threats** as well.

The report is displayed using a graph as well as in a tabular format.

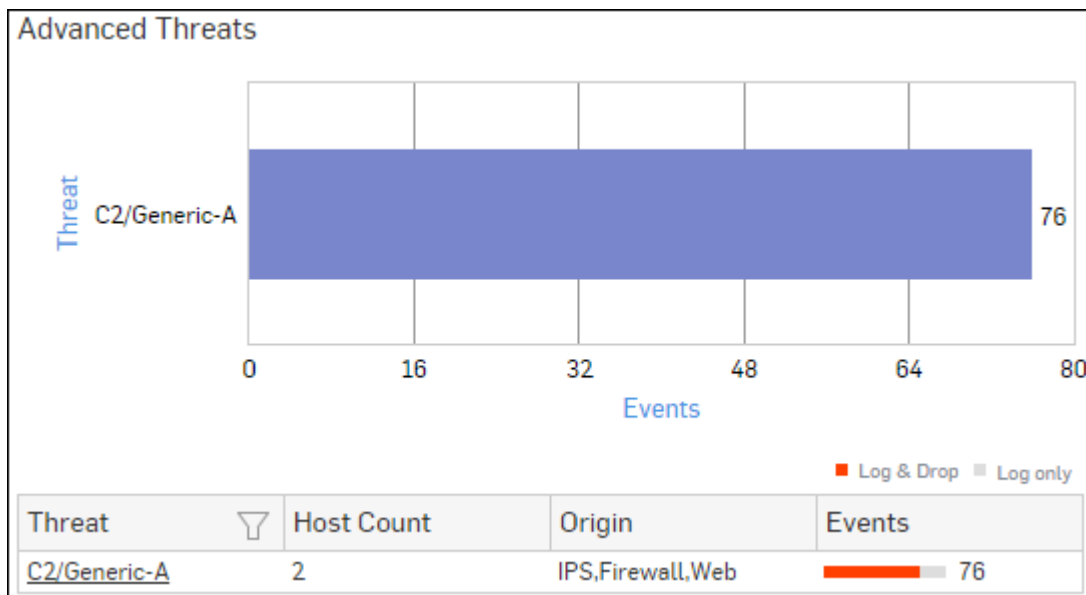
By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of threats along with total number of events per threat while the tabular report contains the following information:

- Threat: Name of the threat.
- Host Count: Number of hosts infected with the threat.

- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Events: Total number of events per threat. The number is summation of Log only and Log & Drop events.

Figure 165: Advanced Threats



Click Threat hyperlink in the table or graph to view the [Filtered ATP Reports](#).

Users - ATP

This report displays a comprehensive summary of user wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Users-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Users-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with total number of events per user while the tabular report contains the following information:

- User: User name of the infected user.
- Host Count: Number of hosts per user.
- Threat Count: Number of threats per user.
- Events: Total number of events per user. The number is summation of Log only and Log & Drop events.

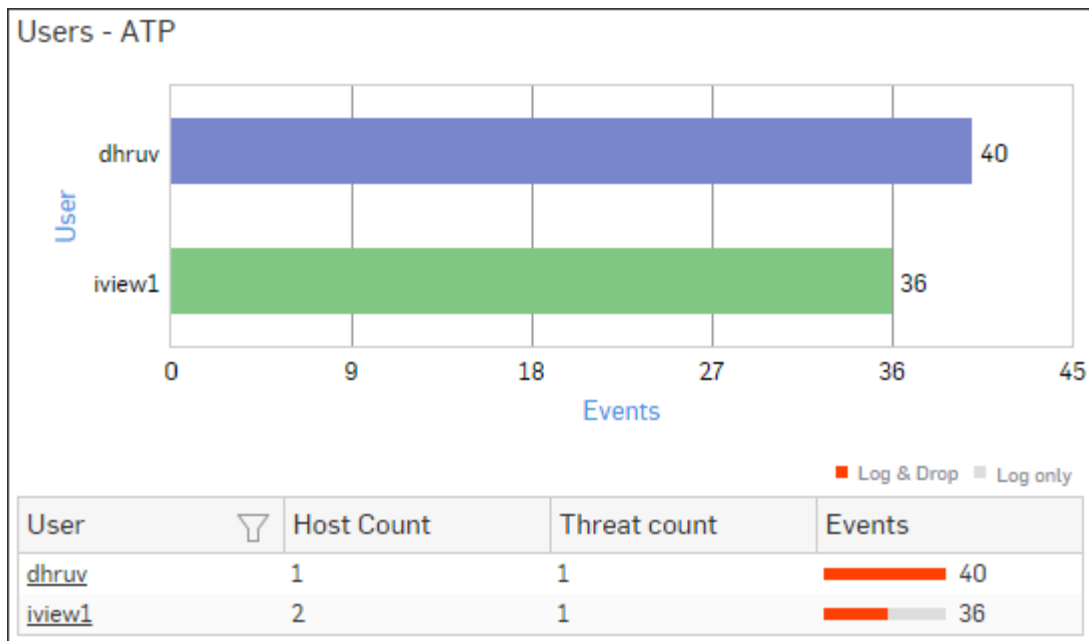


Figure 166: Users - ATP

Click User hyperlink in the table or graph to view the [Filtered ATP Reports](#).

Origins

This report displays a comprehensive summary of origins associated with advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Origins**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of origins along with total number of events per origin while the tabular report contains the following information:

- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Host Count: Number of hosts per origin type.
- Threat Count: Number of threats per origin type.
- Events: Total number of events per origin type. The number is summation of Log only and Log & Drop events.

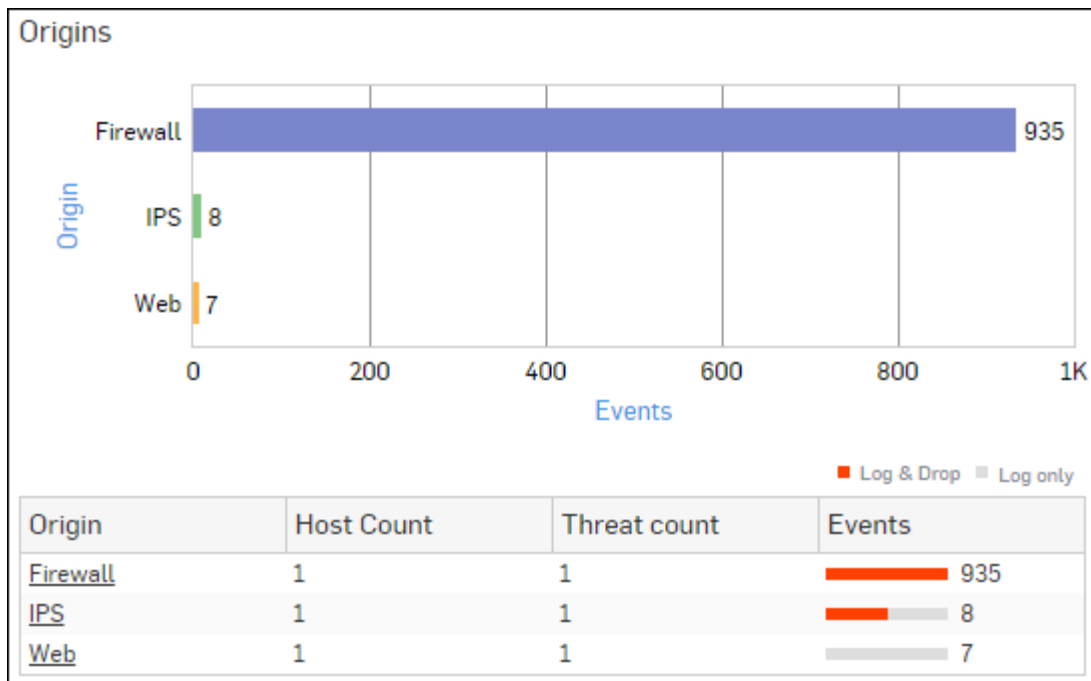


Figure 167: Origins

Click Origin hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Trend - ATP Events

This report displays a comprehensive summary of date wise advanced threats in your network. The report helps an administrator to understand the infection trend, i.e. if it is increasing / reducing or stable over time.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Trend - ATP Events**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.



Note: Report lists only those dates on which a threat has been detected.

The bar graph displays total number of events per day while the tabular report contains the following information:

- Date: Date in YYYY-MM-DD HH:MM:SS format.
- Events: Total number of events per day. The number is summation of Log only and Log & Drop events.

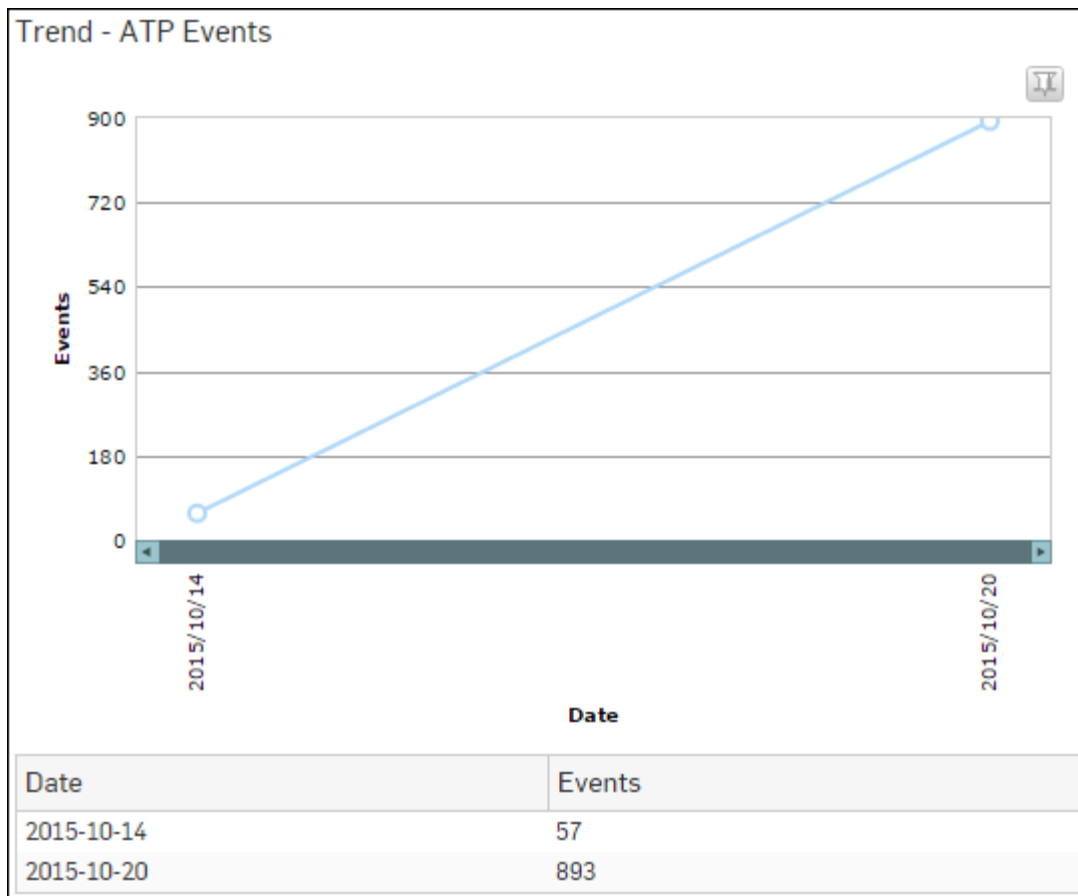


Figure 168: Trend - ATP Events

Threat Destinations

This report displays a comprehensive summary of destination wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Threat Destinations**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of threat destinations along with number of events per destination while the tabular report contains the following information:

- Threat URL/IP: IP Address of the infected destination.
- Host Count: Number of hosts per destination.
- Threat Count: Number of threats per destination.
- Events: Total number of events per destination. The number is summation of Log only and Log & Drop events.

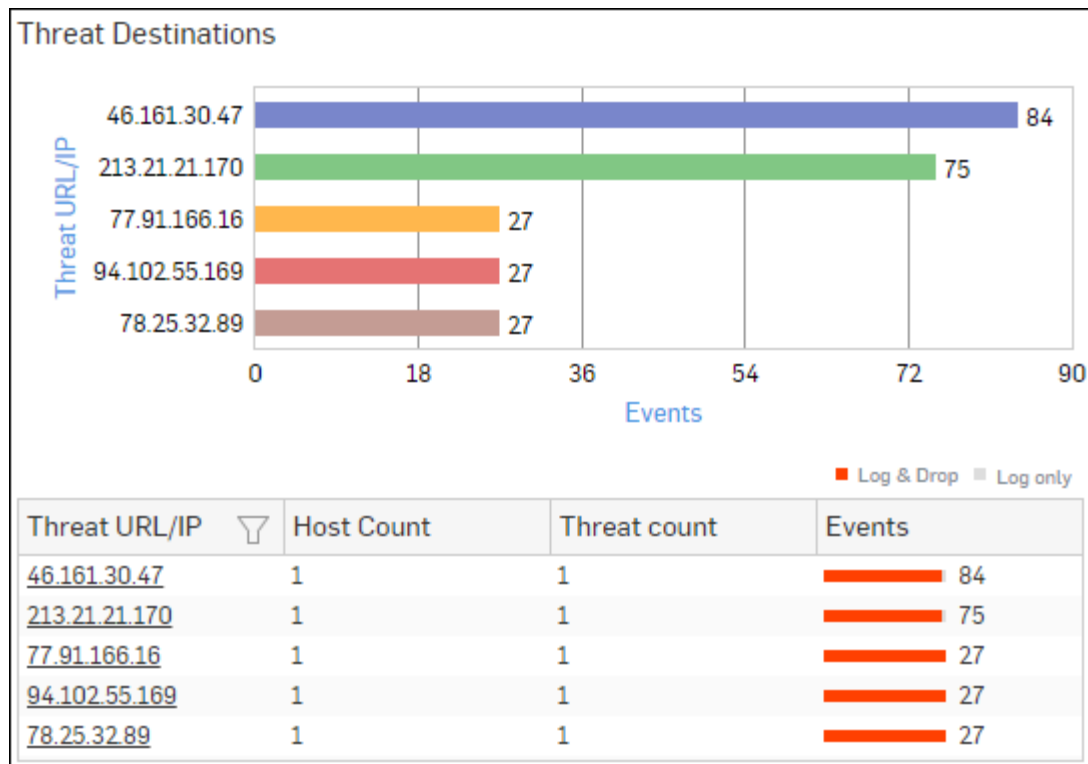


Figure 169: Threat Destinations

Click Threat URL/IP hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Detailed View - ATP

This report provides a detailed summary of advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Detailed View - ATP**.

The report is displayed in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page..

The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- User: Username of the infected user.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Events: Total number of events. The number is summation of Log only and Log & Drop events.
- Action: Action performed by the Device when a threat is detected. Possible options:
 - Log & Drop: The data packet is logged and dropped.
 - Log only: The data packet is logged.

Detailed View - ATP									
Host (Source IP)	User	Threat	Threat URL/IP	Origin	Events	Action			
10.198.47.112	dp	C2/Generic-A	46.161.30.47	Firewall	54	Log & Drop			
10.198.47.112	dp	C2/Generic-A	213.21.21.170	Firewall	45	Log & Drop			
10.198.47.112	atp1	C2/Generic-A	46.161.30.47	Firewall	27	Log & Drop			
10.198.47.112	atp1	C2/Generic-A	213.21.21.170	Firewall	27	Log & Drop			
10.198.47.112	atp1	C2/Generic-A	77.91.166.16	Firewall	18	Log & Drop			

Figure 170: Detailed View - ATP

Security Heartbeat - ATP

This report provides an insight into advanced threats related to endpoints in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Security Heartbeat - ATP**.

The report is displayed in a tabular format. The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Login User: Username of the infected user.
- Process User: Username of the user owning the process.
- Executable: Name of the infected executable file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Event Last Seen: Time when the infected executed file was last found in the host.
- Events: Total number of events. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP									
Host (Source IP)	Login User	Process User	Executable	Threat	Threat URL/IP	Event Last Seen	Events		
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1		

Figure 171: Security Heartbeat - ATP

Suspicious Executable

This report lists executable (.exe) files possibly infected with threats.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Suspicious Executable**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays total number of events per executable file while the tabular report contains the following information:

- Executable: Name of the executable file, possibly infected with a threat.
- Events: Total number of events per file. The number is summation of Log only and Log & Drop events.

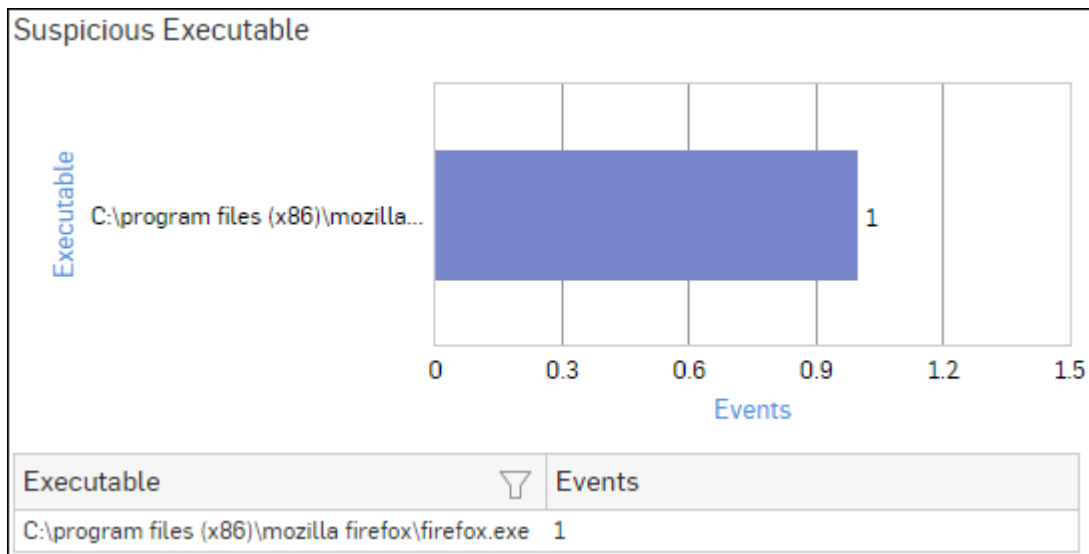


Figure 172: Suspicious Executable

Filtered ATP Reports

The ATP Reports can further be drilled-down to get the second level of ATP reports.

The ATP Reports (except Time Trend - ATP, Suspicious Executable, Detailed View - ATP and Client Insights - ATP) can be filtered to get the following set of reports:

- [Hosts - ATP](#)
- [Advanced Threats](#)
- [Users - ATP](#)
- [Origins](#)
- [Trend - ATP Events](#)
- [Threat Destinations](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)
- [Suspicious Executable](#)

To get filtered ATP reports, you need to choose one of the following filter criteria:

- Host from [Hosts - ATP Report](#)
- Threat from [Advanced Threats Report](#)
- User from [Users - ATP Report](#)
- Origin from [Origins Report](#)
- Destination from [Threat Destinations Report](#)

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format, which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Hosts - ATP widget

This widget displays a comprehensive summary of host wise advanced threats in your network.



Note: This widget will not be displayed for the filter criterion Host.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of events per host while the tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Threat Count: Number of threats per source host.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

Advanced Threats widget

This report displays a comprehensive summary of advanced threats in your network.



Note: This widget will not be displayed for the filter criterion Threat.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of threats along with total number of events per threat while the tabular report contains the following information:

- Threat: Name of the threat.
- Host Count: Number of hosts infected with the threat.
- Origins: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Events: Total number of events per threat. The number is summation of Log only and Log & Drop events.

Users - ATP widget

This widget displays a comprehensive summary of user wise advanced threats in your network.



Note: This widget will not be displayed for the filter criterion User.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of users along with total number of events per user while the tabular report contains the following information:

- User: User name of the infected user.
- Host Count: Number of hosts per user.
- Threat Count: Number of threats per user.
- Events: Total number of events per user. The number is summation of Log only and Log & Drop events.

Origins widget

This widget displays a comprehensive summary of origins associated with advanced threats in your network.



Note: This widget will not be displayed for the filter criterion Origin.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of origins along with total number of events per origin while the tabular report contains the following information:

- Origins: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS

- Web
- Combination of any of the above
- Host Count: Number of hosts per origin.
- Threat Count: Number of threats per origin.
- Attempts: Total number of events per origin. The number is summation of Log only and Log & Drop events.

Trend - ATP Events widget

This report displays a comprehensive summary of date wise advanced threats in your network. The report helps an administrator to understand the infection trend, i.e. if it is increasing / reducing or stable over time.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays total number of attempts per day while the tabular report contains the following information:

- Date: Date in YYYY-MM-DD HH:MM:SS format.
- Events: Total number of events per day. The number is summation of Log only and Log & Drop events.

Threat Destinations widget

This widget displays a comprehensive summary of destination wise advanced threats in your network.



Note: This widget will not be displayed for the filter criterion Destination.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of threat destinations along with number of events per destination while the tabular report contains the following information:

- Threat URL/IP: IP Address of the infected destination.
- Host Count: Number of hosts per destination.
- Threat Count: Number of threats per destination.
- Events: Total number of attempts per destination. The number is summation of Log only and Log & Drop events.

Detailed View - ATP widget

This report provides a detailed summary of advanced threats in your network.

The report is displayed in a tabular format.

The tabular report contains the following information:

- Action: Action performed by the Device when a threat is detected. Possible options:
 - Log & Drop: The data packet is logged and dropped.
 - Log only: The data packet is logged.
- Host (Source IP): IP Address of the source host.
- User: Username of the infected user.
- Threat URL/IP: IP Address of the infected destination.
- Threat: Name of the threat.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - HTTP Proxy
 - Combination of any of the above
- Events: Total number of events. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP widget

This report provides an insight into advanced threats related to endpoints in your network.

The report is displayed in a tabular format. The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Login User: Username of the infected user.
- Process User: Username of the user owning the process.
- Executable: Name of the infected executable file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Event Last Seen: Time when the infected executed file was last found in the host.
- Events: Total number of events. The number is summation of Log only and Log & Drop events.

Suspicious Executable widget

This report lists executable (.exe) files possibly infected with threats.

The report is displayed using a graph as well as in a tabular format.

The bar graph displays total number of attempts per executable file while the tabular report contains the following information:

- Executable: Name of the executable file, possibly infected with a threat.
- Events: Total number of events per file. The number is summation of Log only and Log & Drop events.

Wireless

Wireless Reports dashboard provide an overview of usage of Access Points (AP) and SSIDs configured in the Device. It helps identify wireless traffic passing through the network with the help of AP and SSID Time Trend reports.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless**.

It contains following reports in widget format:

- [APs by Clients](#)
- [SSIDs by Clients](#)
- [Trend - All APs](#)
- [Trend - All SSIDs](#)

APs by Clients

This report provides an overview of maximum, minimum and average number of clients connected for each AP configured in the Device.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > APs by Clients**.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- AP ID: Unique ID of the AP, as configured in the Device.
- Max Clients: Maximum number of connected clients per AP for the selected time period.
- Avg Clients: Average of all the connected clients per AP for the selected time period.
- Min Clients: Minimum number of connected clients per AP for the selected time period.



APs by Clients 			
AP Id 	Max Clients	Avg Clients	Min Clients
A40024A636F7862	8	1	0

Figure 173: APs by Clients

To view the [Filtered AP by Clients Reports](#) for a particular AP, drill down by clicking AP ID from the table.

Filtered AP by Clients Reports

The AP by Clients reports can be filtered to get following set of reports:

- [SSIDs by Clients](#)
- [Trend per AP](#)

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

SSIDs by Clients

This report displays, for the selected AP, details about the SSIDs including maximum, minimum and average number of clients connected for each SSID.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > SSIDs by Clients**.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- SSID: Name of the SSID, as defined in the selected AP.
- Max Clients: Maximum number of connected clients per SSID for the selected AP.
- Avg Clients: Average of all the connected clients per SSID for the selected AP.
- Min Clients: Minimum number of connected clients per SSID for the selected AP.

To view the following granular report of a particular SSID, drill down by clicking SSID from the table:

- [Time Trend](#)

Trend per AP & SSID

This report provides an overview of Time Trend for the selected AP and SSID by plotting total number of connected clients with time period.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > SSIDs by Clients > SSID > AP**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the total number of connected clients from all the configured APs with time period, while the tabular report contains the following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- Avg Connected Clients: Average of all the connected clients per SSID for the selected AP.
- Max Connected Clients: Maximum number of connected clients per SSID for the selected AP.

Trend per AP

This report provides an overview of Time Trend for the selected AP by plotting maximum number of connected clients with time period.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > Trend - All APs**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the total number of connected clients from all the configured APs with time period, while the tabular report contains the following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- AP: Name of the selected AP.
- Avg Connected Clients: Average of all the clients connected with the selected AP for each time period.
- Max Connected Clients: Maximum number of clients connected with selected AP for each time period.

SSIDs by Clients

This report provides an overview of maximum, minimum and average number of clients connected for each SSID configured in the Device.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > SSIDs by Clients**.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- SSID: Name of the SSID, as configured in the Device.
- Max Clients: Maximum number of connected clients per SSID for the selected time period.
- Avg Clients: Average of all the connected clients per SSID for the selected time period.
- Min Clients: Minimum number of connected clients per SSID for the selected time period.



SSIDs by Clients 			
SSID 	Max Clients	Avg Clients	Min Clients
SPIDIGO2015	8	1	0

Figure 174: SSIDs by Clients

To view the *Filtered SSIDs by Clients* reports for a particular SSID, drill down by clicking SSID from the table.

Filtered SSIDs by Clients

The SSIDs by Clients reports can be filtered to get following set of reports:

- [AP](#)
- [Trend per SSID](#)

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Filtered SSIDs by Clients AP

This report provides an overview of maximum, minimum and average number of clients connected for each AP in which the selected SSID is configured.

View the reports from **Reports > Network & Threats > Wireless > SSIDs by Clients > SSID**.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- AP ID: Unique ID of the AP, as configured in the Device.
- Max Clients: Maximum number of connected clients per AP for the selected SSID and time period.
- Avg Clients: Average of all the connected clients per AP for the selected SSID and time period.
- Min Clients: Minimum number of connected clients per AP for the selected SSID and time period.

To view the following report for a particular AP, drill down by clicking AP ID from the table:

- [Time Trend](#)

Trend per AP & SSID

This report provides an overview of Time Trend for the selected AP and SSID by plotting total number of connected clients with time period.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > SSIDs by Clients > SSID > AP**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the total number of connected clients from all the configured APs with time period, while the tabular report contains the following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- Avg Connected Clients: Average of all the connected clients per SSID for the selected AP.
- Max Connected Clients: Maximum number of connected clients per SSID for the selected AP.

Trend per SSID

This report provides an overview of Time Trend for the selected AP by plotting maximum number of connected clients with time period.

View the reports from **Reports > Network & Threats > Wireless > Trend - All SSIDs**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the maximum number of connected clients from all the configured SSIDs with time period, while the tabular report contains the following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- SSID: Name of the selected SSID.
- Avg Connected Clients: Average of all the clients connected with the selected SSID for each time period.
- Max Connected Clients: Maximum number of clients connected with selected SSID for each time period.

Trend - All APs

This report provides an overview of AP Time Trend by plotting maximum number of connected clients from all the configured APs with time period.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > Trend - All APs**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the maximum number of connected clients from all the configured APs with time period, while the tabular report contains the following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- Avg Connected Clients: Average number of connected clients (from all the configured APs) for each time period.
- Max Connected Clients: Maximum number of connected clients (from all the configured APs) for each time period.

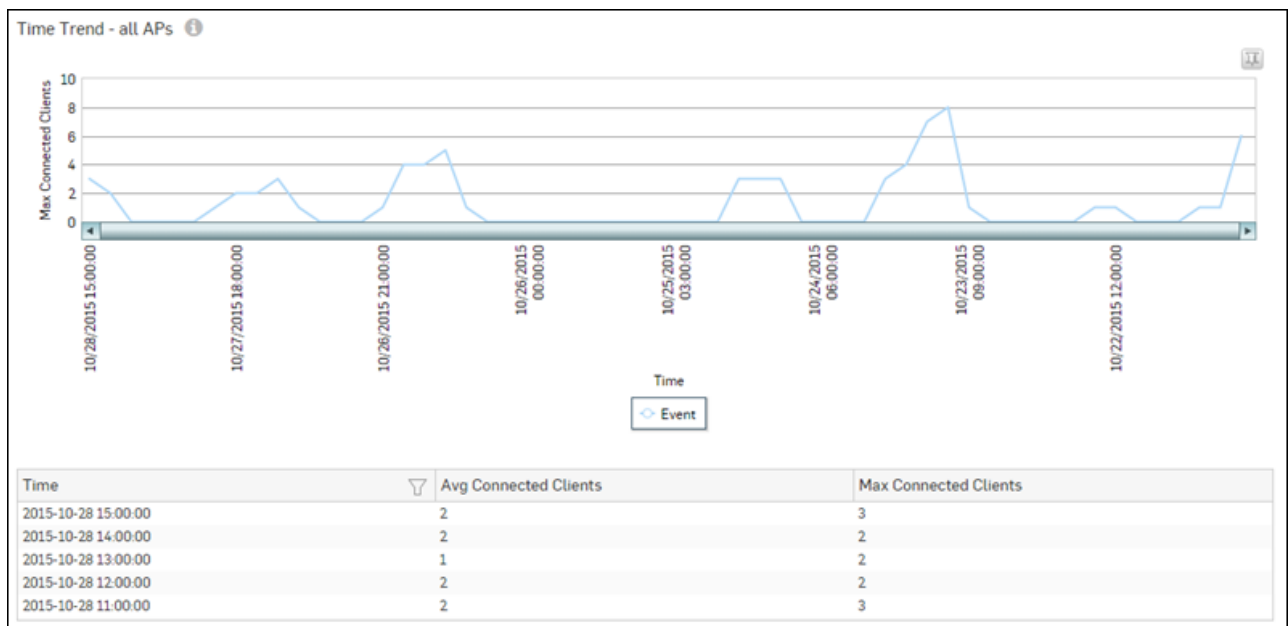


Figure 175: Trend - All APs

Trend - All SSIDs

This report provides an overview of SSID Time Trend by plotting maximum number of connected clients from all the configured SSIDs with time period.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Wireless > Trend - All SSIDs**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays the maximum number of connected clients from all the configured SSIDs with time period, while the tabular report contains the following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- Avg Connected Clients: Average number of connected clients (from all the configured SSIDs) for each time period.
- Max Connected Clients: Maximum number of connected clients (from all the configured SSIDs) for each time period.

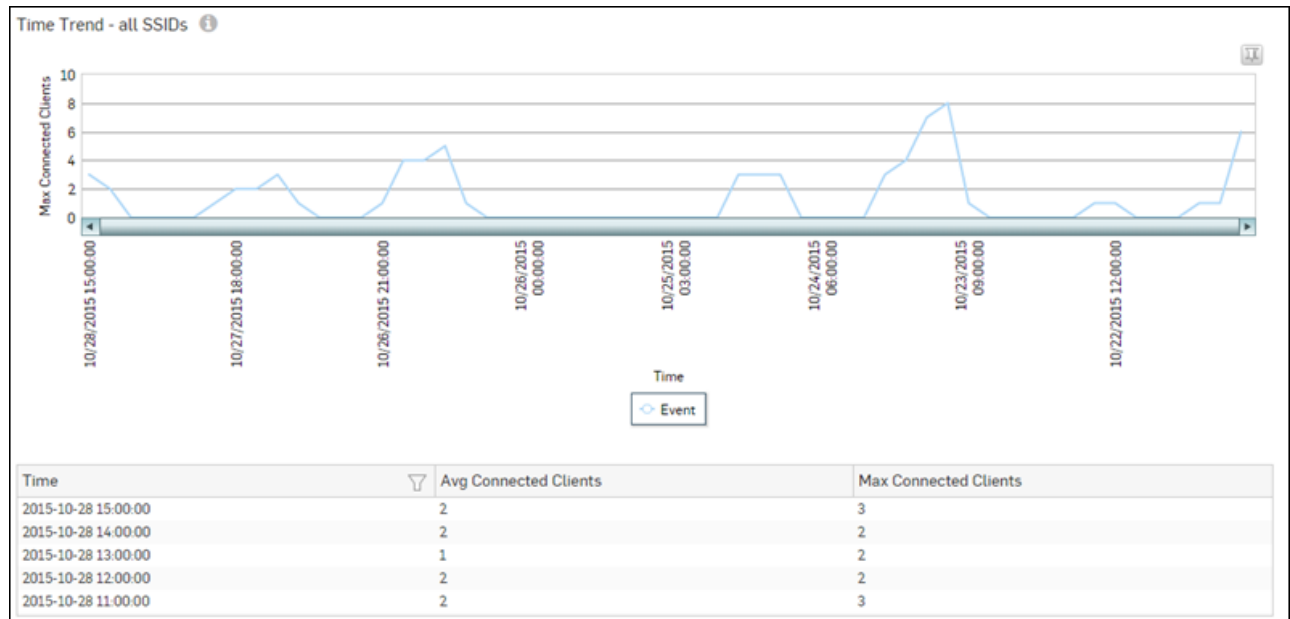


Figure 176: Trend - All SSIDs

Security Heartbeat

Security Heartbeat reports dashboard provide an insight into health of endpoints in your network based on the data collected by the Device from communication between an endpoint and Sophos Central.



Note: An endpoint must be managed by Sophos Central to be able to view its Health Insight reports.

These reports can facilitate an administrator in determining the health status of various endpoints in the network and thus provides a basis for fine tuning the network access policies.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat**.

Security Heartbeat reports dashboard provide following reports:

- [Client Health](#)
- [Detailed View - Client Health](#)
- [Security Heartbeat - ATP](#)
- [Blocked Network Access](#)
- [Missing Heartbeat](#)
- [Trend - Missing Heartbeat](#)
- [Blocked Server Access](#)
-

Client Health

This report shows health status and number of endpoints per health status.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Client Health**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of endpoints per health status, while the tabular report contains the following information:

- Client Health: Displays client health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Count: Number of endpoints per health status.
- Percent: Percent-wise distribution among the client health status.

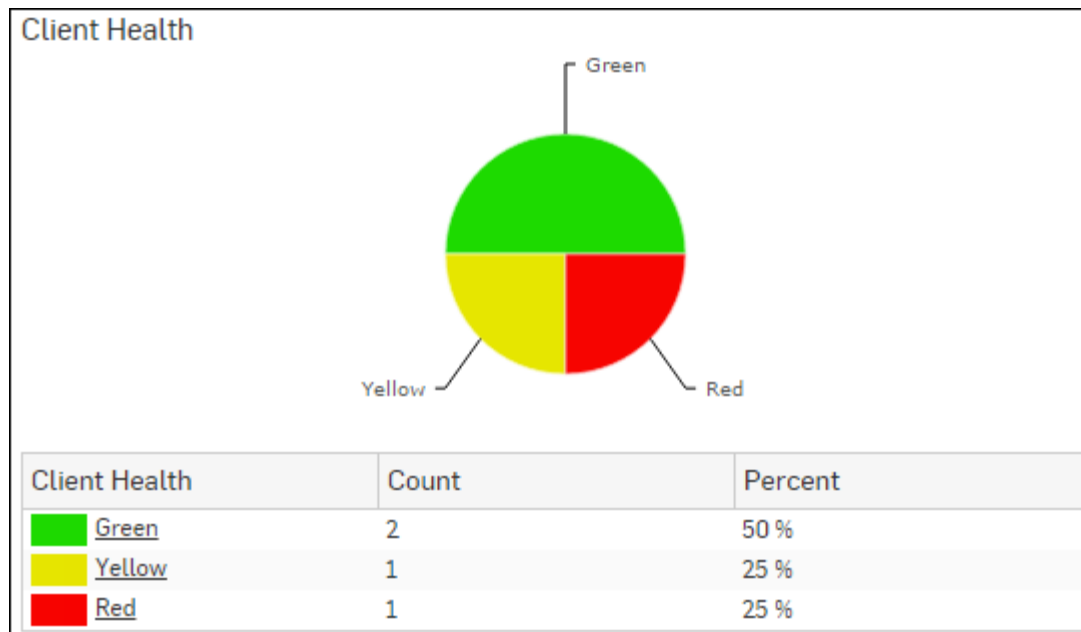


Figure 177: Client health

Click the Client Health status in the table or pie chart to view the [Filtered Security Heartbeat Reports](#).

Filtered Client Health Reports

The Client Health reports can be filtered to get following set of reports:

- [Trend - Client Health](#)
- [Detailed View - Client Health](#)
- [Blocked Network Access](#)

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Trend - Client Health widget

This widget report displays day-wise break-up of number of endpoints with the selected Health status.



Note: This widget is displayed only when the **Client Health** report is drill-downed by selecting a Health status.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays day-wise break-up of number of endpoints with the selected Health status while the tabular report contains the following information:

- Date: Date in YYYY-MM-DD format.
- Client Count: Number of endpoints with the selected Health status for each date.

Detailed View - Client Health widget

This widget report shows in-depth information regarding health status of endpoints in your network.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Client Name: Name of the client.
- Health - Last Seen: Displays latest health status of the selected endpoint. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.

Blocked Network Access widget

This widget report lists hosts that were denied to access the network due to health reasons.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- Host: IP Address of the endpoint.
- User: User name of the user logged into the endpoint.
- Destination: IP Address of the destination.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.
- Health Reason: Displays health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.

Detailed View - Client Health

This report shows in-depth information regarding health status of endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Detailed View - Client Health**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Detailed View - Client Health** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Host Name: Name of the client.
- Health - Last Seen: Displays the latest health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.





Detailed View - Client Health				
Host (Source IP) ▾	Host Name ▾		Health - Last Seen	Last Health
10.20.41.8	TWIN8164BIT		Red	-
10.20.41.7	TWIN864		Yellow	-
10.198.38.8	TWIN764		Green	-
10.20.41.12	TWIN832		Green	-

Figure 178: Detailed View - Client Health

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Security Heartbeat - ATP

The report displays advanced threats associated with the endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Security Heartbeat - ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Heartbeat > Security Heartbeat - ATP** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Login User: User name of the user logged into the endpoint.
- Process User: Username of the user running the process.
- Executable: Name of the infected executable (.exe) file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the destination.
- Event Last Seen: Displays the date in YYYY-MM-DD HH:MM:SS format when the event was last seen.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP									
Host (Source IP) ▾	Login User ▾	Process User ▾	Executable ▾	Threat ▾	Threat URL/IP ▾	Event Last Seen	Events		
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1		

Figure 179: Security Heartbeat - ATP

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Blocked Network Access

This report lists hosts that were denied to access the network due to health reasons.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Blocked Network Access**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host: IP Address of the endpoint.
- User: User name of the user logged into the endpoint.

- Destination: IP Address of the destination.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.
- Health Reason: Displays health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.

Blocked Network Access					
Host	User	Destination	Events	Health Reason	
10.198.47.162	Unidentified	8.8.8.8	989		Unknown/...
10.198.47.4	Unidentified	216.163.176.33	989		Unknown/...
10.198.47.162	Unidentified	4.2.2.2	989		Unknown/...
10.198.47.4	Unidentified	103.243.111.211	988		Unknown/...
10.198.47.4	Unidentified	216.163.188.153	988		Unknown/...

Figure 180: Blocked Network Access

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Missing Heartbeat

The report displays number of heartbeats missing per endpoint, in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Missing Heartbeat**.

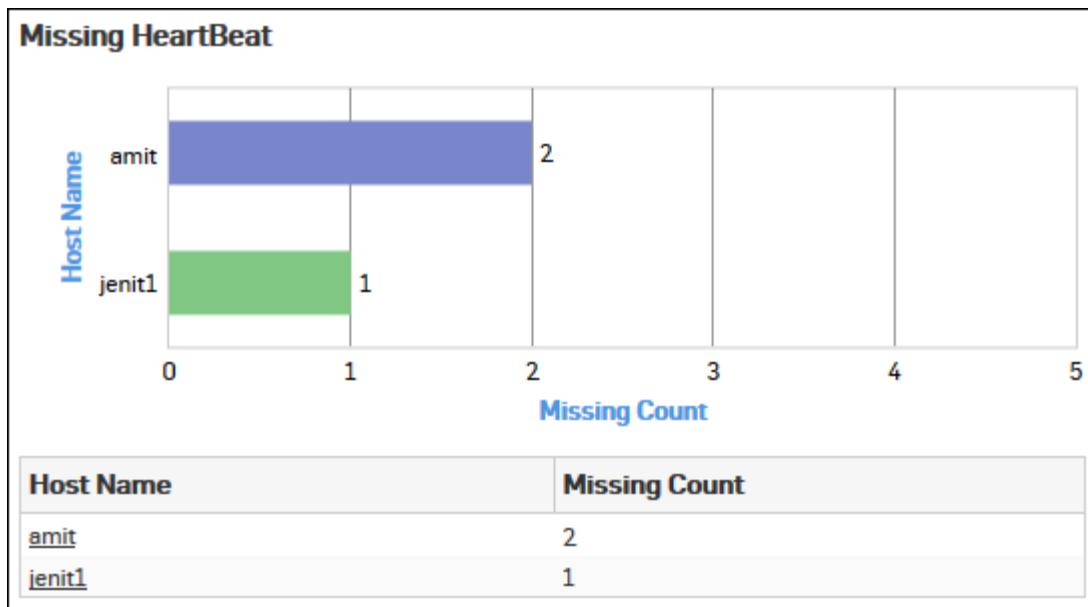
The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of heartbeats missing per endpoint, while the tabular report contains the following information:

- Host Name: Name of the endpoint.
- Missing Count: Number of heartbeats missing per endpoint.

Figure 181: Missing Heartbeat



Click the Host Name status in the table or the graph to view the [Filtered Missing Heartbeat Reports](#)

Filtered Missing Heartbeat Report

The Missing Heartbeat report can be filtered to get following report:

- [Missing Heartbeat](#)

Missing Heartbeat widget

The report displays details of heartbeats missing from an endpoint to the Sophos UTM over a selected period of time.



Note: This widget is displayed only when the **Missing Heartbeat** report is filtered by selecting a Host Name.

The report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host IP: IP Address of the endpoint.
- Missing From: Displays time in YYYY-MM-DD HH:MM:SS format.
- Duration: Displays duration in HH:MM:SS format.

Missing HeartBeat		
Host IP	Missing From ▼	Duration
10.198.46.51	2016-05-09 12:00:00	03:00:00
10.198.46.51	2016-05-09 12:00:00	03:00:00

Figure 182: Missing Heartbeat widget

Trend - Missing Heartbeat

This report displays number of endpoints not connected to Sophos UTM during the selected time period..

View the report from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Trend - Missing Heartbeat**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the number of endpoints not connected to Sophos UTM during a selected time period, while the tabular report contains the following information:

- Time: Displays time in YYYY-MM-DD HH:MM:SS format.
- Host Count: Number of endpoints not connected to Sophos UTM.

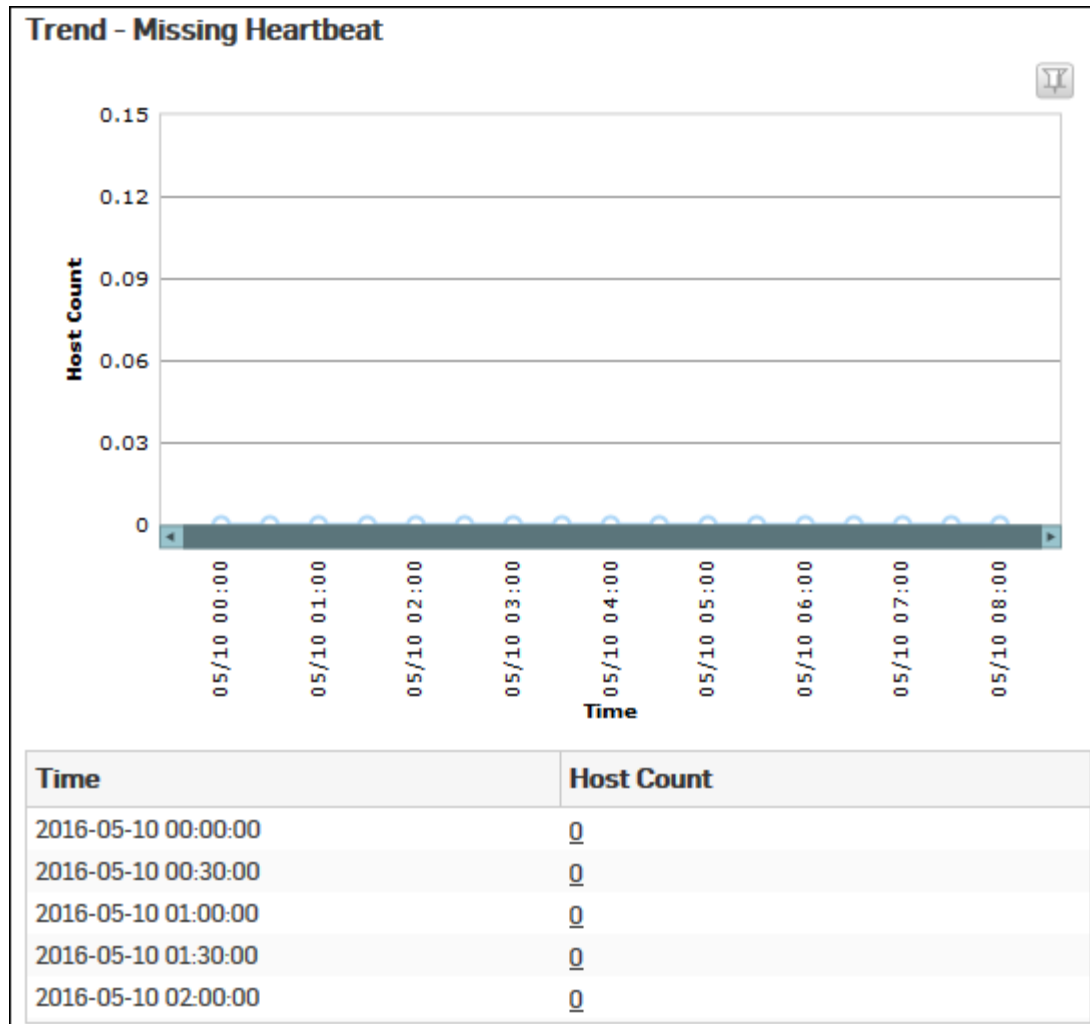


Figure 183: Trend - Missing Heartbeat

Blocked Server Access

This report lists the hosts that were denied access to the server due to health reasons.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Sandstorm > Blocked Server Access**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- User: User name of the user logged into the endpoint.
- Destination: IP Address of the server.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

- Health Reason: Displays health status of server. Possible options are:
 - Yellow: The server is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The server is Objectionable and is infected with some malicious content.






Blocked Server Access					
Host	User	Destinat...	Events	Health	
10.198.47.104	iview2	2.2.2.198	20		Red
10.198.47.104	atp20	2.2.2.223	18		Unknow...
10.198.47.104	Unidentified	2.2.2.223	4		Yellow
10.198.47.104	atp20	2.2.2.223	3		Yellow
10.198.47.104	iview2	2.2.2.149	2		Yellow

Figure 184: Blocked Server Access

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#) on page 212

Filtered Security Heartbeat Reports

The Security Heartbeat reports (except the Client Health report) can be filtered to get following set of reports:

- [Trend - Client Health](#)
- [Detailed View - Client Health](#)
- [Blocked Network Access](#)
- [Security Heartbeat - ATP](#)
- [Blocked Server Access](#)

To get filtered Client Health Insights reports, you need to choose one of the following filter criteria:

- Host from [Detailed View - Client Health report](#)
- Host from [Security Heartbeat - ATP report](#)
- Host from [Blocked Network Access report](#)
- Host from [Blocked Server Access](#) on page 211

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Trend - Client Health widget

This Widget report displays day-wise break-up of Health status for the selected Host.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays day-wise break-up of Health status for the selected Host while the tabular report contains the following information:

- Date: Date in YYYY-MM-DD HH:MM:SS format.
- Client Health: Day-wise Health status for the selected Host.

Detailed View - Client Health widget

This widget report shows in-depth information regarding health status of endpoints in your network.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Client Name: Name of the client.
- Health - Last Seen: Displays latest health status of the selected endpoint. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.

- Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
- Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.

Blocked Network Access widget

This widget report lists hosts that were denied to access the network due to health reasons.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- Host: IP Address of the endpoint.
- User: User name of the user logged into the endpoint.
- Destination: IP Address of the destination.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.
- Health Reason: Displays health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.

Security Heartbeat - ATP widget

The report displays advanced threats associated with the endpoints in your network.



Note: This widget is displayed for all Client Health Insights reports except **Client Health**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Login User: User name of the user logged into the endpoint.
- Process User: Username of the user running the process.
- Executable: Name of the infected executable (.exe) file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the destination.
- Event Last Seen: Displays the date in YYYY-MM-DD HH:MM:SS format when the event was last seen.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

Blocked Server Access widget

This report lists hosts that were denied to access the server due to health reasons.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- Host: IP Address of the endpoint.
- User: User name of the user logged into the endpoint.
- Destination: IP Address of the server.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.
- Health Reason: Displays health status of server. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.

Sandstorm

Sandstorm reports dashboard provides an insight of enhanced protection against advanced and targeted attacks. It provides targeted attack protection, visibility and analysis by detecting, blocking and responding to evasive and unknown threats.

View the reports from **Monitor & Analyze > Reports > Network & Threats > Sandstorm**.

- [Policy and Content - Sandstorm Usage](#) on page 214
- [Sandstorm Web Category](#) on page 214
- [Sandstorm Web Users](#) on page 215
- [Policy and Content - Sandstorm Mail Usage](#) on page 216
- [Sandstorm Mail Category](#) on page 217
- [Sandstorm Mail Senders](#) on page 217

Policy and Content - Sandstorm Usage

This report provides an overall view of the usage of the sandstorm service, listed by analysis result.

View the report from **Monitor & Analyze > Reports > Network & Threats > Sandstorm > Policy and Content - Sandstorm Usage**.

The report is displayed in a tabular format. By default, the report is displayed for the current date. To view report for any other date, select the date from the calendar button provided on top of the page.

The table contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.
 - Clean: Files that have been analysed and that exhibit no malicious behavior.
 - Analysis Unsuccessful: Files that could not be analysed.
- Downloaded: Number of files downloaded per category.
- Bytes: Number of bytes downloaded.
- Sent For Analysis: Number of files sent to Sandstorm for analysis.
- Bytes: Number of bytes sent for analysis.

Policy and Content - Sandstorm Usage				
Category	Downloaded	Bytes	Sent For Analysis	Bytes
Clean	5	621.52 KB	1	23.84 KB
Malicious	5	747.11 KB	3	448.27 KB
Analysis Unsuccessful	2	298.85 KB	0	0 B

Figure 185: Policy & Content: Sandstorm Usage

Click the Category hyperlink in the table to view the [Filtered Sandstorm Reports](#) on page 218.

Sandstorm Web Category

This report displays a list of sandstorm web categories along with the number of access attempts for each category.

View the report from **Monitor & Analyze > Reports > Network & Threats > Sandstorm > Sandstorm Web Category**.

The report is displayed using a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. To view report for any other date, select the date from the calendar button provided on top of the page.

The pie chart displays list of categories of while the tabular report contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.

- Clean: Files that have been analysed and that exhibit no malicious behavior.
- Analysis Unsuccessful: Files that could not be analysed.
- Hits: Number of hits per category.
- Bytes: Number of bytes downloaded per category.

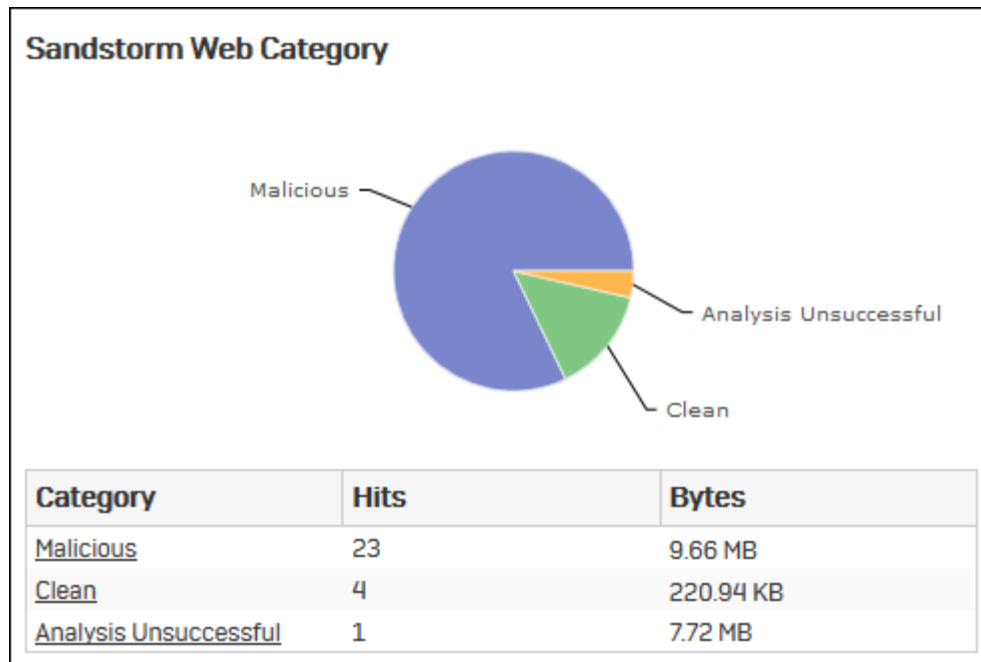


Figure 186: Sandstorm Web Category

Click the Category hyperlink in the table or pie chart to view the [Filtered Sandstorm Reports](#) on page 218.

Sandstorm Web Users

This report displays a list of users whose maximum files are sent to Sandstorm for analysis, each shown as a percentage of the total number of files flagged as suspicious.

View the report from **Monitor & Analyze > Reports > Network & Threats > Sandstorm > Sandstorm Web Users**.

The report is displayed using a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. To view report for any other date, select the date from the calendar button provided on top of the page.

The pie chart displays list of categories of while the tabular report contains the following information:

- User: Name of the user.
- Hits: Number of hits per user.
- Bytes: Number of bytes downloaded per user.

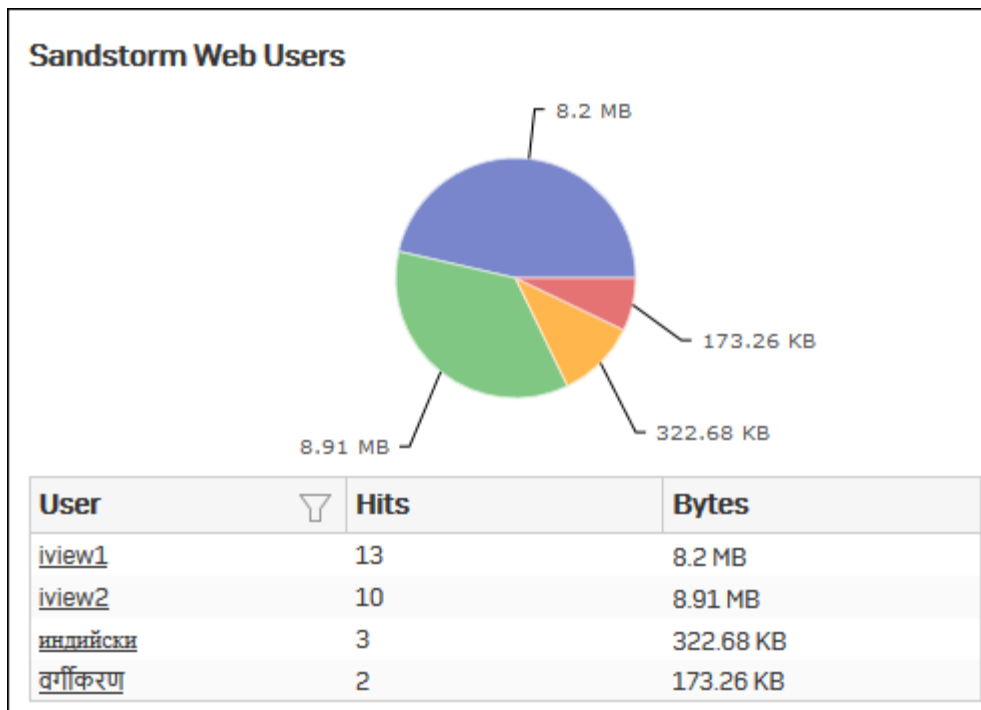


Figure 187: Sandstorm Web Users

Click the User hyperlink in the table or pie chart to view the [Filtered Sandstorm Reports](#) on page 218.

Policy and Content - Sandstorm Mail Usage

This report displays the number of emails forwarded to the Sandstorm for scanning and identifying threats discovered in those files, listed by the analysis result.

View the report from **Monitor & Analyze > Reports > Network & Threats > Sandstorm > Policy and Content - Sandstorm Mail Usage**.

The report is displayed in a tabular format.

By default, the report is displayed for the current date. To view report for any other date, select the date from the calendar button provided on top of the page.

The table contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.
 - Clean: Files that have been analysed and that exhibit no malicious behavior.
 - Analysis Unsuccessful: Files that could not be analysed.
- Downloaded: Number of files downloaded per category.
- Bytes: Number of bytes downloaded.
- Sent For Analysis: Number of files sent to Sandstorm for analysis.
- Bytes: Number of bytes sent for analysis.

Policy and Content - Sandstorm Mail Usage				
Category	Downloaded	Bytes	Sent For Analysis	Bytes
Malicious	1	149.42 KB	1	149.42 KB

Figure 188: Policy and Content - Sandstorm Mail Usage

Click Category hyperlink in the table to view the [Filtered Sandstorm Reports](#) on page 218.

Sandstorm Mail Category

This report displays the list of sandstorm email categories along with the number of access attempts for each category.

View the report from **Monitor & Analyze > Reports > Network & Threats > Sandstorm > Sandstorm Mail Category**.

The report is displayed using a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. To view report for any other date, select the date from the calendar button provided on top of the page.

The pie chart displays list of categories while the tabular report contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.
 - Clean: Files that have been analysed and that exhibit no malicious behavior.
 - Analysis Unsuccessful: Files that could not be analysed.
- Hits: Number of hits per category.
- Bytes: Number of bytes downloaded per category.

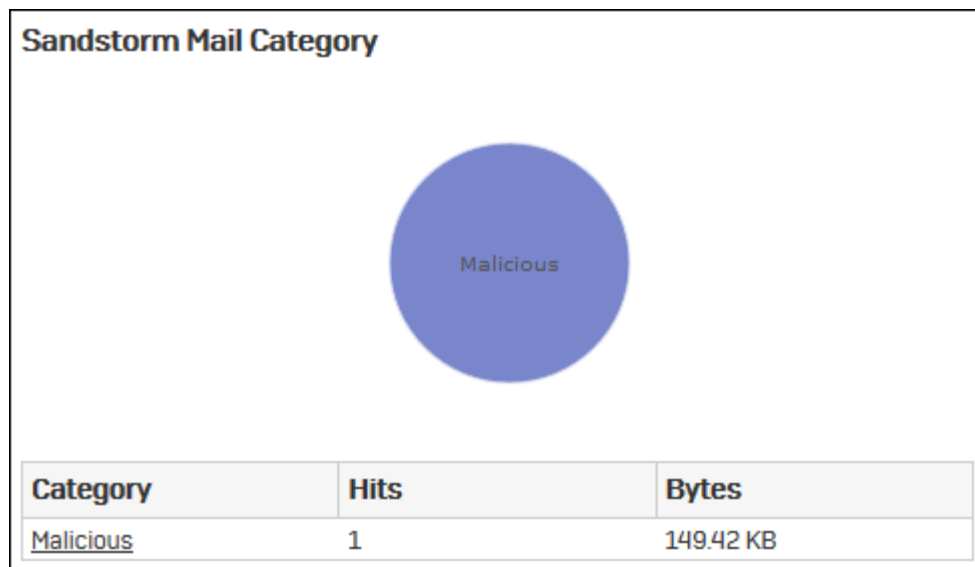


Figure 189: Sandstorm Mail Category

Click Category hyperlink in the table or pie chart to view the [Filtered Sandstorm Reports](#) on page 218.

Sandstorm Mail Senders

This report displays a list of email senders along with the number of suspicious emails forwarded to Sandstorm.

View the report from **Monitor & Analyze > Reports > Network & Threats > Sandstorm > Sandstorm Mail Senders**.

The report is displayed using a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. To view report for any other date, select the date from the calendar button provided on top of the page.

The pie chart displays list of sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Hits: Number of emails sent.
- Bytes: Amount of data transferred.

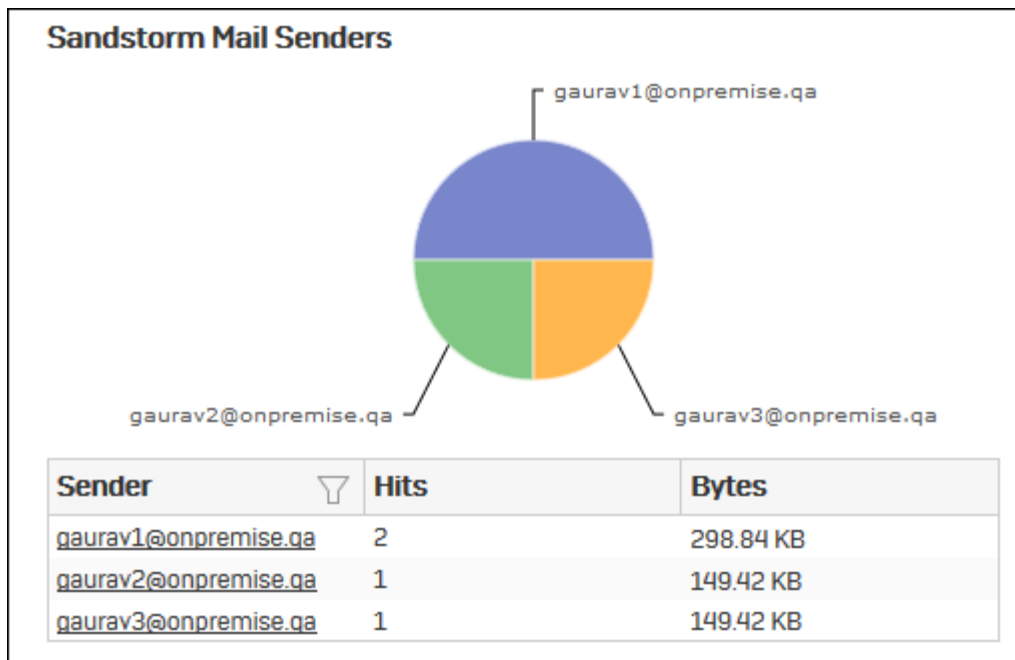


Figure 190: Sandstorm Mail Senders

Click Sender hyperlink in the table or pie chart to view the [Filtered Sandstorm Reports](#) on page 218.

Filtered Sandstorm Reports

Sandstorm reports can be filtered to get following set of reports:

- [Policy and Content - Sandstorm Usage widget](#) on page 218
- [Sandstorm Web Category widget](#) on page 219
- [Sandstorm Web Users widget](#) on page 219
- [Policy and Content - Sandstorm Mail Usage widget](#) on page 219
- [Sandstorm Mail Category widget](#) on page 219
- [Sandstorm Mail Senders](#) on page 220

To get Filtered Sandstorm reports, you need to choose one of the following filter criteria:

- Category from [Policy and Content - Sandstorm Usage](#) on page 214 Report
- Category from [Sandstorm Web Category](#) on page 214 Report
- User from [Sandstorm Web Users](#) on page 215 Report
- Category from [Policy and Content - Sandstorm Mail Usage](#) on page 216
- Category from [Sandstorm Mail Category](#) on page 217
- Sender from [Sandstorm Mail Senders](#) on page 217

Policy and Content - Sandstorm Usage widget

This widget provides an overall view of the usage of the sandstorm service, listed by analysis result.

The table contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.
 - Clean: Files that have been analysed and that exhibit no malicious behavior.
 - Analysis Unsuccessful: Files that could not be analysed.
- Downloaded: Number of files downloaded per category.
- Bytes: Number of bytes downloaded.
- Sent For Analysis: Number of files sent to Sandstorm for analysis.

- Bytes: Number of bytes sent for analysis.

Sandstorm Web Category widget

This widget displays a list of sandstorm web categories that various users tried to access and the number of access attempts to each category.



Note: This widget will not be displayed for filter criterion Category.

The pie chart displays list of categories of while the tabular report contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.
 - Clean: Files that have been analysed and that exhibit no malicious behavior.
 - Analysis Unsuccessful: Files that could not be analysed.
- Hits: Number of hits per category.
- Bytes: Number of bytes downloaded per category.

Sandstorm Web Users widget

This widget displays a list of users who have had the most files referred to Sandstorm.



Note: This widget will not be displayed for filter criterion User.

The pie chart displays list of categories of while the tabular report contains the following information:

- User: Name of the user.
- Hits: Number of hits per user.
- Bytes: Bandwidth used per user.

Policy and Content - Sandstorm Mail Usage widget

This report displays the number of emails forwarded to the Sandstorm for scanning and identifying threats discovered in those files, listed by the analysis result.

The table contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.
 - Clean: Files that have been analysed and that exhibit no malicious behavior.
 - Analysis Unsuccessful: Files that could not be analysed.
- Downloaded: Number of files downloaded per category.
- Bytes: Number of bytes downloaded.
- Sent For Analysis: Number of files sent to Sandstorm for analysis.
- Bytes: Number of bytes sent for analysis.

Sandstorm Mail Category widget

This widget displays the list of sandstorm email categories along with the number of access attempts for each category.



Note: This widget will not be displayed for filter criterion Category.

The pie chart displays list of categories while the tabular report contains the following information:

- Category: Name of the category. Possible options are:
 - Malicious: Files that Sandstorm has determined are malicious.
 - Clean: Files that have been analysed and that exhibit no malicious behavior.
 - Analysis Unsuccessful: Files that could not be analysed.
- Hits: Number of hits per category.
- Bytes: Number of bytes downloaded per category.

Sandstorm Mail Senders

This widget displays the list of email senders along with the number of suspicious emails forwarded to Sandstorm.



Note: This widget will not be displayed for filter criterion Sender.

The pie chart displays list of categories while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Hits: Number of emails sent.
- Bytes: Amount of data transferred.

VPN

VPN reports provide an in-depth insight into VPN usage by remote users connecting to your network using IPsec VPN, SSL VPN and Clientless Access.



Note: The VPN sub sections can be accessed by selecting drop-down 1 given at the upper left corner of the page.

The section includes following reports:

- [VPN](#)
- [SSL VPN](#)
- [Clientless Access](#)

VPN

VPN Reports dashboard provide a snapshot of the network traffic generated by remote users with the help of IPsec, L2TP or PPTP connections. It helps to identify top connections, users and interfaces which are generating maximum traffic through the network.

View the VPN reports dashboard from **Monitor & Analyze > Reports > VPN > VPN**.

It contains following reports in widget format:

- [IPSec Usage](#)
- [IPSec Users](#)
- [L2TP & PPTP Usage](#)
- [L2TP Users](#)
- [PPTP Users](#)
- [VPN Event](#)
- [RED Usage](#)
- [RED Usage by ID](#)
- [RED Disconnects](#)

IPSec Usage

This report provides an overview of IPsec VPN Usage in terms of Connection Name along with the number of connections.

View report from VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > VPN > IPSec Usage**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays number of connections per IPsec VPN Connection Name, while the tabular report contains the following information:

- Connection Name: Name of the IPsec VPN connection.
- Connections: Number of connections per IPsec VPN Connection Name.

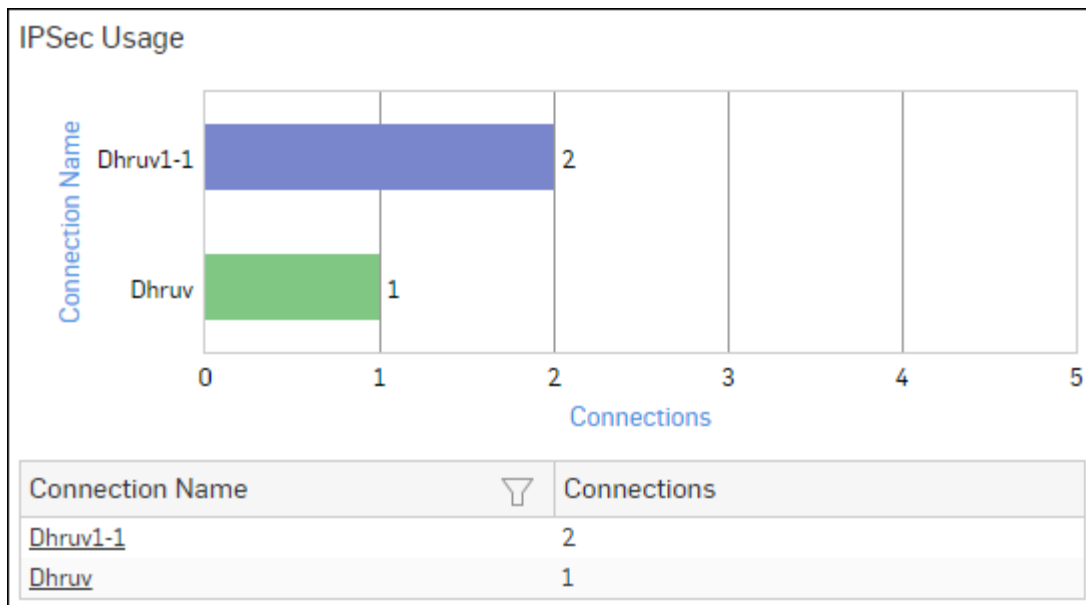


Figure 191: IPSec Usage

Click Connection Name hyperlink in the table or graph to view the [Filtered IPSec Usage by Data Transfer Reports](#).

Filtered IPSec Usage Reports

The IPSec Usage by Data Transfer report can be further drilled-down to view the Filtered IPSec Usage by Data Transfer reports.

View report from **Monitor & Analyze > Reports > VPN > VPN > IPSec Usage > Connection Name**.

It enables to view the following set of filtered reports:

- [IPSec Users](#)
- [IPSec Connection Details](#)

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

IPSec Users widget

This widget report provides an overview of the users using the selected IPSec VPN connection.

View report from **Monitor & Analyze > Reports > VPN > VPN > IPSec Usage > Connection Name**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays number of connections per user, while the tabular report contains the following information:

- User: Name of the user, as defined in the Device.
- Connections: Number of connections per user.

IPSec Connection Details widget

This widget report provides an overview of connection details for the selected IPSec connection.

View report from **Monitor & Analyze > Reports > VPN > VPN > IPSec Usage > Connection Name**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The tabular report contains the following information:

- User: Name of the user as defined in the Device. If the user is unauthenticated, then the VPN traffic will be considered as traffic generated by an Unidentified user.
- Local Interface IP: IP Address of local interface.
- Local Gateway IP: IP Address of local gateway.
- Internal Network: IP Address of the Internal Network. This field displays 'Not Available' in case of Remote Access connection type.
- Remote Interface IP: IP Address of remote interface.

IPSec Users

This report provides an overview of Users using IPsec VPN in terms of their User Name along with the number of connections.

View report from VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > VPN > IPSec Users**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays number of connections per user, while the tabular report contains the following information:

- User: Name of the User, as defined in the Device.
- Connections: Number of connections per user.

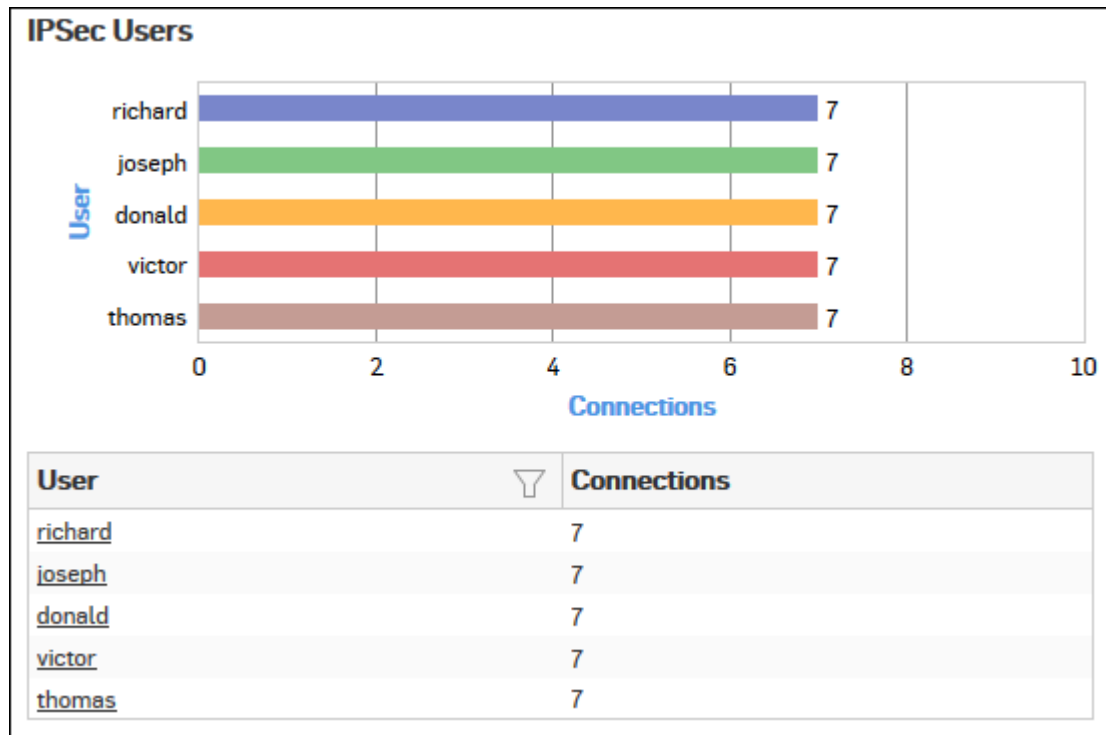


Figure 192: IPSec Users

Click User hyperlink in the table or graph to view the [Filtered IPSec Users Reports](#).

Filtered IPSec Users Reports

The IPSec Users report can be further drilled-down to view the Filtered IPSec Users reports.

View report from **Monitor & Analyze > Reports > VPN > VPN > IPSec Users > User**.

It enables to view the following set of reports:

- [IPSec Usage by Data Transfer](#)
- [Connection Details](#)

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

IPsec Usage widget

This widget report provides, for the selected user, an overview of IPsec VPN Usage in terms of Connection Name along with the number of connections.

View report from **Monitor & Analyze > Reports > VPN > VPN > IPsec Users > User**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays number of connections per IPsec VPN Connection Name, while the tabular report contains the following information:

- Connection Name: Name of the IPsec VPN connection.
- Connections: Number of connections per IPsec VPN Connection Name.

IPsec Connection Details widget

This widget report provides an overview of IPsec VPN connection details for the selected user.

View report from **Monitor & Analyze > Reports > VPN > VPN > IPsec Users > User**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The tabular report contains the following information:

- Connection Name: Name of the IPsec VPN connection.
- Local Interface IP: IP Address of local interface.
- Local Gateway IP: IP Address of local gateway.
- Internal Network: IP Address of the Internal Network. This field displays 'Not Available' in case of Remote Access connection type.
- Remote Interface IP: IP Address of remote interface.

L2TP & PPTP Usage

This report provides an overview of L2TP & PPTP Usage in terms of VPN connection type, number of connections and amount of data transferred per VPN type.

View report from VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > VPN > L2TP & PPTP Usage**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per VPN connection type, while the tabular report contains the following information:

- VPN Type: Type of VPN connection. Possible options are:
 - PPTP
 - L2TP
- Connections: Number of connections per VPN Type.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per VPN Type.

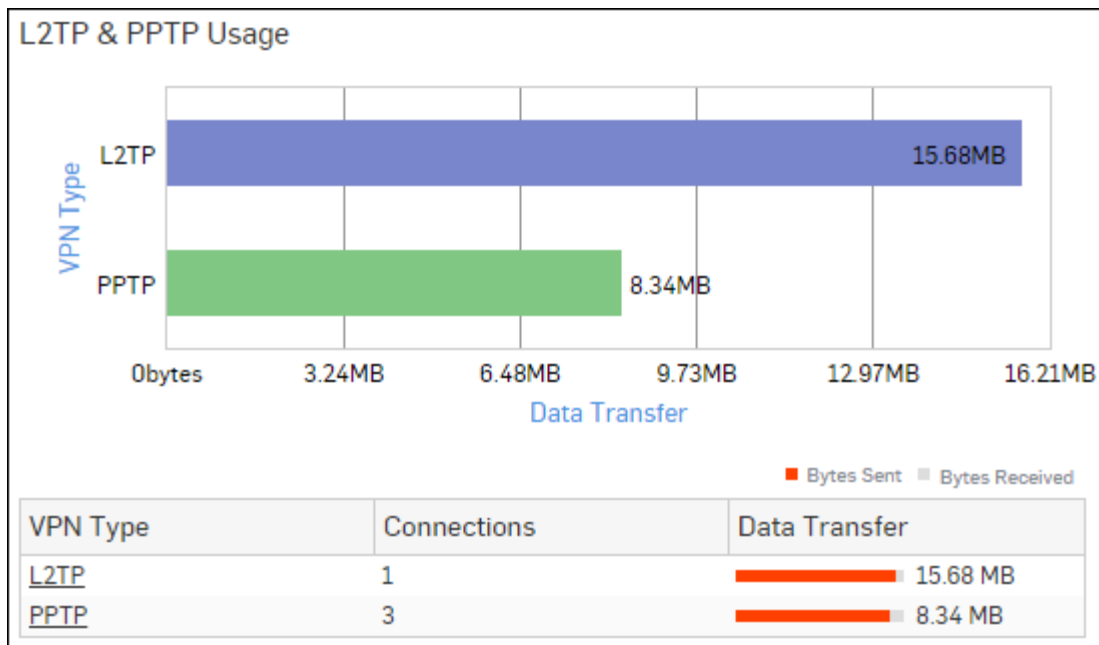


Figure 193: L2TP & PPTP Usage

Click VPN Type hyperlink in the table or graph to view the [Filtered L2TP & PPTP Usage Reports](#).

Filtered L2TP & PPTP Usage Reports

The VPN Usage report can be further drilled-down to view the Filtered VPN Usage Reports.

View report from **Monitor & Analyze > Reports > VPN > VPN > L2TP & PPTP Usage > VPN Type**.

It enables to view the following set of filtered reports:

- [Users](#)
- [Connection Details](#)
- [Time Trend](#)

Filtered Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Users widget

This widget report displays details of the users using the selected VPN Type.

View report from **Monitor & Analyze > Reports > VPN > VPN > L2TP & PPTP Usage > VPN Type**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per user, while the tabular report contains the following information:

- User: Name of the user, as defined in the Device.
- Connections: Number of connections per user.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per user.

Connection Details widget

This widget report displays, for the selected VPN Type, list of connection names along with the details of internal and remote network and users.

View report from **Monitor & Analyze > Reports > VPN > VPN > L2TP & PPTP Usage > VPN Type**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The tabular report contains the following information:

- Connection Name: Name of the connection
- User: User Name of the user as defined in the Device. If the user is unauthenticated or a clientless user, then the VPN traffic will be considered as traffic generated by an Unidentified user.
- Local Interface IP: IP Address of local interface.
- Local Gateway IP: IP Address of local gateway.
- Internal Network: IP Address of the Internal Network. This field displays 'Not Available' in case of Remote Access connection type.
- Remote Interface IP: IP Address of remote interface.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per connection.

Time Trend widget

This widget report displays time trend for the selected VPN Type.

View report from **Monitor & Analyze > Reports > VPN > VPN > L2TP & PPTP Usage > VPN Type**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays data transfer over the selected time period, while the tabular report contains the following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- VPN Type: Displays the selected VPN Type.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per time period.

L2TP Users

This report provides an overview of Users using L2TP VPN in terms of their User Name, number of connections and amount of data transferred.

View report from VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > VPN > L2TP Users**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per user, while the tabular report contains the following information:

- User: Name of the User, as defined in the Device.
- Connections: Number of connections per user.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per user.

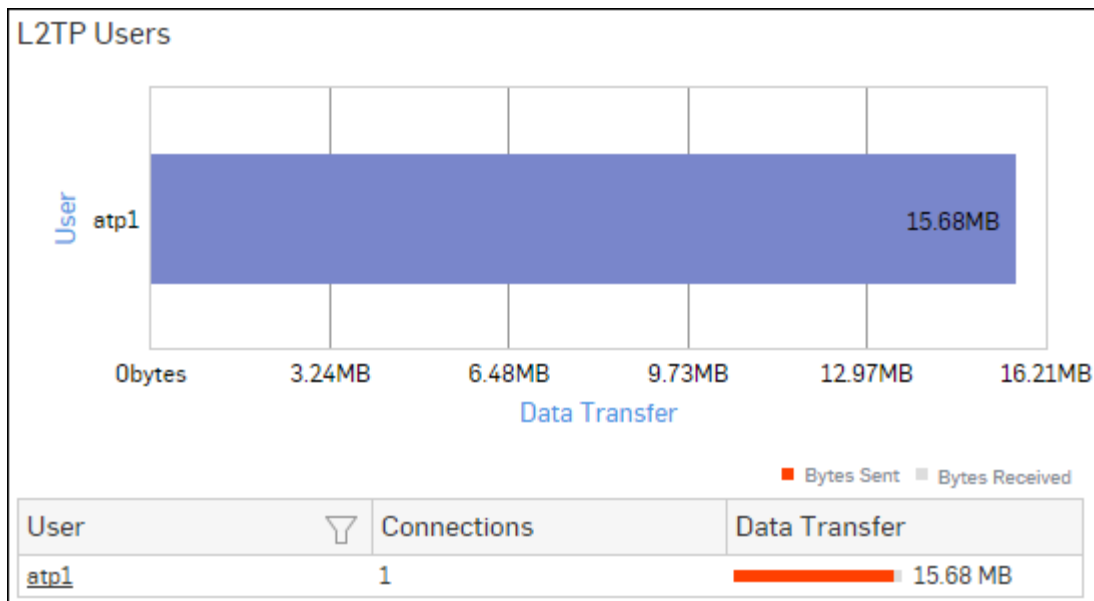


Figure 194: L2TP Users

Click User hyperlink in the table or graph to view the following set of reports:

- [L2TP Connection Details](#)

L2TP Connection Details

This report provides an overview of L2TP VPN connection details for the selected user.

View report from **Monitor & Analyze > Reports > VPN > VPN > L2TP Users > User**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The tabular report contains the following information:

- Local Interface IP: IP Address of the local interface.
- Leased IP: IP Address leased to the user.
- Remote Interface IP: IP Address of the remote interface.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per user.

PPTP Users

This report provides an overview of Users using PPTP VPN in terms of their User Name, number of hits and amount of data transferred.

View report from VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > VPN > PPTP Users**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per user, while the tabular report contains the following information:

- User: Name of the User, as defined in the Device.
- Connections: Number of connections per user.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per user.

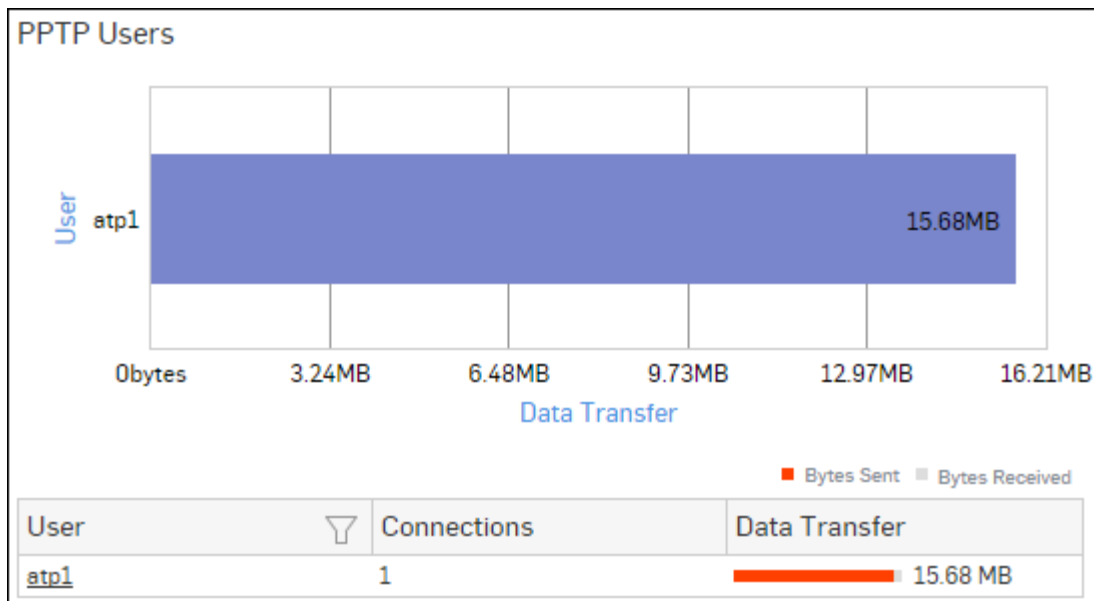


Figure 195: PPTP Users

Click User hyperlink in the table or graph to view the following set of reports:

- [PPTP Connection Details](#)

PPTP Connection Details

This report provides an overview of PPTP VPN connection details for the selected user.

View report from **Monitor & Analyze > Reports > VPN > VPN > PPTP Users > User**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The tabular report contains the following information:

- Local Interface IP: IP Address of the local interface.
- Leased IP: IP Address leased to the user.
- Remote Interface IP: IP Address of the remote interface.
- Data Transfer: Amount of data transferred (Bytes Sent + Bytes Received) per user.

VPN Event

This report provides an overview of VPN Events.

View report from VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > VPN > VPN Event**.

The Report is displayed in a tabular format.

The tabular report contains the following information:

- Time: Time when the event occurred.
- User: Name of the User, as defined in the Device.
- Source: IP Address of the Source generating the event.
- Severity: Severity level associated with the event. Predefined level are:
 - EMERGENCY
 - ALERT
 - CRITICAL
 - ERROR
 - WARNING

- NOTICE
- INFORMATION
- DEBUG
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- Status: Status of the VPN event.

VPN Event						
Time	User		Source		Severity	Message
2015-10-17 1...	atp1		10.198.233.52		Information	User atp1 log...
2015-10-17 1...	atp1		10.198.233.52		Information	User atp1 log...
2015-10-17 1...	atp1		10.198.233.48		Information	User atp1 log...
2015-10-17 1...	atp1		10.198.233.48		Information	User atp1 log...
2015-10-17 1...	atp1		10.198.233.48		Information	User atp1 log...

Figure 196: VPN Event

RED Usage

This report provides an overview of the amount of data transferred through various RED Devices connected with the Sophos Firewall.



Note: Network Protection subscription is required to view the RED Usage reports. Without a valid subscription, some reports do not show any data.

View report from VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > VPN > RED Usage**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per RED Device, while the tabular report contains the following information:

- RED ID: Displays the unique ID of the RED Device.
- Branch Name: Displays branch name, as configured in the Sophos Firewall.
- Data Transfer: Amount of data transferred per RED Device.

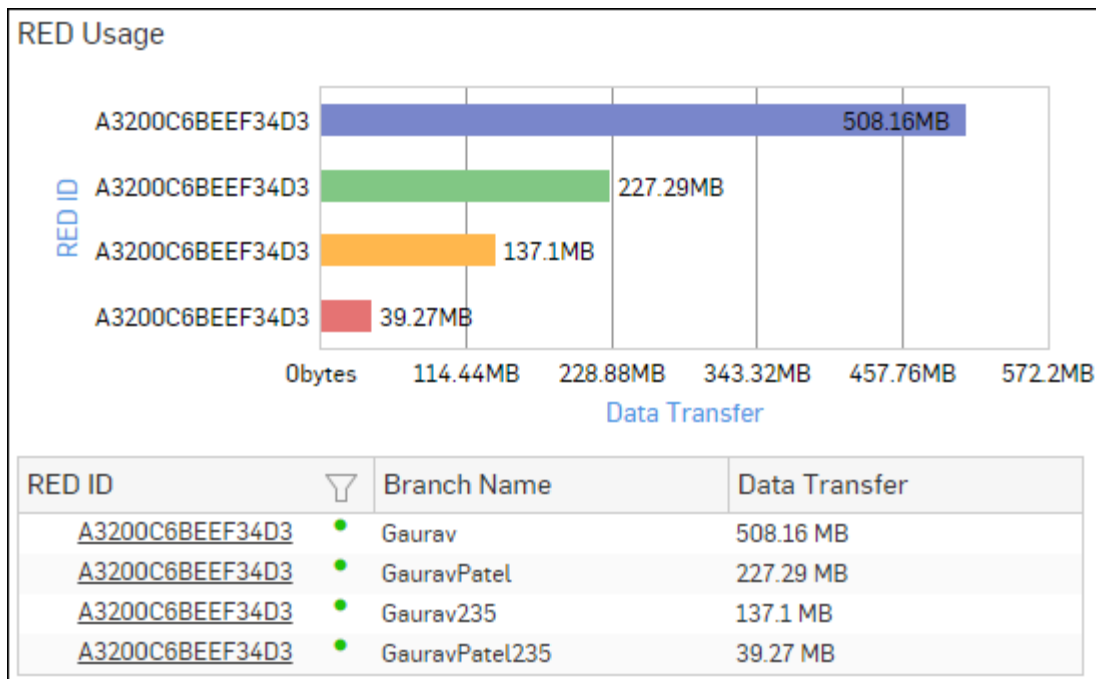


Figure 197: RED Usage

Click RED ID hyperlink in the table or graph to view the [RED Trend Report](#).

RED Trend Report

The report displays, for the selected RED Device, RED Usage statistics over the selected time period.

View report from **Monitor & Analyze > Reports > VPN > VPN > RED Usage > RED ID**.



Note: This report can also be viewed for **RED Usage by ID** from **Monitor & Analyze > Reports > VPN > VPN > Red Usage by ID > RED ID**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer over a time period, while the tabular report contains the following information:

- Time: Displays time in YYYY-MM-DD HH:MM:SS format.
- RED ID: Displays the unique ID of the RED Device.
- Branch Name: Displays branch name, as configured in the Sophos Firewall.
- RED Usage: For the selected RED Device, it displays amount of data transferred over the selected time period.

RED Usage by ID

This report provides an overview of the amount of data transferred through various RED Devices connected with the Sophos Firewall.



Note: This report will not display the information of branch names for same RED ID.

View report from VPN reports dashboard or from **Monitor & AnalyzeReportsVPNVPNRED Usage by ID**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per RED Device, while the tabular report contains the following information:

- RED ID: Displays the unique ID of the RED Device.

- Data Transfer: Amount of data transferred per RED Device.

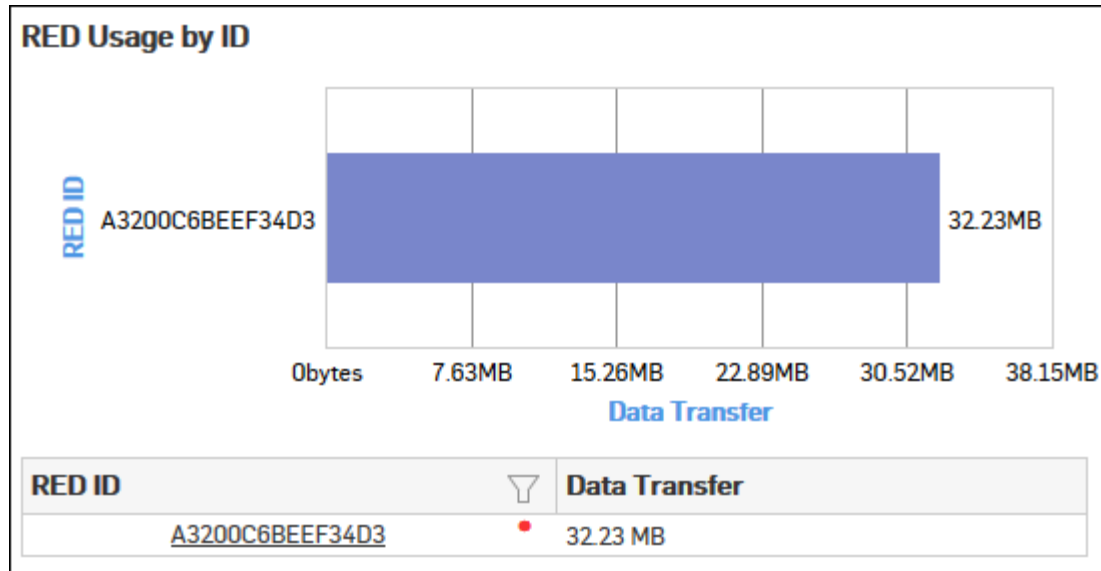


Figure 198: RED usage by ID

Click RED ID hyperlink in the table or graph to view the [RED Trend Report](#).

RED Disconnects

This report provides an overview of total number of times a RED Device was disconnected from the Sophos Firewall.



Note: Network Protection subscription is required to view the RED Disconnects reports. Without a valid subscription, some reports do not show any data.

View report from VPN reports dashboard or from **Monitor & AnalyzeReportsVPNVPNRED Disconnects**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays total number of times a RED Device was disconnected from the Sophos Firewall, while the tabular report contains the following information:

- RED ID: Displays the unique ID of the RED Device.
- Branch Name: Displays branch name, as configured in the Sophos Firewall.
- Total Disconnection: Total number of times the RED Device was disconnected from the Sophos Firewall.
- Duration of Disconnection: Total number of hours for which the RED Device was disconnected from the Sophos Firewall.
- Average Time: Displays the average disconnection time per RED Device. The time is calculated by dividing Duration of Disconnection with Total Disconnection.

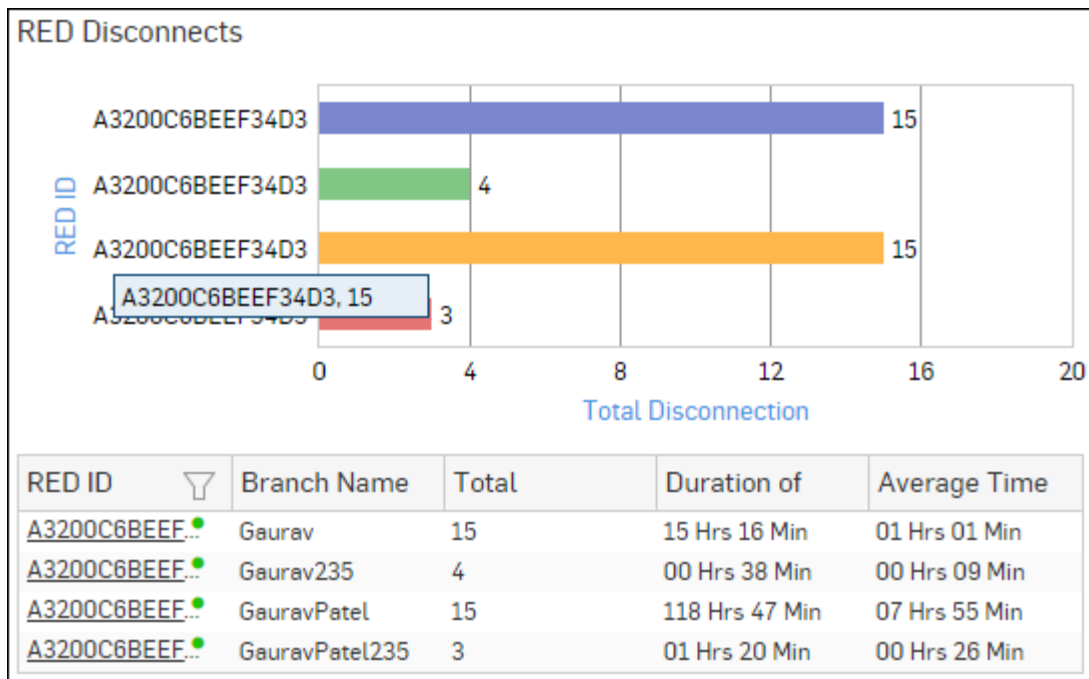


Figure 199: RED Disconnects

Click RED ID hyperlink in the table or graph to view the [RED Disconnects Detailed Report](#).

RED Disconnects Detailed Report

This report provides a detailed summary of disconnection details of the selected RED Device.

View report from **Monitor & Analyze > Reports > VPN > VPN > RED Disconnects > RED ID**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

For the selected RED Device, the tabular report contains following information:

- Time: Displays time in YYYY-MM-DD HH:MM:SS format.
- RED ID: Displays the unique ID of the RED Device.
- Branch Name: Displays branch name, as configured in the Sophos Firewall.
- Duration of Disconnection: Number of hours for which the RED Device was disconnected, per time period.

SSL VPN

The SSL VPN reports dashboard provide a snapshot of the network traffic generated by remote users connecting to the network through a remote SSL VPN client.

View the SSL VPN reports dashboard from **Monitor & Analyze > Reports > VPN > SSL VPN**.

It contains following reports in widget format:

- [Remote Access Users](#)
- [Site to Site Usage](#)

Remote Access Users

This report displays details of the users using the Remote Access VPN Type.

View report from SSL VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > SSL VPN > Remote Access Users**.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per user, while the tabular report contains the following information:

- User Name: Name of the user, as defined in the device.
- Connections: Number of connections per user.
- Data Transfer: Amount of data transferred (bytes sent + bytes received) per user.



Note: Data transfer is only displayed when the connection is terminated. Having shut down the connection, it takes a few minutes until the table contents is updated.

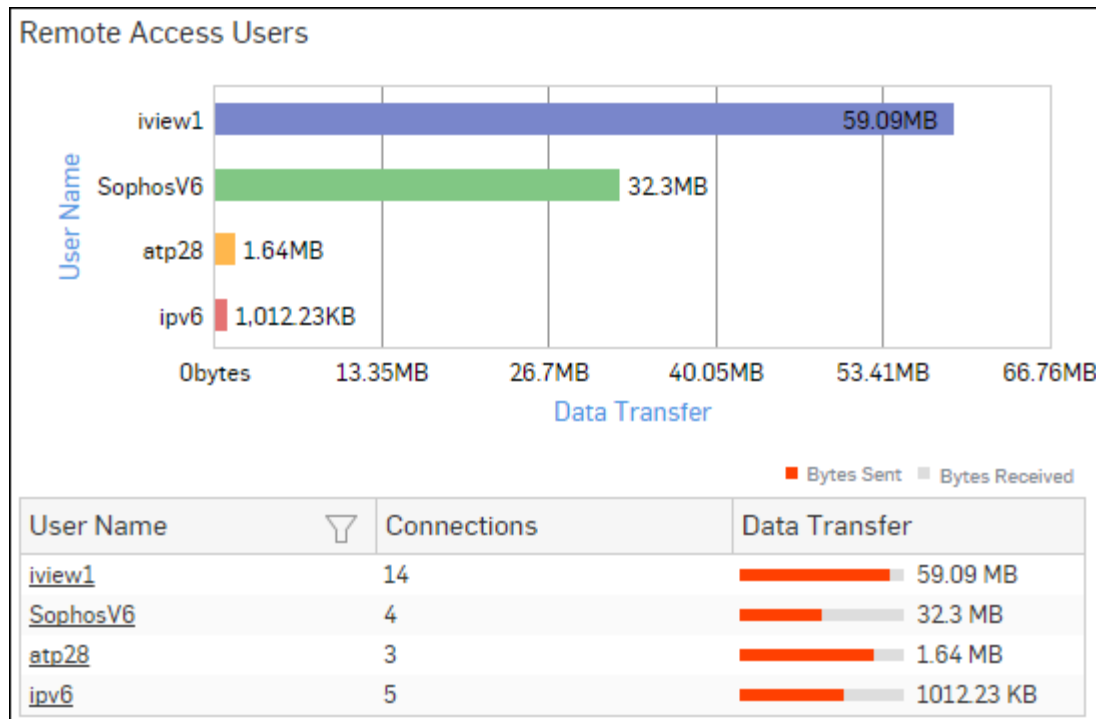


Figure 200: Remote Access Users

To view the following granular report of a particular remote access user, drill down by clicking **User Name** in the graph or the user name hyperlink in the table:

- [Remote Access - Connection details](#)

Remote Access - Connection details widget

This widget report displays, for the selected remote access user, details like source IP address and amount of data transferred.

The report is displayed as a graph as well as in a tabular format.

The tabular report contains the following information:

- Source IP Address: IP address of the source client.
- Data Transfer: Amount of data transferred (bytes sent + bytes received) for the selected remote access user.



Note: Data transfer is only displayed when the connection is terminated. Having shut down the connection, it takes a few minutes until the table contents is updated.

Site to Site Usage

This report displays information related to SSL VPN Site to Site Usage like name of the remote access connection, amount of data transferred per connection etc.

View report from SSL VPN reports dashboard or from **Monitor & Analyze > Reports > VPN > SSL VPN > Site to Site Usage**.

The report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the amount of data transfer per connection name, while the tabular report contains the following information:

- Connection Name: Name of the SSL VPN connection.
- Connections: Number of connections per connection name.
- Data Transfer: Amount of data transferred (bytes sent + bytes received) per connection name.



Note: Data transfer is only displayed when the connection is terminated. Having shut down the connection, it takes a few minutes until the table contents are updated.

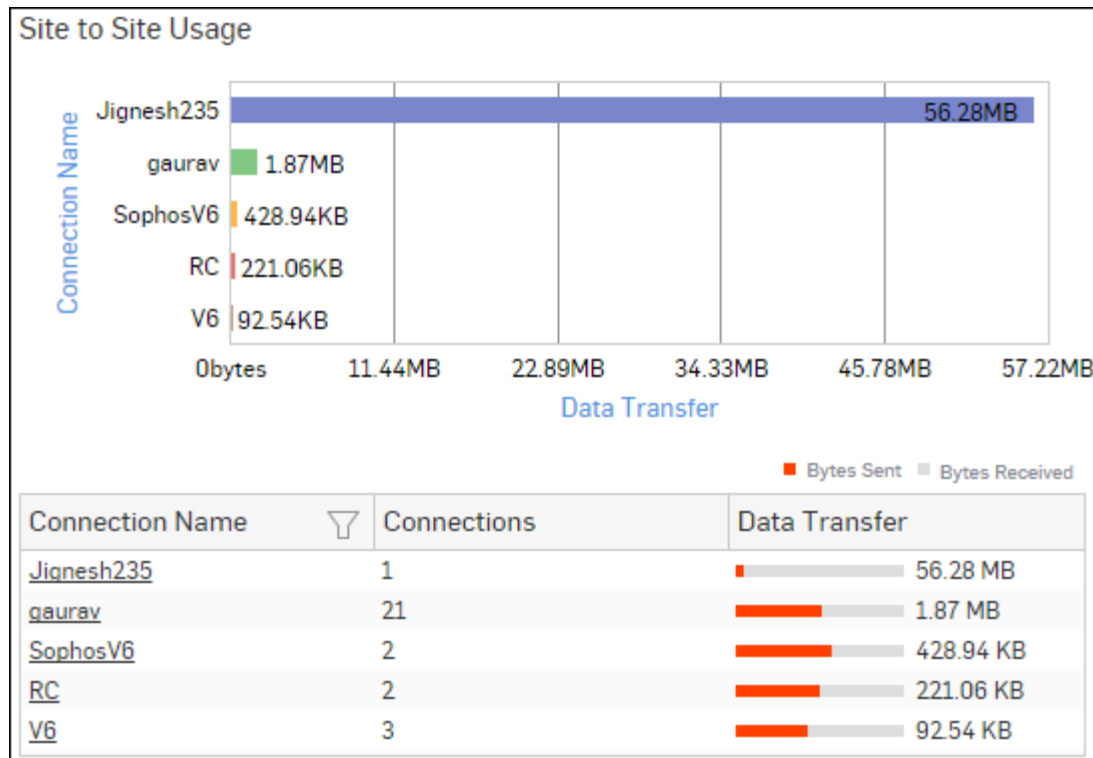


Figure 201: Site to Site Usage

Click Connection Name hyperlink in the table or graph to view the [Site to Site - Connection Details](#) report.

Site to Site - Connection Details widget

This widget report displays, for the selected Site to Site connection, details like IP addresses of local & remote interfaces and data transferred.

The report is displayed in a tabular format.

The tabular report contains the following information:

- Local Interface IP: IP address of the local interface.
- Remote Interface IP: IP address of the remote interface.
- Data Transfer: Amount of data transferred (bytes sent + bytes received) for the selected connection.



Note: Data transfer is only displayed when the connection is terminated. Having shut down the connection, it takes a few minutes until the table contents are updated.

Clientless Access

The Clientless Access reports dashboard provide a snapshot of the network traffic generated by remote users using a web browser i.e., clientless access.

View the reports dashboard from **Monitor & Analyze > Reports > VPN > Clientless Access**.

It enables to view traffic generated by:

- [Web Access Users](#)
- [Denied Web Access Users](#)
- [Denied Web Access Resources](#)

Web Access Users

This report displays details of the users using the Clientless Access SSL VPN Type.

View report from Clientless Access reports dashboard or from **Monitor & Analyze > Reports > VPN > Clientless Access > Web Access Users**.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The bar graph displays the number of hits per user, while the tabular report contains the following information:

- User Name: Name of the user, as defined in the Device.
- Hits: Number of hits per user.

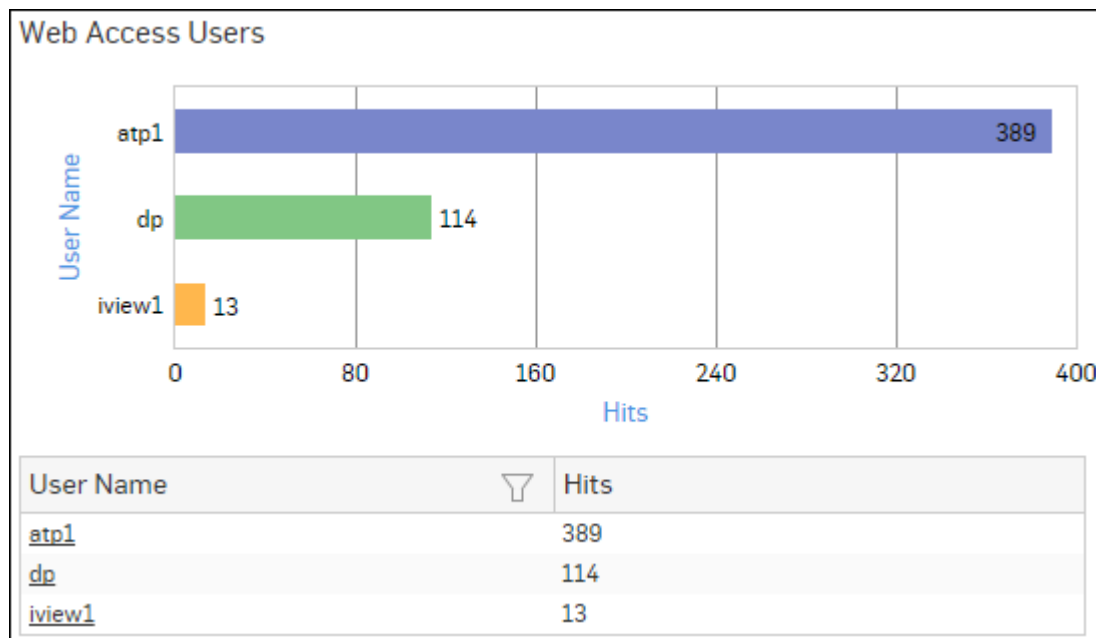


Figure 202: Web Access Users

Click User Name hyperlink in the table or graph to view [Web Access Details](#) report.

Web Access Details

This report displays, for the selected user, details like Source IP Address, URL/IP & type of the accessed resource.

View report from **Monitor & Analyze > Reports > VPN > Clientless Access > Web Access Users > User Name**.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Report date can be changed from the top most row of the page.

The tabular report contains the following information:

- Source IP Address: IP Address of the source client.
- Resource URL/IP: URL/IP Address of the accessed resource.
- Resource Type: Type of the accessed resource.

Denied Web Access Users

This Report displays a list of the Denied Web Users along with the number of hits.

View report from Clientless Access reports dashboard or from **Monitor & Analyze > Reports > VPN > Clientless Access > Denied Web Access Users**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of denied connections per Web Access User while the tabular report contains following information:

- User Name: Username of the denied Web Access user.
- Hits: Number of hits denied per user.

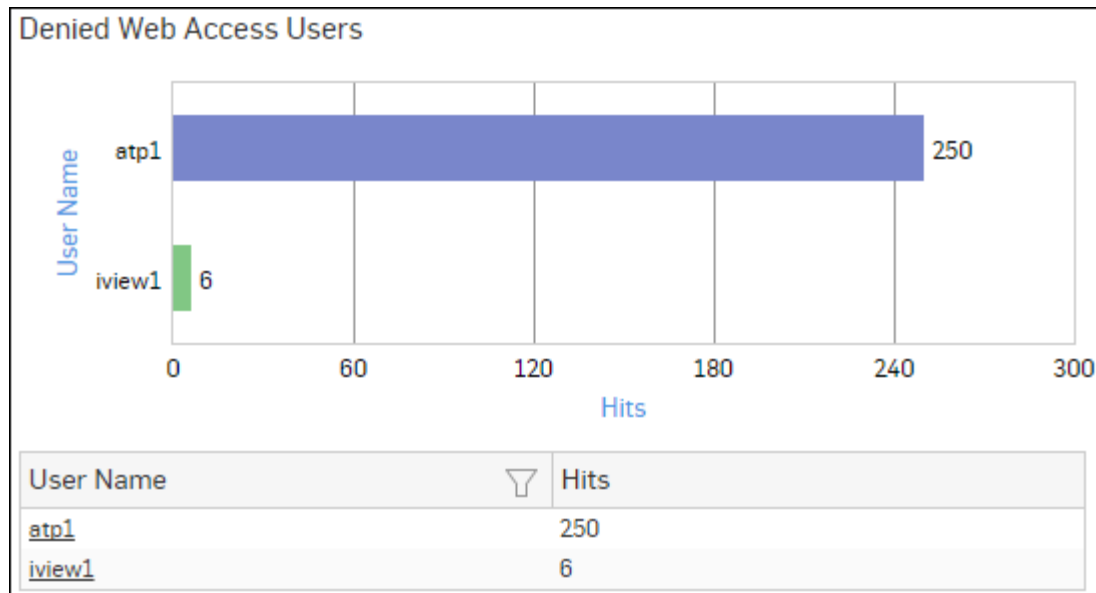


Figure 203: Denied Web Access Users

Click User Name hyperlink in the table or graph to view [Denied Web Access Details](#) report.

Denied Web Access Details

This Report displays a list of the resource URL/ IP Address along with the source IP Address and the number of hits.

View the report from **Monitor & Analyze > Reports > VPN > Clientless Access > Denied Web Access Users > User Name**.

The bar graph displays the number of times the access to a particular resource URL was denied while the tabular report contains the following information:

- Resource URL/IP: URL name or IP Address of the resource URL.
- Source IP: IP Address of the source.
- Hits: Number of denied hits per resource.

Denied Web Access Resources

This Report displays a list of the resource URL or IP Addresses along with the number of hits.

View report from Clientless Access reports dashboard or from **Monitor & Analyze > Reports > VPN > Clientless Access > Denied Web Access Resources**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the number of hits per resource URL while the tabular report contains the following information:

- Resource URL/IP: URL name or IP Address of resource URL.

- Hits: Number of hits per Resource URL/IP.

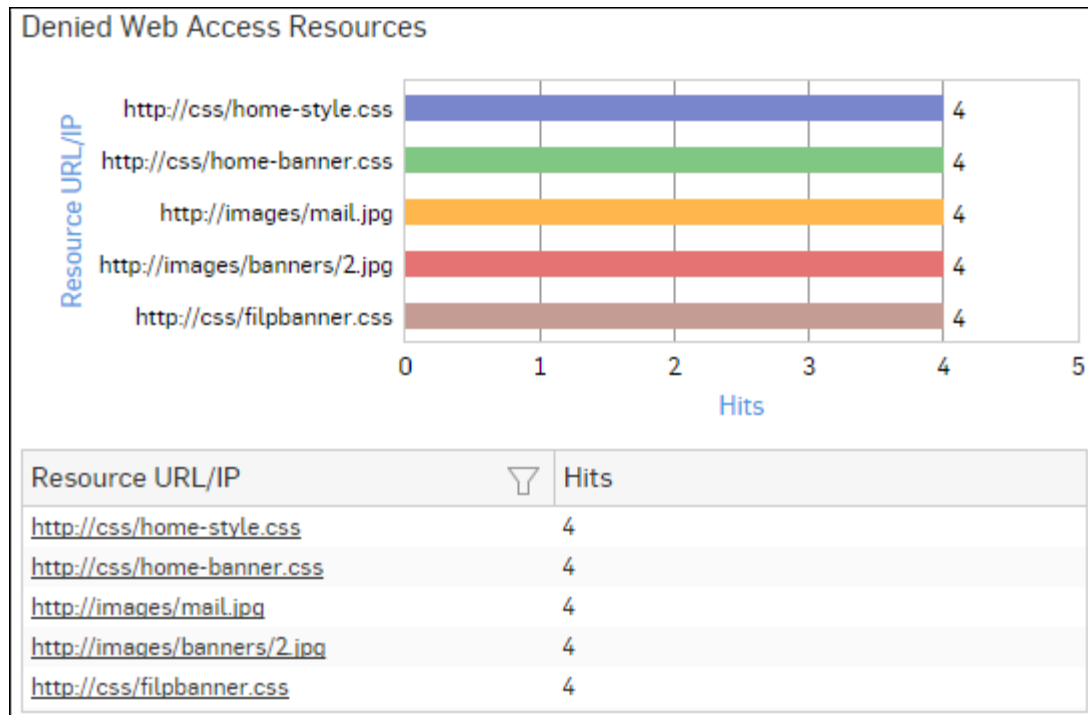


Figure 204: Denied Web Access Resources

Click Resource URL/IP hyperlink in the table or graph to view [Denied Web Access Details](#) report.

Denied Web Access Details

This Report displays a list of the resource URL/ IP Address along with the number of hits.

View the report from **Monitor & Analyze > Reports > VPN > Clientless Access > Denied Web Access Resources > Resource URL/IP**.

The bar graph displays the number of times the access to a particular user was denied while the tabular report contains the following information:

- User Name: Username of the denied Web Access user.
- Source IP: IP Address of the source.
- Hits: Number of denied hits per user.

Email

The Email reports provide snapshot of Email based traffic through your network.

The reports help to identify high volume traffic generators who are affecting the overall network traffic and provides statistics based on the traffic generated by Emails. In addition, the reports provide an overview of the traffic generated by Spam and Virus Emails.



Note: Email Protection subscription is required to view all the Email reports. Without a valid subscription, some reports do not show any data. The Email sub sections can be accessed by selecting drop-down 1 given at the upper left corner of the page.

Email Reports are further divided into two sub-sections:

- [Email Usage](#)
- [Email Protection](#)

Email Usage

The Email Usage reports dashboard provides snapshot of Email based traffic through your network.

The reports help to identify high volume traffic generators who are affecting the overall network traffic and provides statistics based on the traffic generated by Emails.

These reports can help determine Email traffic behaviors and provide a basis for fine-tuning the configuration to efficiently control traffic flow.

View the Email Usage reports dashboard from **Monitor & Analyze > Reports > Email > Email Usage**

The Email Usage reports enable to view the traffic generated by:

- [Mail Senders](#)
- [Mail Recipients](#)
- [Mail Users](#)
- [Mail Hosts](#)
- [Mail Applications](#)
- [Source Countries](#)
- [Destination Countries](#)
- [Trend - Mail Usage](#)

Mail Senders

This Report displays a list of the top Email senders along with the number of emails that generate the most traffic for various users, destinations, hosts and applications.

View the report from Email Usage reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Mail Senders**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of emails sent.
- Bytes: Amount of data transferred.

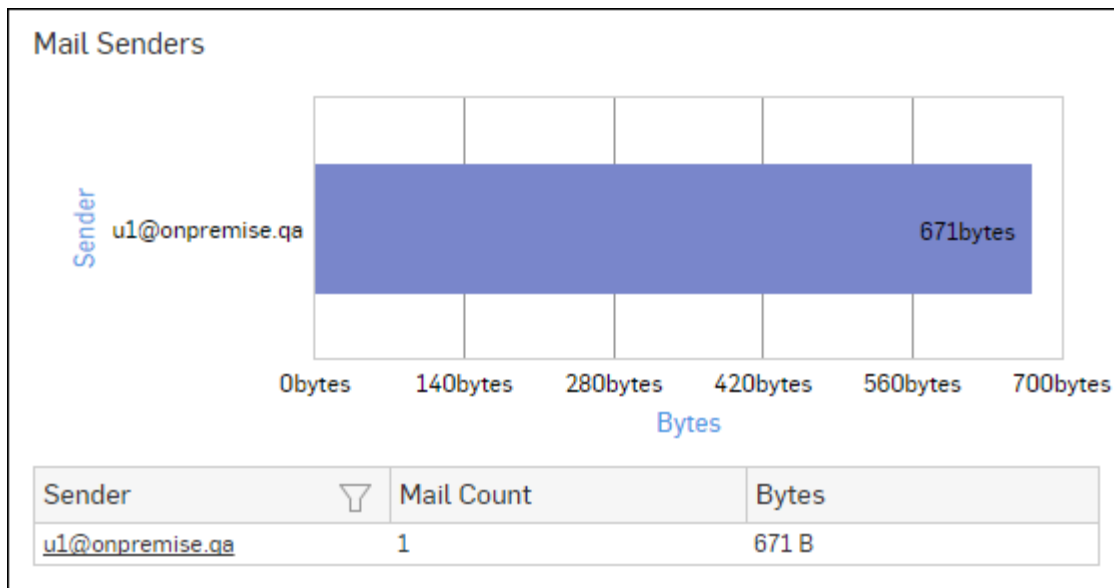


Figure 205: Mail Senders

Click the Sender hyperlink in the table or the graph to view the underlying level of reports:

- [Mail Recipients](#)
- [Mail Users](#)
- [Mail Hosts](#)
- [Mail Applications](#)
- [Source Countries](#)
- [Destination Countries](#)

Mail Recipients

This Report displays a list of the top Email recipients along with the number of emails that generate the most traffic for various users, destinations, hosts and applications.

View the report from Email Usage reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Mail Recipients**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred to each recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of emails received.
- Bytes: Amount of data transferred.

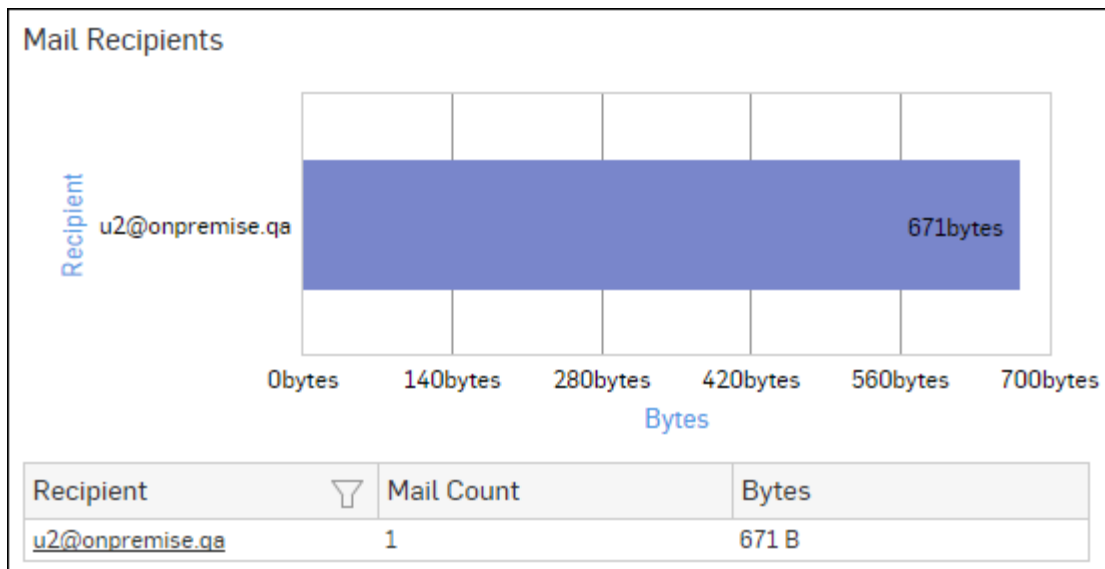


Figure 206: Mail Recipients

Click the Recipient hyperlink in the table or the graph to view the underlying level of reports:

- [Mail Senders](#)
- [Mail Users](#)
- [Mail Hosts](#)
- [Mail Applications](#)
- [Source Countries](#)
- [Destination Countries](#)

Mail Users

This Report displays a list of the top Email users along with the number of emails that generate the most traffic for various senders, recipients, destinations, hosts and applications.

View the report from Email Usage reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Mail Users**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each user while the tabular report contains the following information:

- User: Name of the user as defined in the Device. If the User is not defined, then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Mail Count: Number of emails per user.
- Bytes: Amount of data transferred.

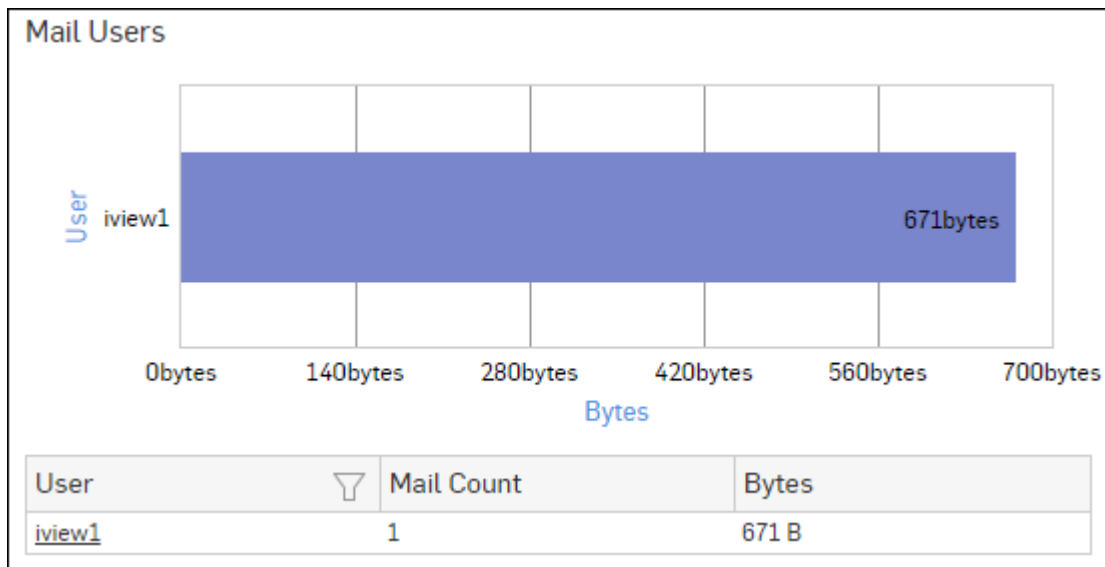


Figure 207: Mail Users

Click the User hyperlink in the table or the graph to view the underlying level of reports:

- [Mail Senders](#)
- [Mail Recipients](#)
- [Mail Hosts](#)
- [Mail Applications](#)
- [Source Countries](#)
- [Destination Countries](#)

Mail Hosts

This Report displays a list of the top Email hosts along with the number of emails that generate the most traffic for various senders, recipients, destinations, user and applications.

View the report from Email Usage reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Mail Hosts**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each user while the tabular report contains the following information:

- Host: IP Address of the host.
- Mail Count: Number of emails per host.
- Bytes: Amount of data transferred.

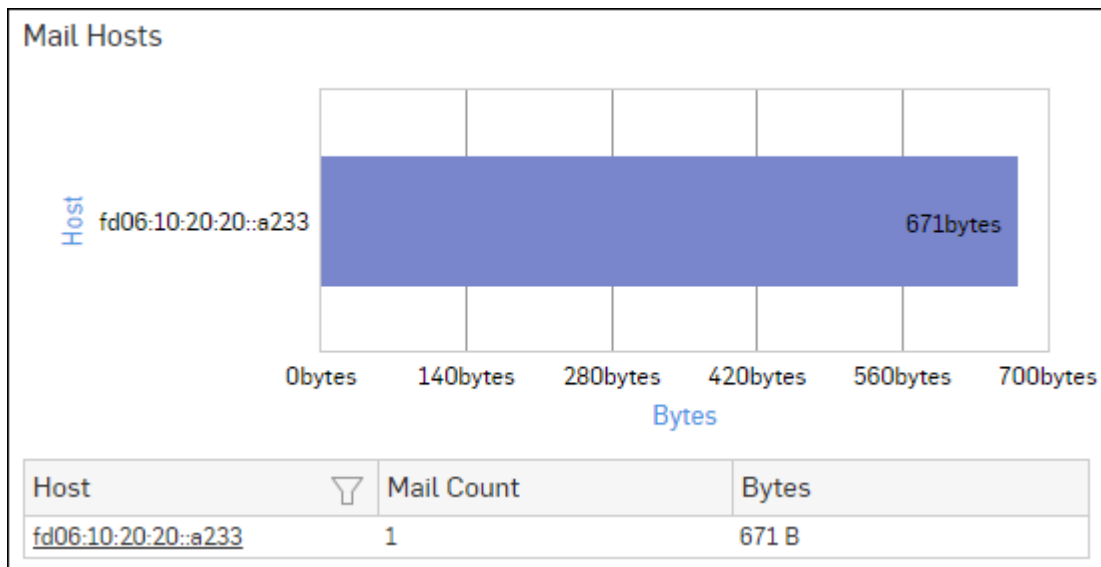


Figure 208: Mail Hosts

Click the Host hyperlink in the table or the graph to view the underlying level of reports:

- [Mail Senders](#)
- [Mail Recipients](#)
- [Mail Users](#)
- [Mail Applications](#)
- [Source Countries](#)
- [Destination Countries](#)

Mail Applications

This Report displays a list of the top Email applications along with the number of emails that generate the most traffic for various senders, recipients, users, destinations and hosts.

View the report from Email Usage reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Mail Applications**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each application while the tabular report contains the following information:

- **Application/Proto:Port:** Displays name of the application as defined in the Device. If application is not defined, then this field will display application identifier as combination of protocol and port number.
- **Mail Count:** Number of emails per application..
- **Bytes:** Amount of data transferred.

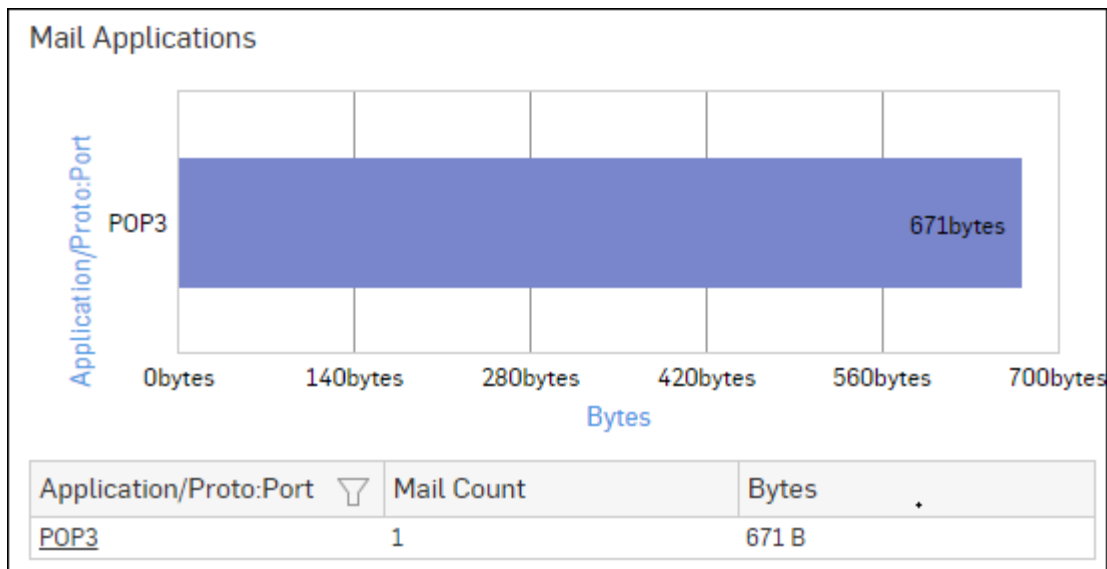


Figure 209: Mail Applications

Click the Application hyperlink in the table or the graph to view the underlying level of reports:

- [Mail Senders](#)
- [Mail Recipients](#)
- [Mail Users](#)
- [Mail Hosts](#)
- [Source Countries](#)
- [Destination Countries](#)

Source Countries

This Report displays a list of countries from where the maximum volume of email traffic is originated, along with number of emails and the total amount of data transfer per country.

View the report from Email Usage reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Source Countries**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each source country while the tabular report contains the following information:

- **Source Country:** Name of the source country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- **Mail Count:** Number of emails per country.
- **Bytes:** Amount of data transferred.

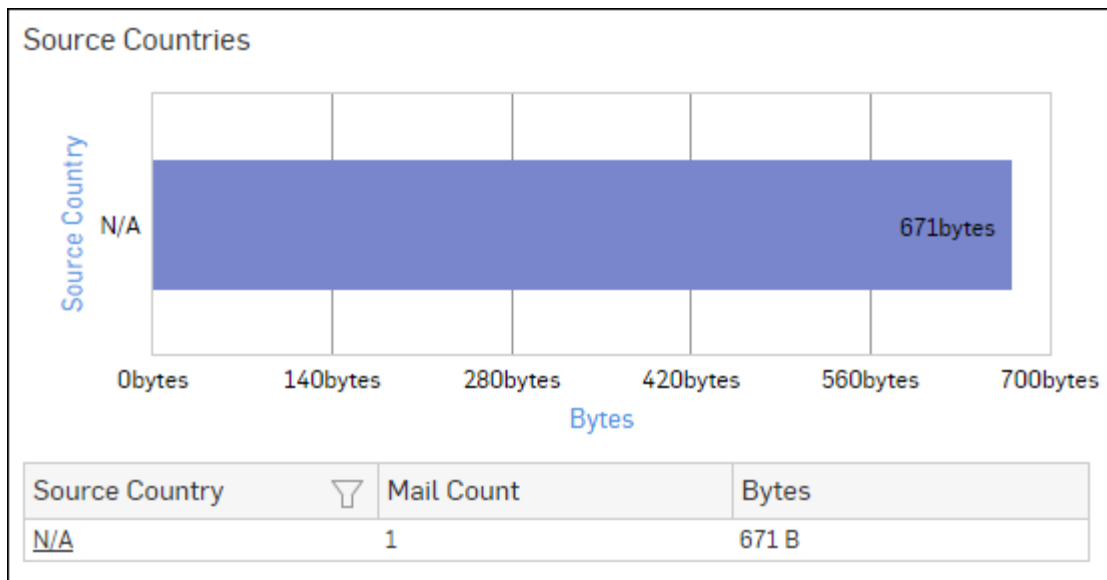


Figure 210: Source Countries

Click the Source Country hyperlink in the table or the graph to view the underlying level of reports:

- [Mail Senders](#)
- [Mail Recipients](#)
- [Mail Users](#)
- [Mail Hosts](#)
- [Mail Applications](#)
- [Destination Countries](#)

Destination Countries

This Report displays a list of those countries which are destined to most of the email traffic along with number of emails and the total amount of data transfer per country.

View the report from Email Usage reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Destination Countries**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each destination country while the tabular report contains the following information:

- **Destination Country:** Name of the destination country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- **Mail Count:** Number of emails per country.
- **Bytes:** Amount of data transferred.

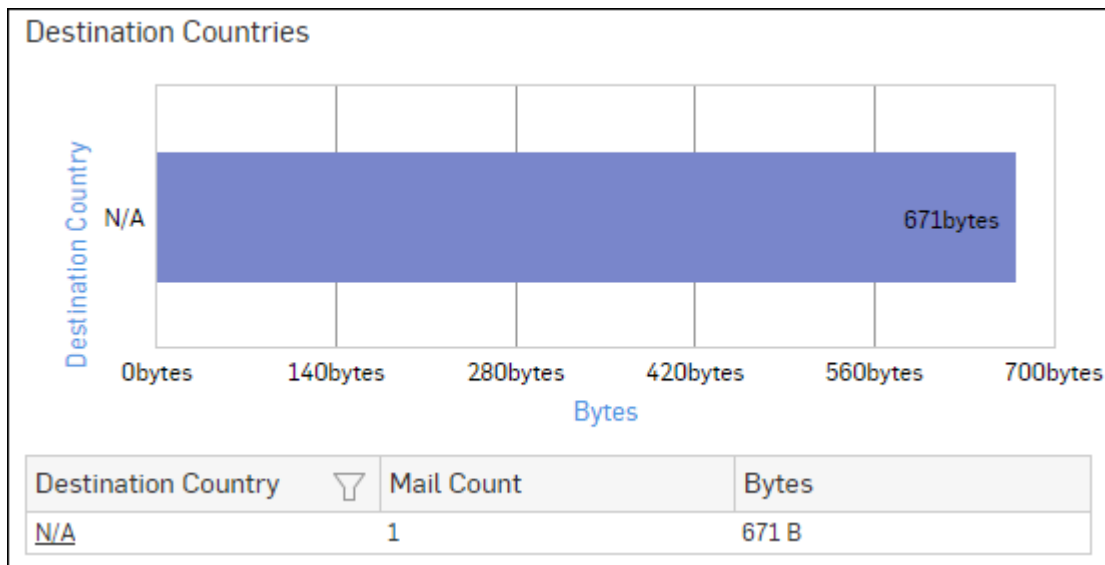


Figure 211: Destination Countries

Click the Destination Country hyperlink in the table or the graph to view the underlying level of reports:

- [Mail Senders](#)
- [Mail Recipients](#)
- [Mail Users](#)
- [Mail Hosts](#)
- [Mail Applications](#)
- [Source Countries](#)

Trend - Mail Usage

This report provides mail usage trend in terms of number of mail usage event per time period.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Usage > Trend - Mail Usage**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays mail usage event trend per time while the tabular report displays following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- Event Type: Displays event type i.e. Mail Usage.
- Event: Number of events per time period.

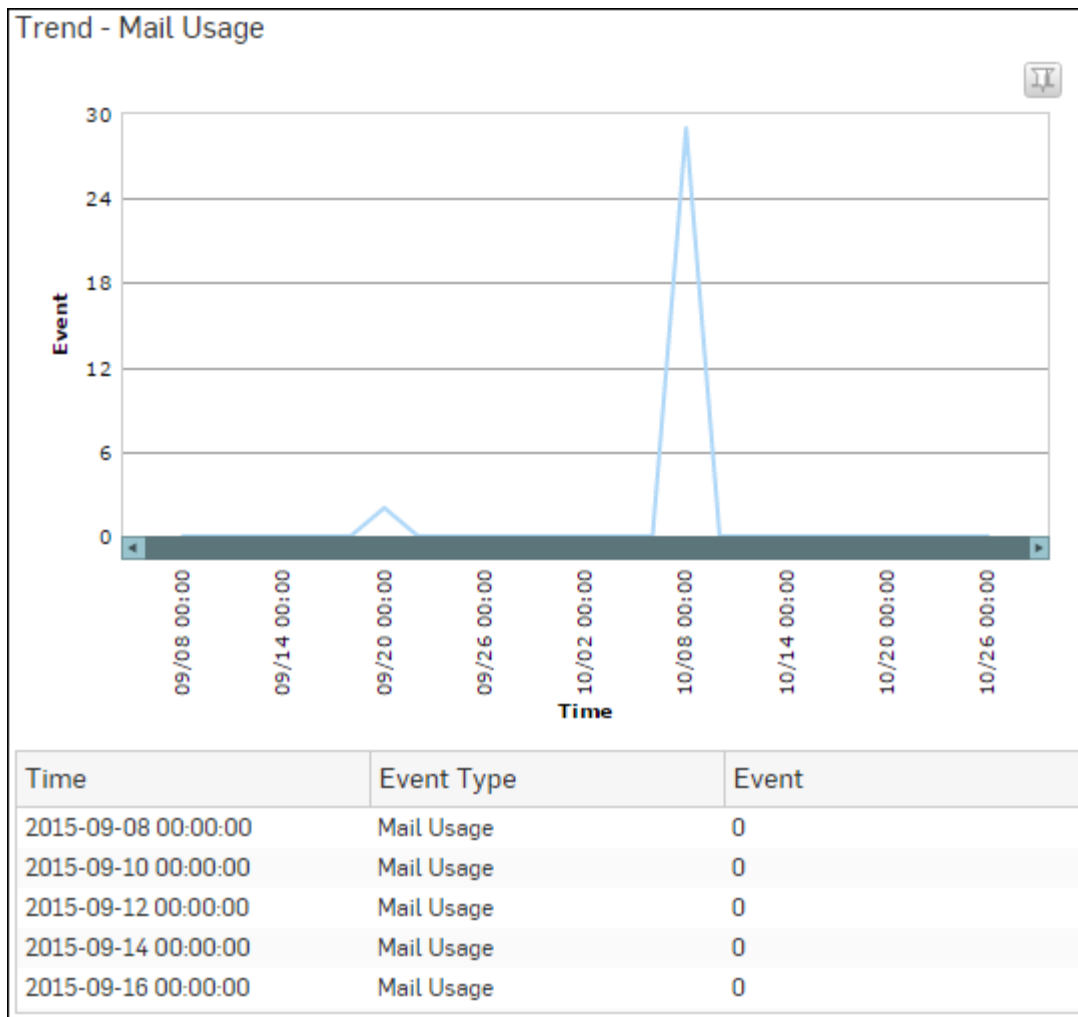


Figure 212: Trend - Mail Usage

Filtered Email Usage Reports

The Email Usage Reports can be filtered to get the following set of reports.

- [Mail Senders](#)
- [Mail Recipients](#)
- [Mail Users](#)
- [Mail Hosts](#)
- [Mail Applications](#)
- [Source Countries](#)
- [Destination Countries](#)

To view the Filtered Email Usage reports, you need to choose one of the following filter criteria:

- Sender from [Mail Senders Report](#)
- Recipient from [Mail Recipients Report](#)
- User from [Mail Users Report](#)
- Host from [Mail Hosts Report](#)
- Application from [Mail Applications Report](#)
- Country from [Source Countries Reports](#)
- Country from [Destination Countries Report](#)

Based on the filter criterion, reports will be displayed in the following format:

- Summary - Reports in graphical format
- Details - Reports in tabular format

The Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered. Detailed Reports are displayed in tabular format which can be filtered by clicking hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Mail Senders widget

This Widget Report displays a list of the top Email senders along with the number of emails and amount of data transfer.



Note: This widget will not be displayed for filter criterion Sender.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of emails sent.
- Bytes: Amount of data transferred.

Mail Recipients widget

This Widget Report displays a list of the top Email recipients along with the number of emails and amount of data transfer.



Note: This widget will not be displayed for filter criterion 'Recipient'.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of emails received.
- Bytes: Amount of data transferred.

Mail Users widget

This Widget Report displays a list of the top Email users along with the number of emails and amount of data transfer.



Note: This widget will not be displayed for filter criterion User.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each user while the tabular report contains the following information:

- User: User name as defined in the Device.
- Mail Count: Number of emails per user.
- Bytes: Amount of data transferred.

Mail Hosts widget

This Widget Report displays a list of the top Email hosts along with the number of emails and amount of data transfer.



Note: This widget will not be displayed for filter criterion Host.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each host while the tabular report contains the following information:

- Host: Host IP Address of the host.
- Mail Count: Number of emails per host.
- Bytes: Amount of data transferred.

Mail Applications widget

This Widget Report displays a list of the top applications along with the number of emails and amount of data transfer.



Note: This widget will not be displayed for filter criterion Application.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each application while the tabular report contains the following information:

- Application/Proto:Port: Name of the application.
- Mail Count: Number of emails per application..
- Bytes: Amount of data transferred.

Source Countries widget

This widget displays a list of countries from where the maximum volume of email traffic is originated, along with number of emails and the total amount of data transfer per country.



Note: This widget will not be displayed for filter criterion Source Country.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each source country while the tabular report contains the following information:

- Source Country: Name of the source country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Mail Count: Number of emails per country.
- Bytes: Amount of data transferred.

Destination Countries widget

This widget displays a list of those countries which are destined to most of the email traffic along with number of emails and the total amount of data transfer per country.



Note: This widget will not be displayed for filter criterion Destination Country.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the amount of data transferred by each destination country while the tabular report contains the following information:

- Destination Country: Name of the destination country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.

- Mail Count: Number of emails per country.
- Bytes: Amount of data transferred.

Email Protection

The Email Protection reports dashboard provides a snapshot of Virus and Spam infected mail traffic through your network.

The report provide an overview of the traffic generated by Spam and Email viruses.

These reports can help to determine Email traffic behavior and provide a basis for fine-tuning the configuration to efficiently control the traffic flow.

The Email Protection reports dashboard enables to view the traffic generated by:

- [Spam Recipients](#)
- [Spam Senders](#)
- [Outbound Spam Recipients](#)
- [Outbound Spam Senders](#)
- [Applications used for Spam](#)
- [Spam Sending Countries](#)
- [Spam Receiving Countries](#)
- [Mail Virus by Application Type](#)
- [Mail Virus](#)
- [Users - Mail Virus](#)
- [Mail Virus Senders](#)
- [Mail Virus Recipients](#)
- [Hosts - Mail Virus Senders](#)
- [Hosts - Mail Virus Recipients](#)
- [SPX Summary](#)
- [Trend - SPX](#)
- [Users\(SPX\)](#)
- [Senders\(SPX\)](#)
- [Recipients\(SPX\)](#)
- [Senders\(DLP\)](#)

Spam Recipients

This Report displays a list of Spam Recipients along with number of emails and percent distribution among the spam recipients.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Recipients**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Recipients** as well.

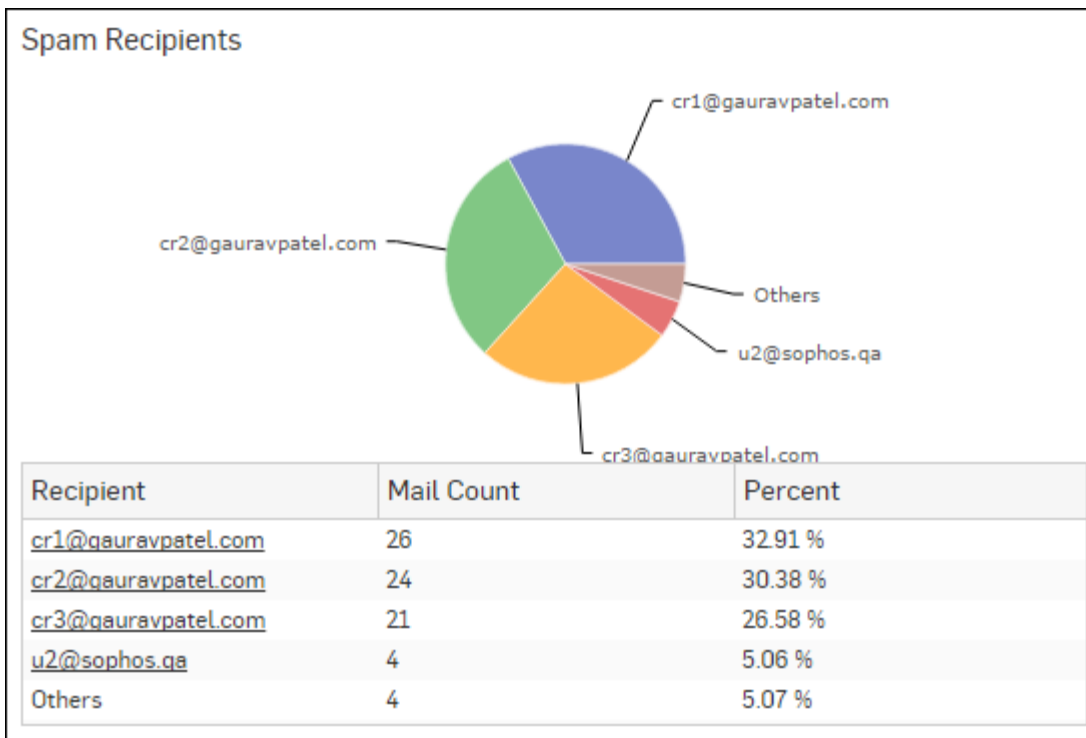
The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.
- Percent: Relative percent distribution among the spam recipients.

Figure 213: Spam Recipients



Click the Recipient hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Spam Senders

This Report displays a list of Spam Senders along with number of emails and percent distribution among the spam senders.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Senders**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Senders** as well.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of spam emails sent.
- Percent: Relative percent distribution among the spam sender.

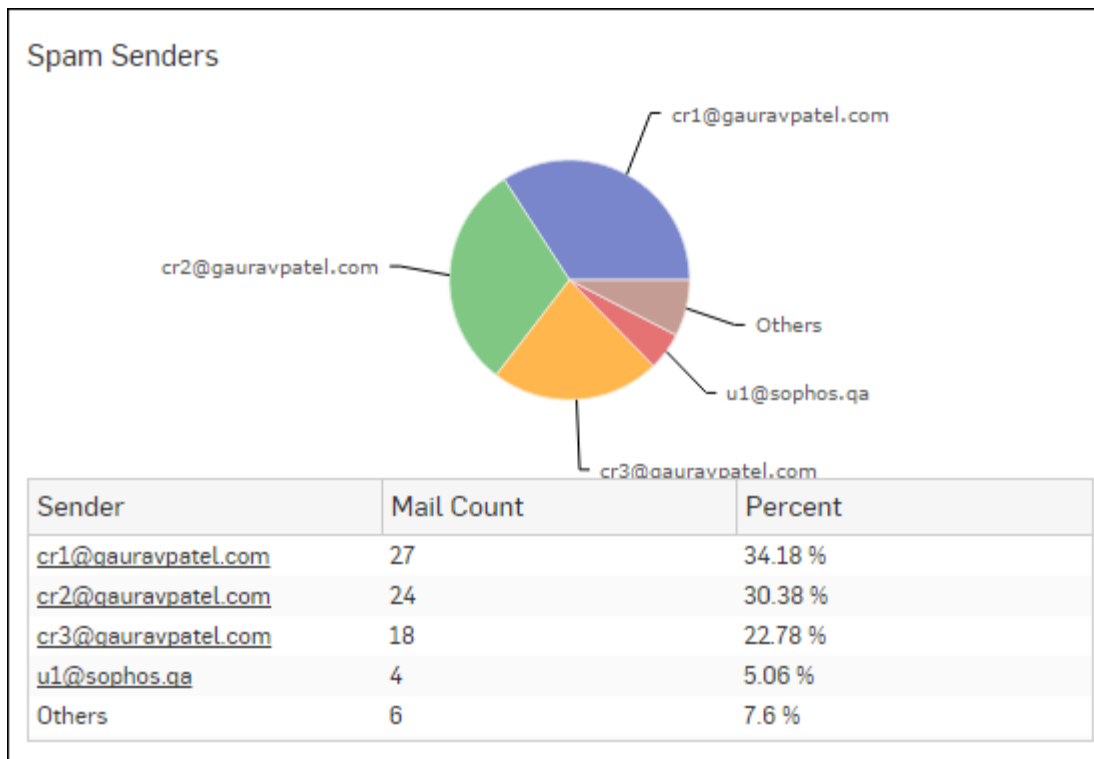


Figure 214: Spam Senders

Click the Sender hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Outbound Spam Recipients

This Report displays a list of Outbound Spam Recipients along with the number of emails and percent distribution among the recipients.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Outbound Spam Recipients**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of outbound spam per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.
- Percent: Relative percent distribution among the outbound spam recipients.

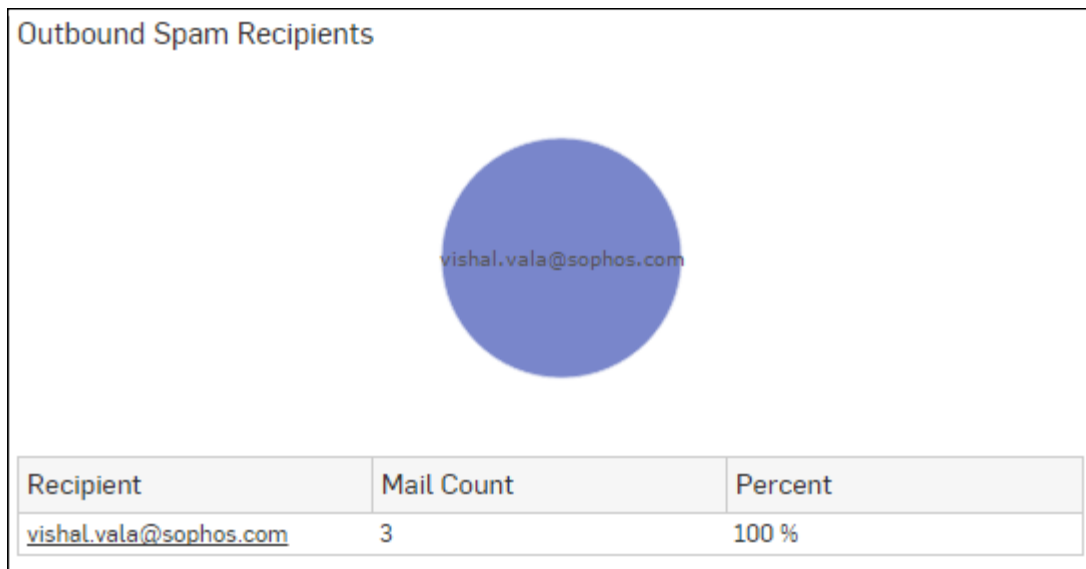


Figure 215: Outbound Spam Recipients

Click the Recipient hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Outbound Spam Senders

This Report displays a list of Outbound Spam Senders along with the number of emails and percent distribution among the senders..

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Outbound Spam Senders**.

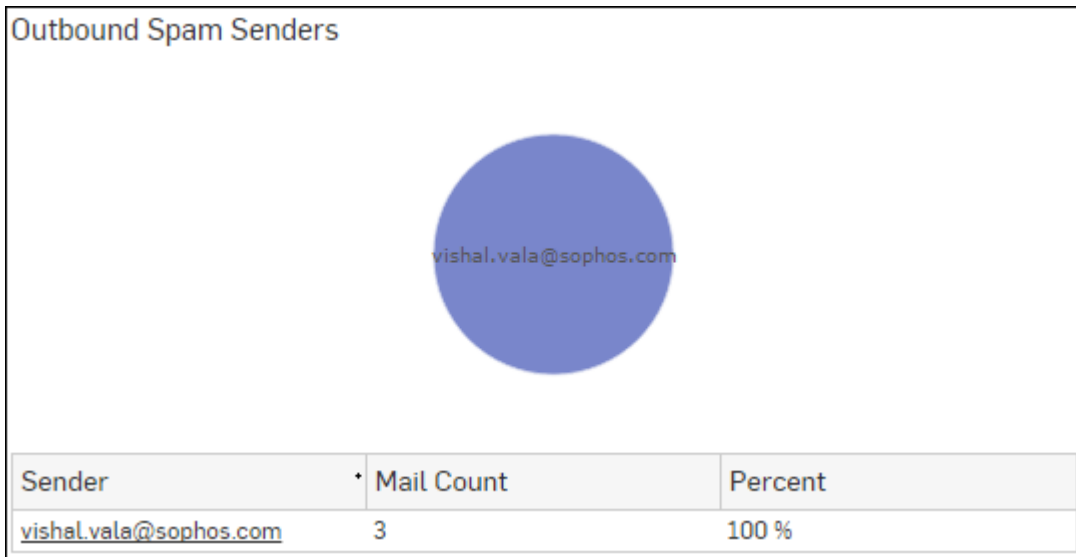
The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of outbound spam per sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of spam emails sent.
- Percent: Relative percent distribution among the outbound spam sender.

Figure 216: Outbound Spam Senders



Click the Sender hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Applications used for Spam

This Report displays a list of Applications used to generate Spam along with the number of emails.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Applications used for Spam**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of spam emails per application while the tabular report contains the following information:

- Application/Proto:Port: Displays the name of the application as defined in the Device. If application is not defined in the Device then this field will display application identifier as combination of the protocol and port number.
- Mail Count: Number of spam emails per application.

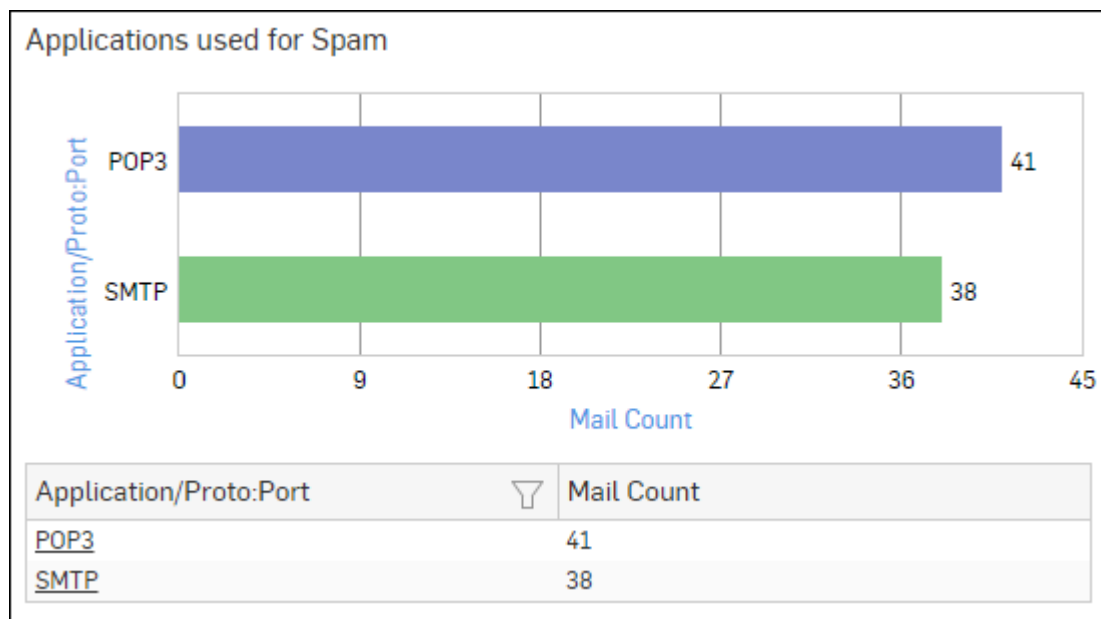


Figure 217: Applications used for Spam

Click the Application hyperlink in the table or graph to view the [Filtered Spam Reports](#).

Spam Sending Countries

This Report displays a list of countries from where the maximum volume of spam traffic is originated along with number of emails per country.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Sending Countries**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of spam emails sent per source country while the tabular report contains the following information:

- Source Country: Name of the spam sending country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Mail Count: Number of spam emails sent per country.

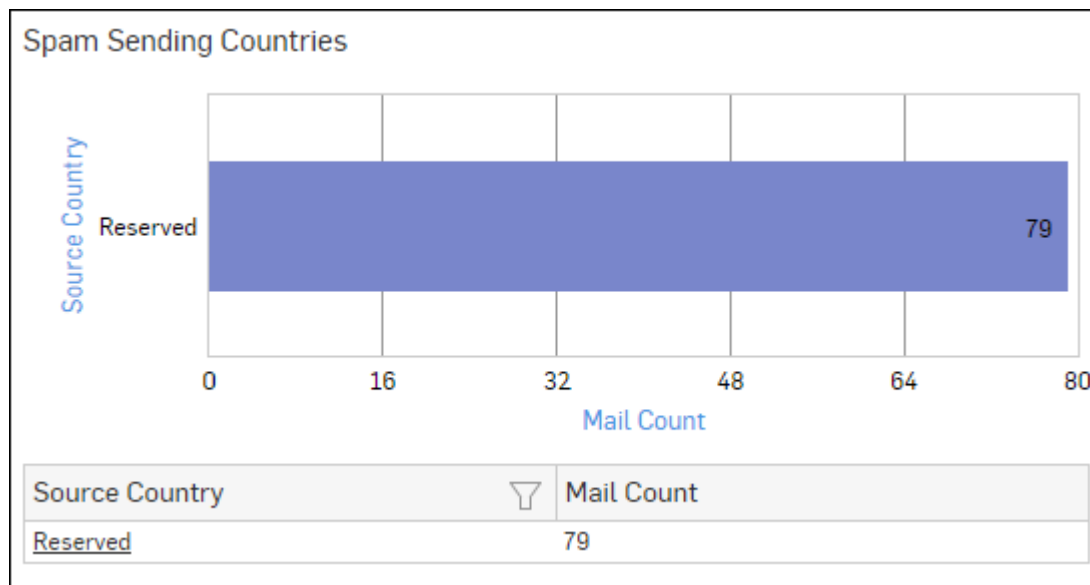


Figure 218: Spam Sending Countries

Click the Source Country hyperlink in the table or graph to view the [Filtered Spam Reports](#).

Spam Receiving Countries

This Report displays a list of those countries which are destined to most of the spam traffic along with number of emails per country.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Receiving Countries**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of spam emails received per destination country while the tabular report contains the following information:

- Destination Country: Name of the spam receiving country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Mail Count: Number of spam emails received per country.

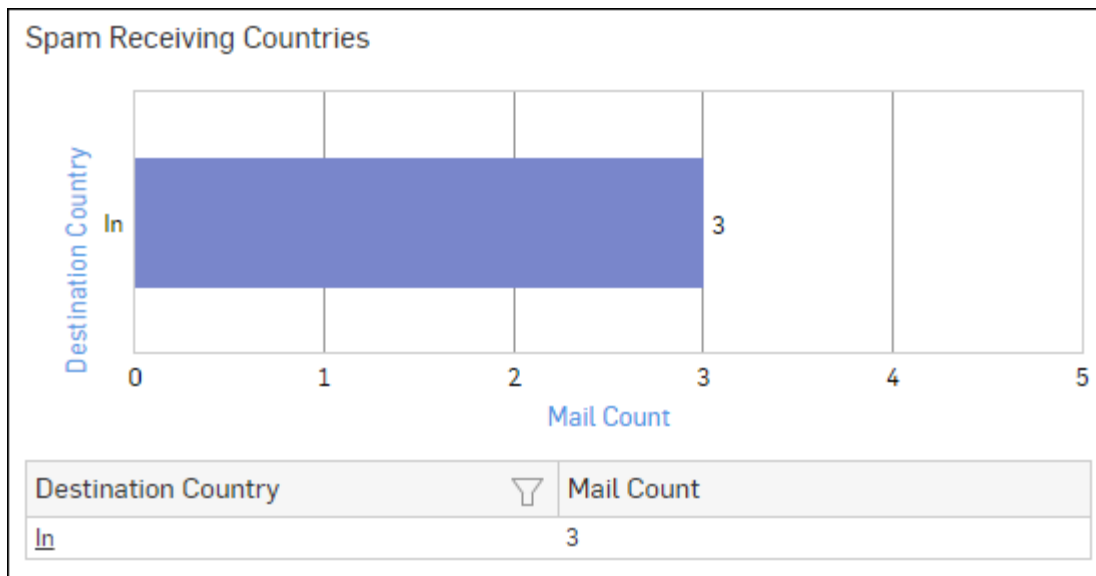


Figure 219: Spam Receiving Countries

Click the Destination Country hyperlink in the table or graph to view the [Filtered Spam Reports](#).

Mail Virus by Application Type

This Report provides an overview of mail viruses by their application type.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus by Application Type**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of email viruses per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the application, as defined in the Device. If the application is not defined in the Device then this field displays the application identifier as combination of protocol and port number.
- Count: Number of email viruses per application.

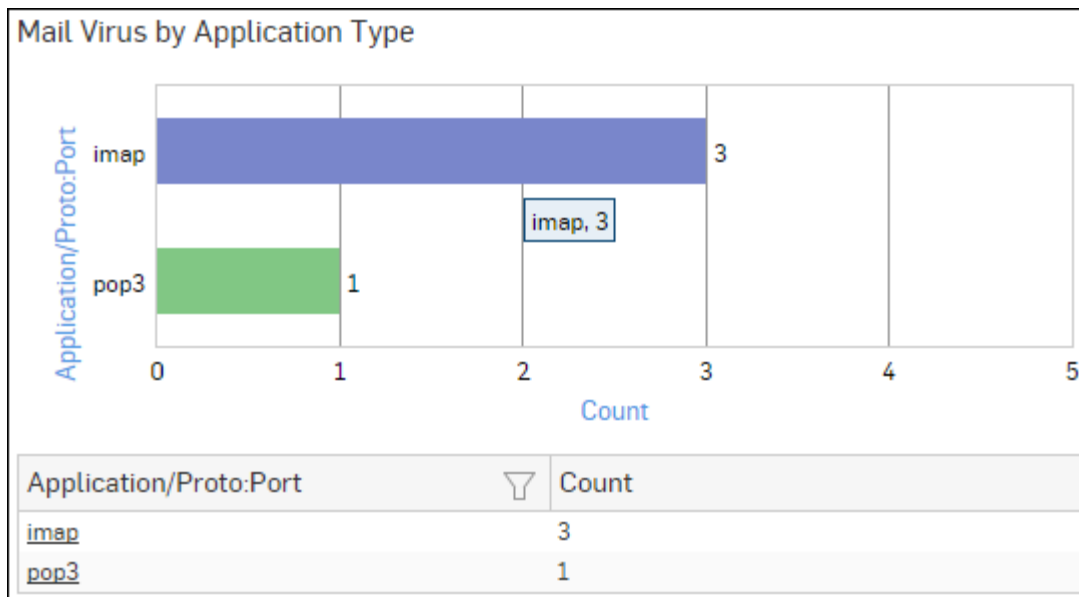


Figure 220: Mail Virus by Application Type

Click the Application hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Mail Virus

This Report displays Viruses detected in your network along with number of hits per Virus.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus while the tabular report contains the following information:

- Virus: Name of the virus.
- Count: Number of counts per mail virus.

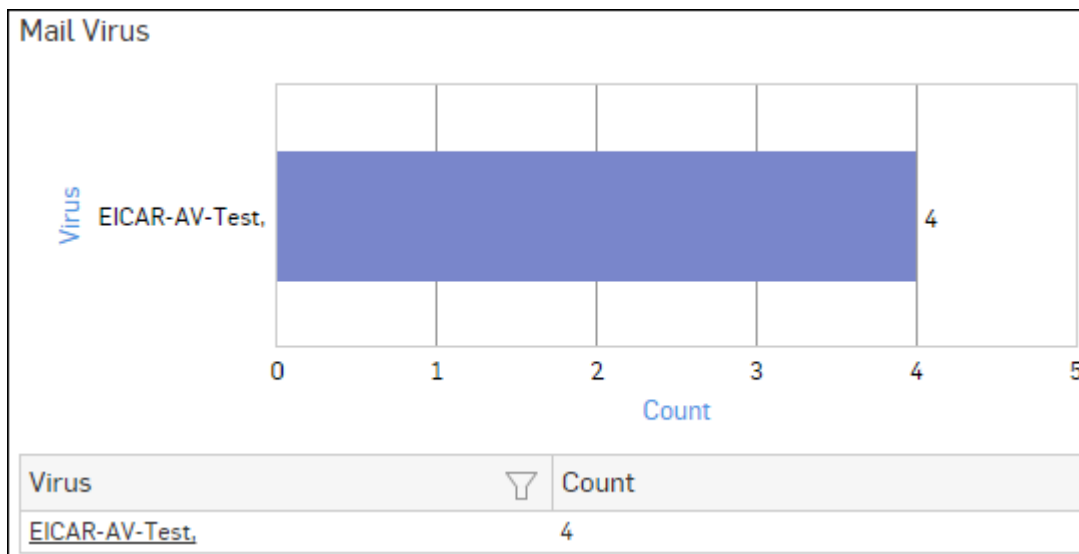


Figure 221: Mail Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Users - Mail Virus

This Report provides an overview of mail virus users along with number of counts per user.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Users - Mail Virus**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus user while the tabular report contains the following information:

- User: Name of the mail virus user.
- Count: Number of counts per mail virus user.

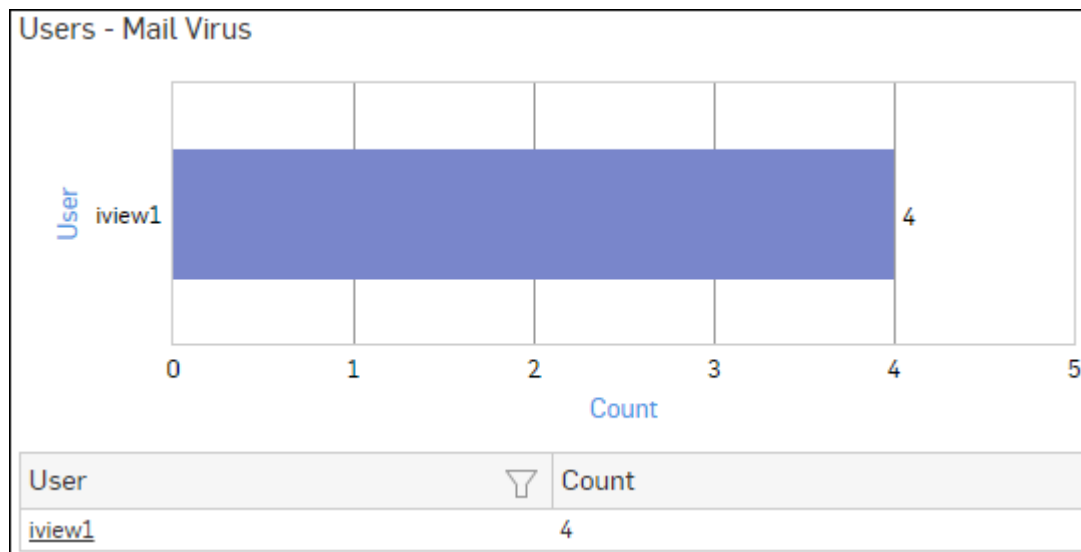


Figure 222: Users - Mail Virus

Click the User hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Mail Virus Senders

This Report displays mail virus senders along with number of hits per sender.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus Senders**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus sender while the tabular report contains the following information:

- Sender: Name of the mail virus sender.
- Count: Number of counts per mail virus sender.

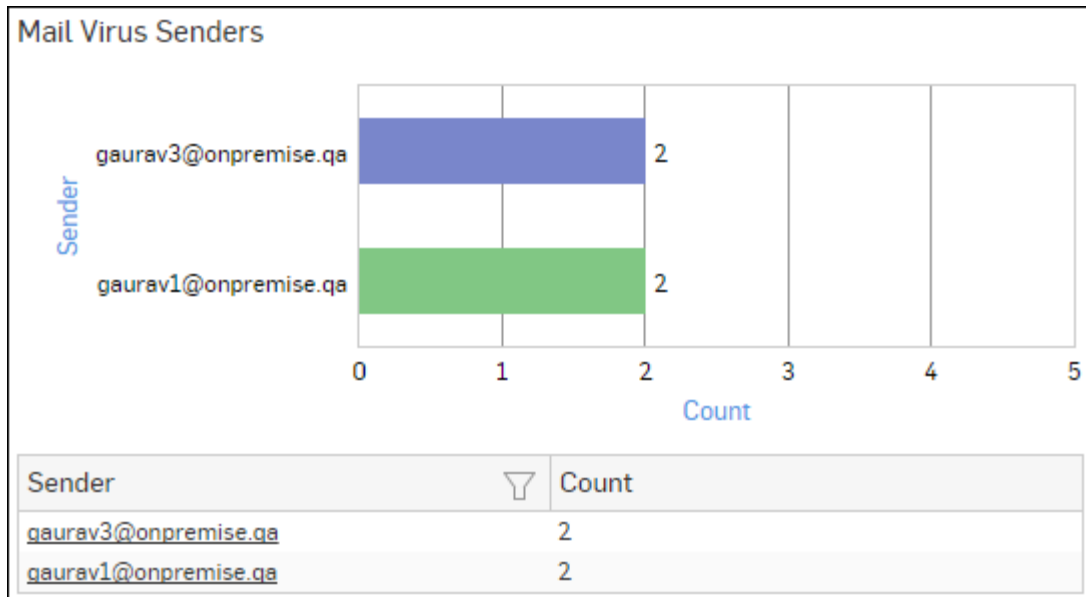


Figure 223: Mail Virus Senders

Click the Sender hyperlink in the table or graph to view the *Filtered Virus Reports*.

Mail Virus Recipients

This Report displays mail virus recipients along with number of hits per recipient.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus Recipients**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus recipient while the tabular report contains the following information:

- Recipient: Name of the mail virus recipient.
- Count: Number of counts per mail virus recipient.

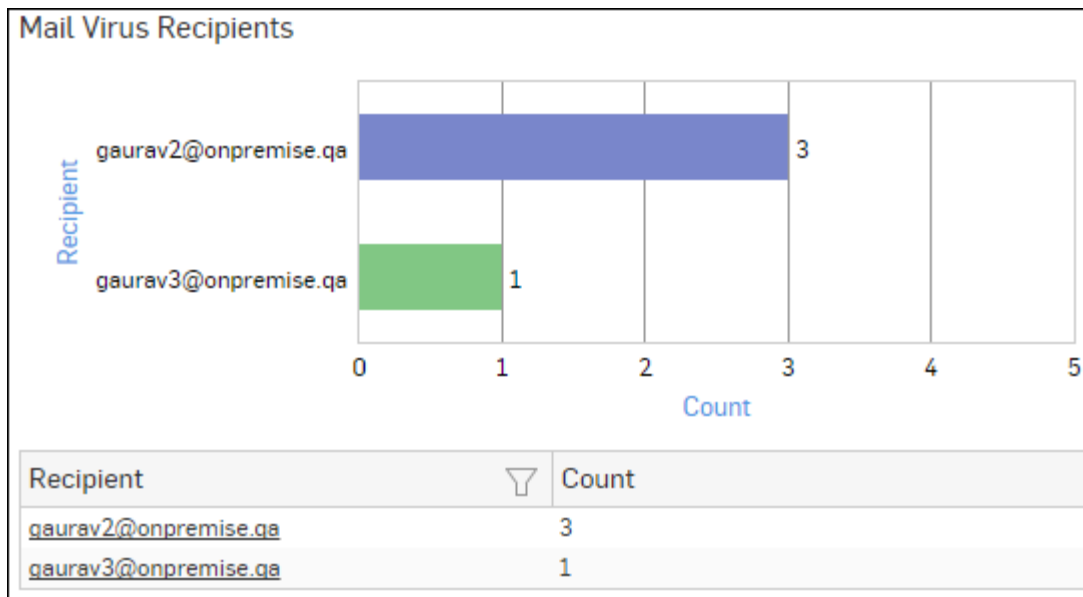


Figure 224: Mail Virus Recipients

Click the Recipient hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Hosts - Mail Virus Senders

This Report displays mail virus sender hosts along with number of hits per host.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Hosts - Mail Virus Senders**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus sender host while the tabular report contains the following information:

- Sender Host: IP Address of the mail virus sender host.
- Count: Number of counts per mail virus sender host.

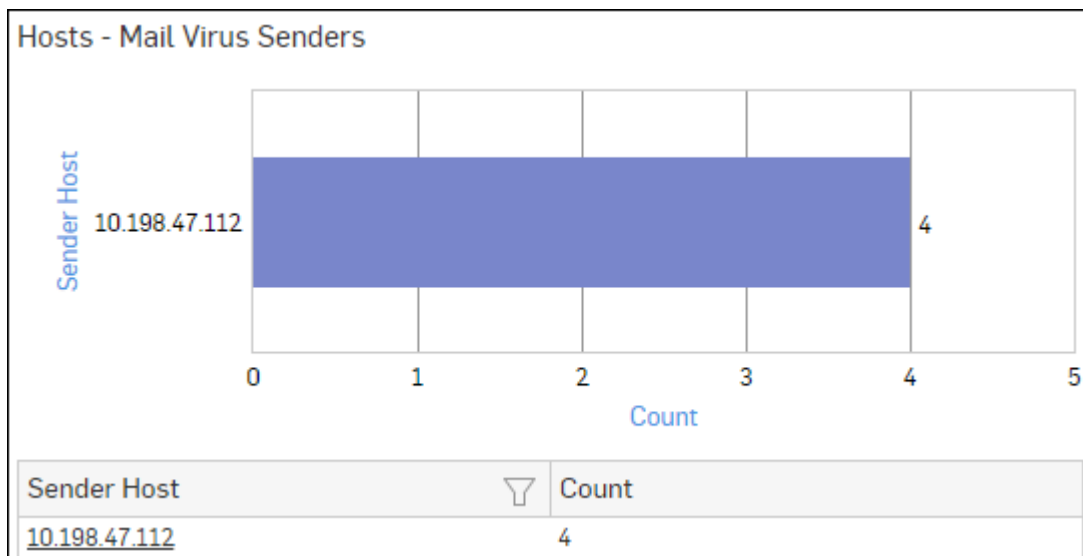


Figure 225: Hosts - Mail Virus Senders

Click the Sender Host hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Hosts - Mail Virus Recipients

This Report displays mail virus recipient hosts along with number of hits per host.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Hosts - Mail Virus Recipients**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus recipient host while the tabular report contains the following information:

- Receiver Host: IP Address of the mail virus recipient host.
- Count: Number of counts per mail virus recipient host.

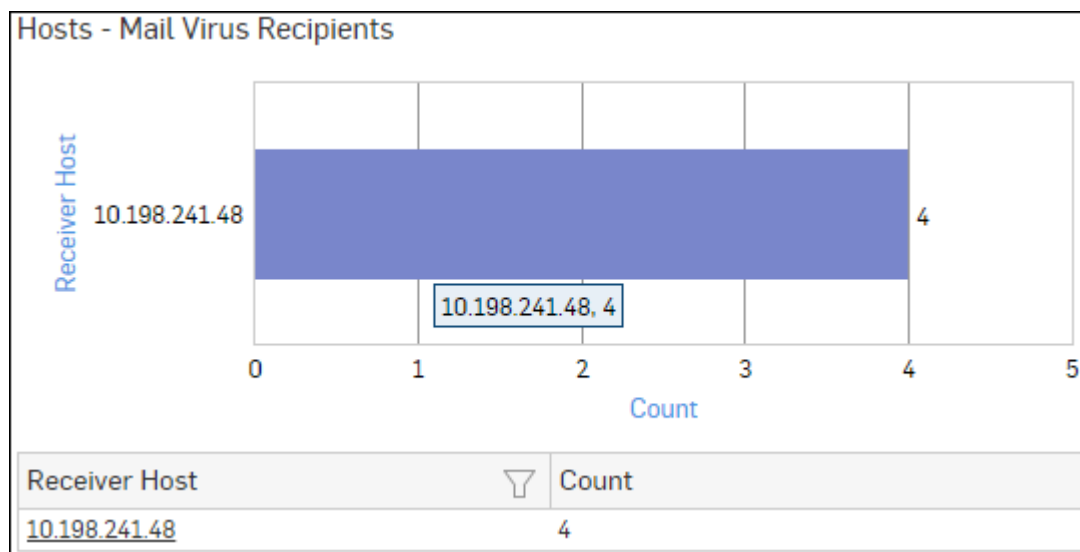


Figure 226: Hosts - Mail Virus Recipients

Click the Receiver Host hyperlink in the table or graph to view the [Filtered Virus Reports](#).

SPX Summary

This Report provides an overview of SPX email encryption used in mail communication in your network.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > SPX Summary**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays percent distribution among SPX Failed and Success parameters, while the tabular report displays following table:

- SPX Summary: Status of SPX usage. Possible options are:
 - Failed: SPX encryption failed.
 - Success: SPX encryption completed successfully.
- Count: Number of instances per SPX status.
- Percent: Percent distribution among SPX status.

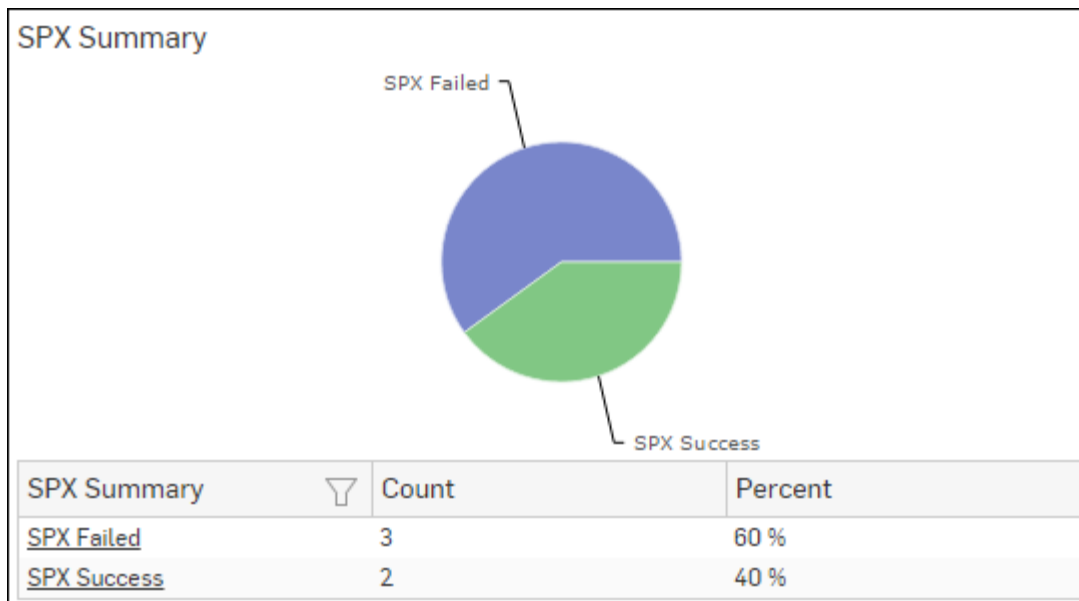


Figure 227: SPX Summary

Click any of the SPX status to view the [Filtered SPX Summary Report](#) for the selected SPX status.

Filtered SPX Summary Report

The SPX Summary Reports can be drilled down to get the following set of Filtered SPX Summary Reports in widget format:

- [SPX Success_Users](#)
- [SPX Success_Senders](#)
- [SPX Success_Recipients](#)
- [SPX Failed_Users](#)
- [SPX Failed_Senders](#)
- [SPX Failed_Recipients](#)

To view the Filtered SPX reports, you need to choose one of the following filter criteria:

- SPX Failed from [SPX Summary Report](#)
- SPX Success from [SPX Summary Report](#)

The Filtered SPX Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

SPX Success_Users widget

This widget report provides an overview of users who have successfully used SPX email encryption along with number of such mails per user.

View the report from **Monitor & Analyze > Reports > Email > Email Protection > SPX Summary > SPX Success**.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of mail count per user while the tabular report contains the following information:

- User: Name of the user using SPX email encryption.
- Mail Count: Number of mails (sent + received) with SPX email encryption, per user.

SPX Success_Senders widget

This widget report displays Email IDs of the users who have successfully sent mails encrypted with SPX encryption along with number of such mails sent per user.

View the report from **Monitor & Analyze > Reports > Email > Email Protection > SPX Summary > SPX Success.**

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of Email sent using SPX per user while the tabular report contains the following information:

- Sender: Email ID of the user using SPX email encryption.
- Mail Count: Number of mails sent using SPX email encryption, per user.

SPX Success_Recipients widget

This Widget report displays Email IDs of the users who have successfully received mails encrypted with SPX encryption along with number of such mails received per user.

View the report from **Monitor & Analyze > Reports > Email > Email Protection > SPX Summary > SPX Success.**

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of mails encrypted with Secure PDF Exchange (SPX) received per user while the tabular report contains the following information:

- Recipient: Email ID of the user receiving mails encrypted with SPX.
- Mail Count: Number of SPX encrypted mail received per user.

SPX Failed_Users widget

This Widget report provides an overview of users who have failed to use SPX email encryption along with number of such mails per user.

View the report from **Monitor & Analyze > Reports > Email > Email Protection > SPX Summary > SPX Failed.**

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of mail count per user while the tabular report contains the following information:

- User: Name of the user failed to use SPX email encryption.
- Mail Count: Number of times the SPX email encryption failed, per user.

SPX Failed_Senders widget

This Widget report displays Email IDs of the users who have failed to use SPX email encryption along with number of such mails sent per user.

View the report from **Monitor & Analyze > Reports > Email > Email Protection > SPX Summary > SPX Failed.**

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of failed attempts to use SPX email encryption per sender Email ID while the tabular report contains the following information:

- Sender: Email ID of the mail sender who failed to use SPX email encryption.
- Mail Count: Number of times the SPX email encryption failed, per Email ID.

SPX Failed_Recipients widget

This Widget report displays Email IDs of the users who failed to use SPX email encryption along with number of such mails sent per user.

View the report from **Monitor & Analyze > Reports > Email > Email Protection > SPX Summary > SPX Failed.**

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of failed attempts to use SPX email encryption per Recipient Email ID while the tabular report contains the following information:

- Recipient: Email ID of the mail recipient user who failed to use SPX email encryption.
- Mail Count: Number of times the SPX email encryption failed, per Email ID.

Trend - SPX

This report provides SPX usage time trend in terms of number of SPX events per time period.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Trend - SPX**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays number of SPX usage events per time period while the tabular report displays following information:

- Time: Time in the format of YYYY-MM-DD HH:MM:SS.
- Event: Number of events per time period.

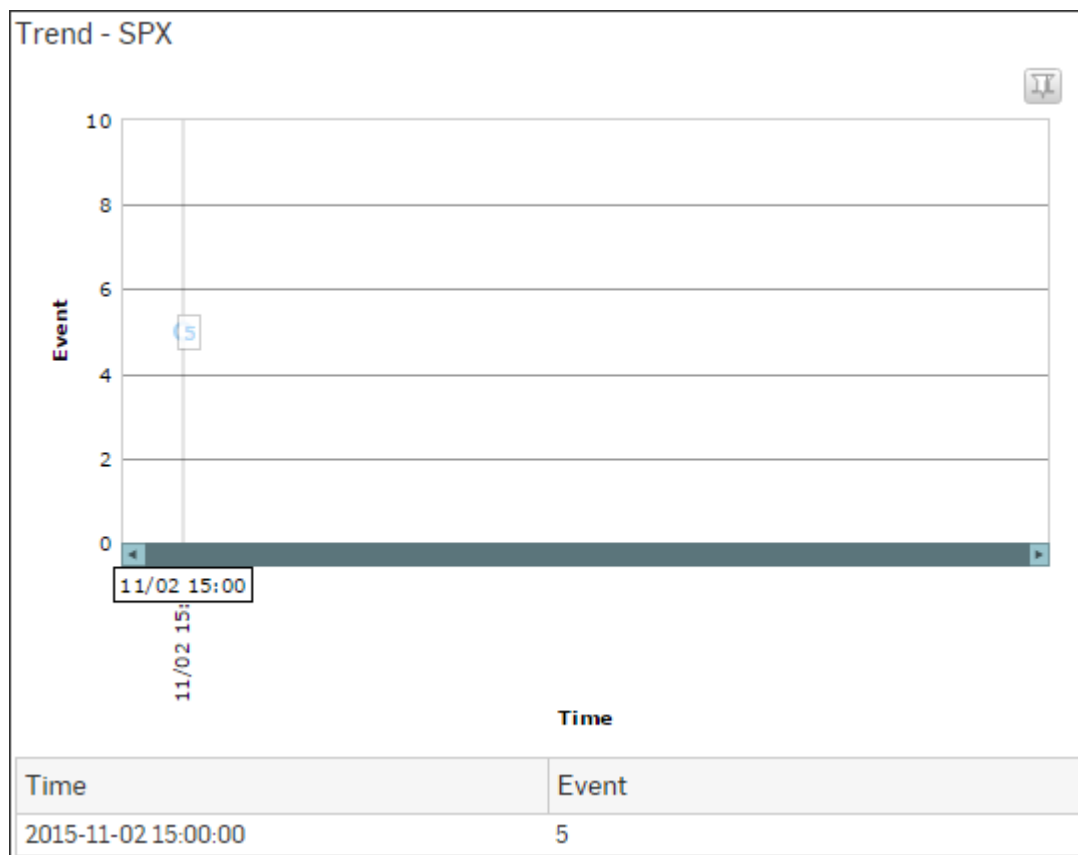


Figure 228: Trend - SPX

Users (SPX)

This Report provides an overview of users using Secure PDF Exchange (SPX) email encryption along with number of such mails per user.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Users (SPX)**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of mail count per user while the tabular report contains the following information:

- Users (SPX): Name of the user using SPX email encryption.
- Mail Count: Number of mails (sent + received) with SPX email encryption, per user.

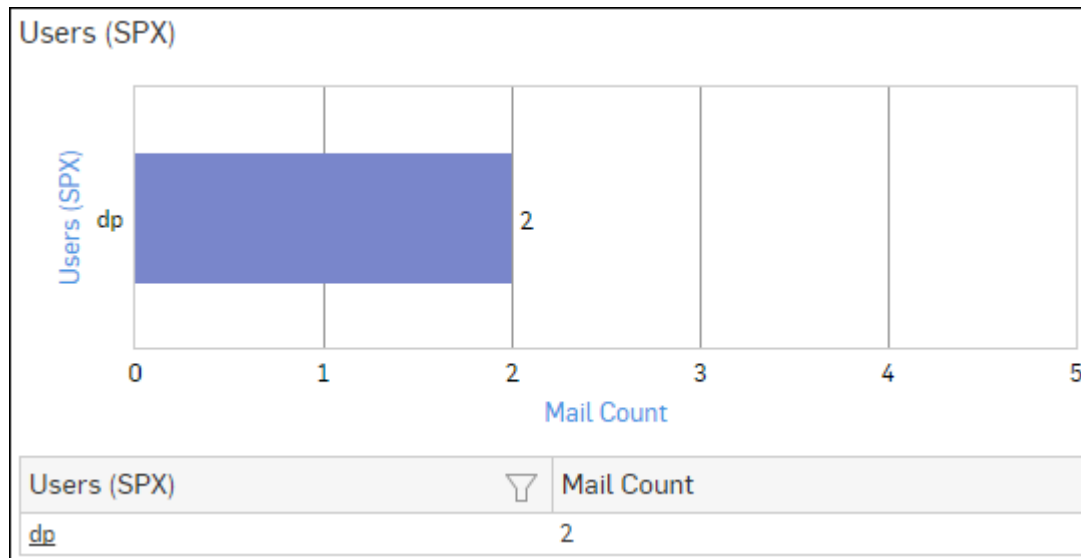


Figure 229: Users (SPX)

Click the Users (SPX) hyperlink in the table or graph to view the [Filtered SPX Reports](#).

Senders (SPX)

This Report provides an overview of users using Secure PDF Exchange (SPX) email encryption for sending Emails along with number of such mails sent per user.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Senders (SPX)**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of Email sent using SPX per user while the tabular report contains the following information:

- Senders (SPX): Email ID of the user using SPX email encryption.
- Mail Count: Number of mails sent using SPX email encryption, per user.

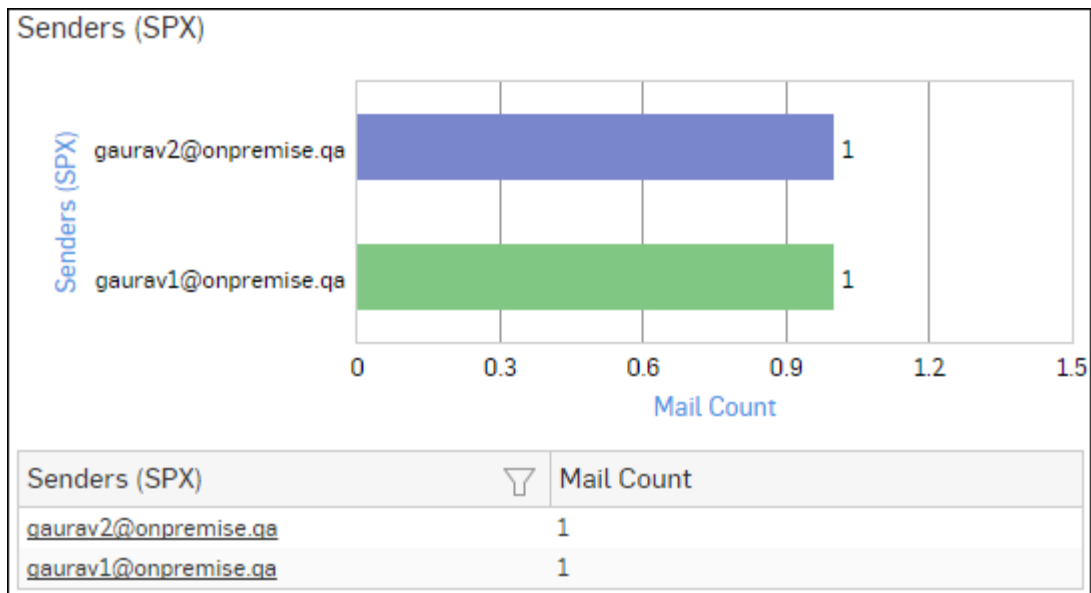


Figure 230: Senders (SPX)

Click the Senders (SPX) hyperlink in the table or graph to view the [Filtered SPX Reports](#).

Recipients (SPX)

This Report provides an overview of users receiving mails encrypted with Secure PDF Exchange (SPX) along with number of such mails received per user.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Recipients (SPX)**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of mails encrypted with Secure PDF Exchange (SPX) received per user while the tabular report contains the following information:

- Recipients (SPX): Email ID of the user receiving mails encrypted with Secure PDF Exchange (SPX).
- Mail Count: Number of SPX encrypted mail received per user.

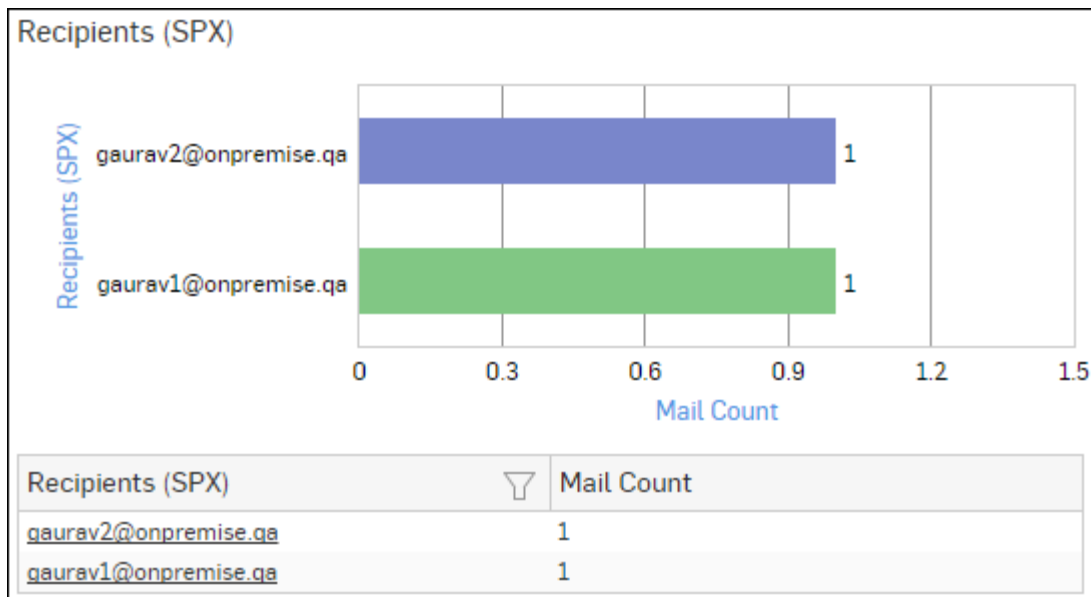


Figure 231: Recipients (SPX)

Click the Recipients (SPX) hyperlink in the table or graph to view the [Filtered SPX Reports](#).

Senders (DLP)

This Report provides an overview of users sending mails protected with Data Protection feature along with number of such mails sent per user.

The Data Protection scans outgoing emails including subject line, message body and attachments for sensitive or confidential information. Based on the outcome, the email can be encrypted using SPX encryption, or the email can be rejected or sent.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Senders (DLP)**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of mails protected with Data Protection sent per user while the tabular report contains the following information:

- Senders (DLP): Email ID of the user sending mails protected with Data Protection.
- Count: Number such mails sent per user.

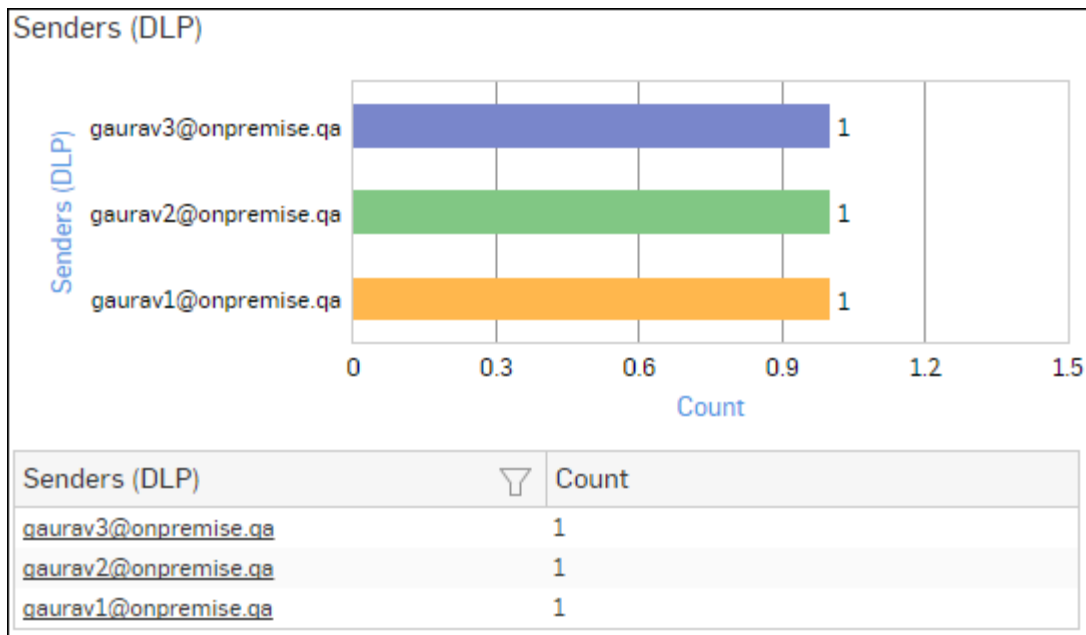


Figure 232: Senders (DLP)

Click the Senders (DLP) hyperlink in the table or graph to view the [Recipients \(DLP\)](#) report.

Recipients (DLP)

This Report provides a list of users receiving mails from the selected mail sender along with number of mails received per Recipients' Email ID.

View the report from **Monitor & Analyze > Reports > Email > Email Protection > Senders (DLP) > Senders (DLP)**.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of mails a recipient received from the selected mail sender, while the tabular report contains the following information:

- Recipients (DLP): Email ID of the user receiving mails (protected with Data Protection) from the selected mail sender.
- Count: Number such mails received per user.

Filtered Spam Reports

The Email Protection Reports can be drilled down to get the following set of Filtered Spam Reports in widget format:

- [Spam Recipients](#)
- [Spam Senders](#)
- [Outbound Spam Recipients](#)
- [Outbound Spam Sender](#)
- [Applications used for Spam](#)
- [Spam Sending Countries](#)
- [Spam Receiving Countries](#)

To view the Filtered Email Usage reports, you need to choose one of the following filter criteria:

- Recipient from [Spam Recipients Report](#)
- Sender from [Spam Senders Report](#)
- Recipient from [Outbound Spam Recipients Report](#)

- Sender from [Outbound Spam Sender Report](#)
- Application from [Applications used for Spam Report](#)
- Country from [Spam Sending Countries Report](#)
- Country from [Spam Receiving Countries Report](#)

Based on the filter criterion, reports will be displayed in the following format:

- Summary - Reports in graphical format
- Details - Reports in tabular format

The Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered. Detailed Reports are displayed in tabular format which can be filtered by clicking hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Spam Recipients widget

This widget report displays a list of Spam Recipients along with number of emails per spam recipient.



Note: This widget will not be displayed for filter criterion Recipient.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays number of hits per spam per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.

Spam Senders widget

This widget report displays a list of Spam Senders along with number of emails per spam sender.



Note: This widget will not be displayed for filter criterion Sender.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays number of hits per spam per sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of spam emails sent.

Outbound Spam Recipients widget

This widget report displays a list of Outbound Spam Recipients along with number of emails per spam recipient.



Note: This widget will not be displayed for filter criterion Recipient.

The Report is displayed as a pie chart as well as in a tabular format.

The Pie chart displays number of hits per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.

Applications used for Spam widget

This widget report displays a list of Applications used to generate Spam along with the number of emails.



Note: This widget will not be displayed for filter criterion Application.

The report is displayed as a pie chart as well as in a tabular format.

The bar graph displays number of hits per application while the tabular report contains the following information:

- Application/Proto:Port: Displays the name of the application as defined in the Device. If application is not defined in the Device then this field will display application identifier as combination of the protocol and port number.
- Mail Count: Number of spam emails per application.

Spam Sending Countries widget

This widget displays a list of countries from where the maximum volume of spam traffic is originated along with number of emails per country.



Note: This widget will not be displayed for filter criterion Source Country.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of hits per spam sending country while the tabular report contains the following information:

- Source Country: Name of the spam sending country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Mail Count: Number of spam emails sent per country.

Outbound Spam Sender widget

This widget report displays a list of Outbound Spam Senders along with number of emails per spam sender.



Note: This widget will not be displayed for filter criterion Sender.

The Report is displayed as a pie chart as well as in a tabular format.

The Pie chart displays number of hits per sender while the tabular report contains the following information:

- Sender: Email ID of the recipient.
- Mail Count: Number of spam emails sent.

Spam Receiving Countries widget

This widget displays a list of those countries which are destined to most of the spam traffic along with number of emails per country.



Note: This widget will not be displayed for filter criterion Destination Country.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of hits per spam receiving country while the tabular report contains the following information:

- Destination Country: Name of the spam receiving country. Note that country association is not applicable to local hosts and Reserved is displayed in such cases.
- Mail Count: Number of spam emails received per country.

Filtered Virus Reports

The Email Protection Reports can be drilled down to get the following set of Filtered Virus Reports in widget format:

- [Mail Virus by Application Type](#)
- [Mail Virus](#)
- [Users - Mail Virus](#)
- [Mail Virus Senders](#)
- [Mail Virus Recipients](#)
- [Hosts - Mail Virus Senders](#)
- [Hosts - Mail Virus Recipients](#)

To view the Filtered Email Usage reports, you need to choose one of the following filter criteria:

- Application from [Mail Virus by Application Type Report](#)
- Virus from [Mail Virus Report](#)
- User from [Users - Mail Virus Report](#)
- Sender from [Mail Virus Senders Report](#)
- Recipient from [Mail Virus Recipients Report](#)
- Host from [Hosts - Mail Virus Senders Report](#)
- Host from [Hosts - Mail Virus Recipients Report](#)

Based on the filter criterion, reports will be displayed in the following format:

- Summary - Reports in graphical format
- Details - Reports in tabular format

The Filtered Summary Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered. Detailed Reports are displayed in tabular format which can be filtered by clicking hyperlinks in the table.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Mail Virus by Application Type widget

This Widget report provides an overview of mail viruses by their application type.



Note: This widget will not be displayed for filter criterion Application.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of mail viruses per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the application, as defined in the Device.
- Count: Number of mail viruses per application.

Mail Virus widget

This Widget report displays Viruses detected in your network along with number of hits per virus.



Note: This widget will not be displayed for filter criterion Virus.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of counts per mail virus while the tabular report contains the following information:

- Virus: Name of the virus.
- Count: Number of counts per mail virus.

Users - Mail Virus widget

This Widget report provides an overview of mail virus users along with number of hits per user.



Note: This widget will not be displayed for filter criterion User.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of counts per mail virus user while the tabular report contains the following information:

- User: Name of the mail virus user.
- Count: Number of counts per mail virus user.

Mail Virus Senders widget

This Widget report displays mail virus senders along with number of hits per sender.



Note: This widget will not be displayed for filter criterion Sender.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of counts per mail virus sender while the tabular report contains the following information:

- Sender: Name of the mail virus sender.
- Count: Number of counts per mail virus sender.

Mail Virus Recipients widget

This Widget report displays mail virus recipients along with number of hits per recipient.



Note: This widget will not be displayed for filter criterion Recipient.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of counts per mail virus recipient while the tabular report contains the following information:

- Recipient: Name of the mail virus recipient.
- Count: Number of counts per mail virus recipient.

Hosts - Mail Virus Senders widget

This Widget report displays mail virus sender hosts along with number of hits per host.



Note: This widget will not be displayed for filter criterion Sender Host.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of counts per mail virus sender host while the tabular report contains the following information:

- Sender Host: IP Address of the mail virus sender host.
- Count: Number of counts per mail virus sender host.

Hosts - Mail Virus Recipients widget

This Widget report displays mail virus recipient hosts along with number of hits per host.



Note: This widget will not be displayed for filter criterion Receiver Host.

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of counts per mail virus recipient host while the tabular report contains the following information:

- Receiver Host: IP Address of the mail virus recipient host.
- Count: Number of counts per mail virus recipient host.

Filtered SPX Reports

The Users (SPX), Senders (SPX) and Recipients (SPX) Reports can be drilled down to get the following set of Filtered SPX Reports in widget format:

- [Users \(SPX\)](#)
- [Senders \(SPX\)](#)
- [Recipients \(SPX\)](#)

To view the Filtered SPX reports, you need to choose one of the following filter criteria:

- User from [Users \(SPX\) Report](#)
- Sender from [Senders \(SPX\) Report](#)
- Recipient from [Recipients \(SPX\) Report](#)

The Filtered SPX Reports consist of multiple report widgets except the filter criterion widget. Each widget displays the report in a graph as well as in a tabular format which can again be filtered.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

Users (SPX) widget

This Report provides an overview of users using SPX email encryption along with number of such mails per user.



Note: This widget is not displayed for the filter criterion Users (SPX).

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of mail count per user while the tabular report contains the following information:

- Users (SPX): Name of the user using SPX email encryption.
- Mail Count: Number of mails (sent + received) with SPX email encryption, per user.

Senders (SPX) widget

This Report provides an overview of Email IDs using SPX email encryption for sending Emails along with number of such mails sent per user.



Note: This widget is not displayed for the filter criterion Senders (SPX).

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of Email sent using SPX per Email ID while the tabular report contains the following information:

- Senders (SPX): Email ID of the user using SPX email encryption.
- Mail Count: Number of mails sent using SPX email encryption, per user.

Recipients (SPX) widget

This Report provides an overview of Email IDs receiving mails encrypted with SPX along with number of such mails received per user.



Note: This widget is not displayed for the filter criterion Recipients (SPX).

The Report is displayed as a pie chart as well as in a tabular format.

The bar graph displays the number of mails encrypted with Secure PDF Exchange (SPX) received per Email ID while the tabular report contains the following information:

- Recipients (SPX): Email ID of the user receiving mails encrypted with Secure PDF Exchange (SPX).
- Mail Count: Number of SPX encrypted mail received per user.

Compliance

Regulatory compliance has become a priority for organizations, requiring overwhelming effort, time and cost in the form of retrieval and storage of logs and reports from multiple devices. Correlating the vast amount of logs and reports to complete the compliance picture is a complicated and time-consuming task.



Note: The Compliance sub sections can be accessed by selecting drop-down 1 given at the upper left corner of the page.

The Device Reports enable organizations to meet the requirements of following compliance:

- [HIPAA](#)
- [GLBA](#)
- [SOX](#)
- [FISMA](#)
- [PCI](#)
- [NERC CIP v3](#)
- [CIPA](#)

- [Events](#)

HIPAA

HIPAA report is the grouping of various network security reports, which ensures compliance with Health Insurance Portability and Accountability Act (HIPAA).

The HIPAA security standards are mandatory to follow when an organization stores and transmits health information of the patients in electronic form.

View HIPAA reports from **Monitor & Analyze > Reports > Compliance > HIPAA**.

It enables to view the following reports:

- [Spam Recipients](#)
- [Spam Senders](#)
- [Web Virus](#)
- [Virus Summary](#)
- [Mail Virus](#)
- [Mail Virus by Application Type](#)
- [Web Server Virus](#)
- [FTP Virus](#)
- [Intrusion Attacks](#)
- [Intrusion Source](#)
- [Web Server Users](#)
- [Blocked Web Server Requests](#)
- [Admin Events](#)
- [Authentication Events](#)
- [Hosts - ATP](#)
- [Detailed View - Client Health](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)

Spam Recipients

This Report displays a list of Spam Recipients along with number of emails and percent distribution among the spam recipients.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Recipients**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Recipients** as well.

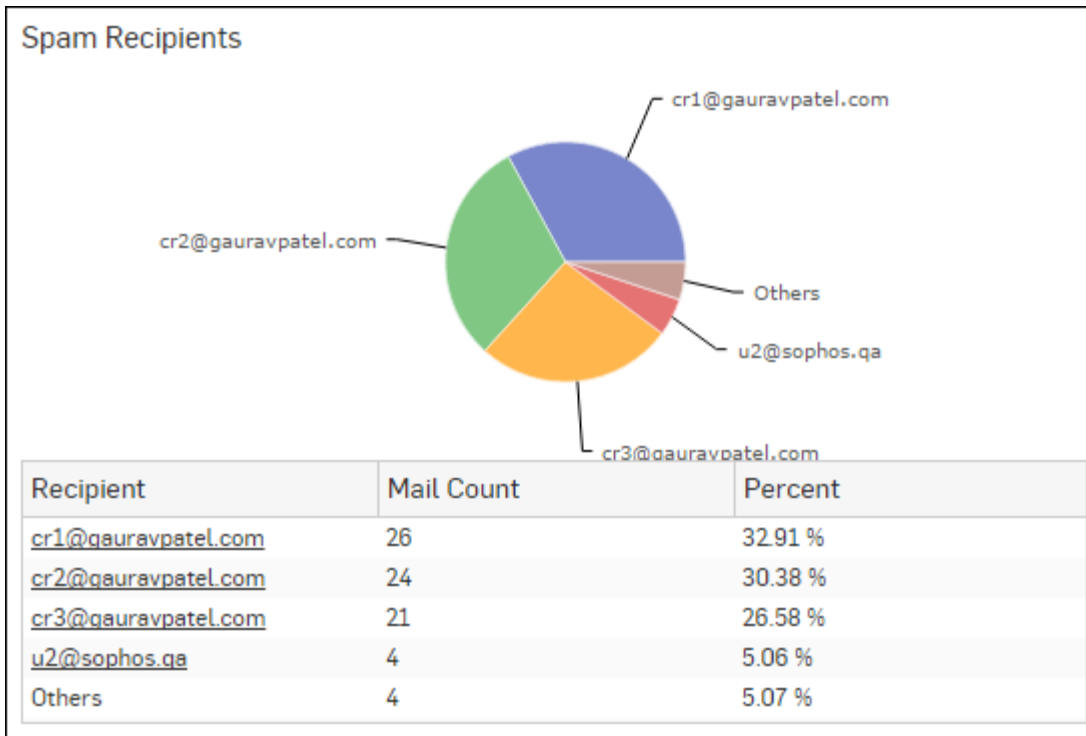
The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.
- Percent: Relative percent distribution among the spam recipients.

Figure 233: Spam Recipients



Click the Recipient hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Spam Senders

This Report displays a list of Spam Senders along with number of emails and percent distribution among the spam senders.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Senders**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Senders** as well.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of spam emails sent.
- Percent: Relative percent distribution among the spam sender.

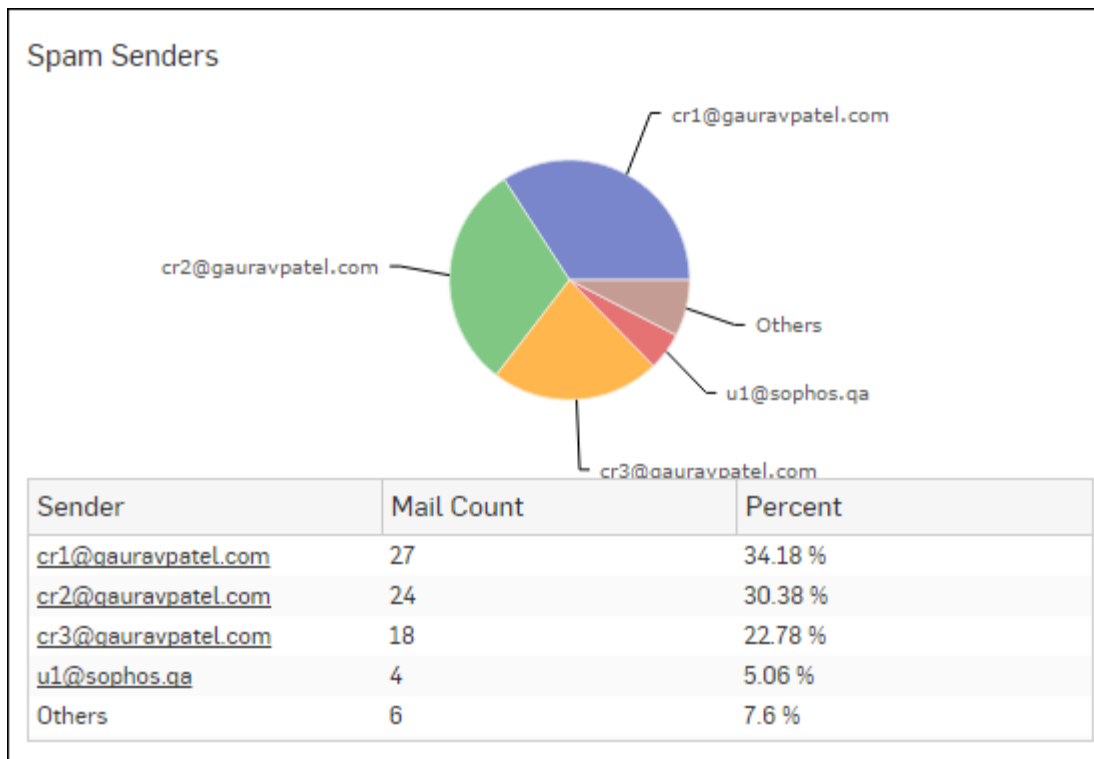


Figure 234: Spam Senders

Click the Sender hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Web Virus

This Report lists viruses blocked by the Device as well as number of occurrence per blocked virus.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked web viruses along with number of counts per virus while the tabular report contains the following information:

- Virus: Name of the blocked web virus.
- Count: Number of times a virus was blocked.

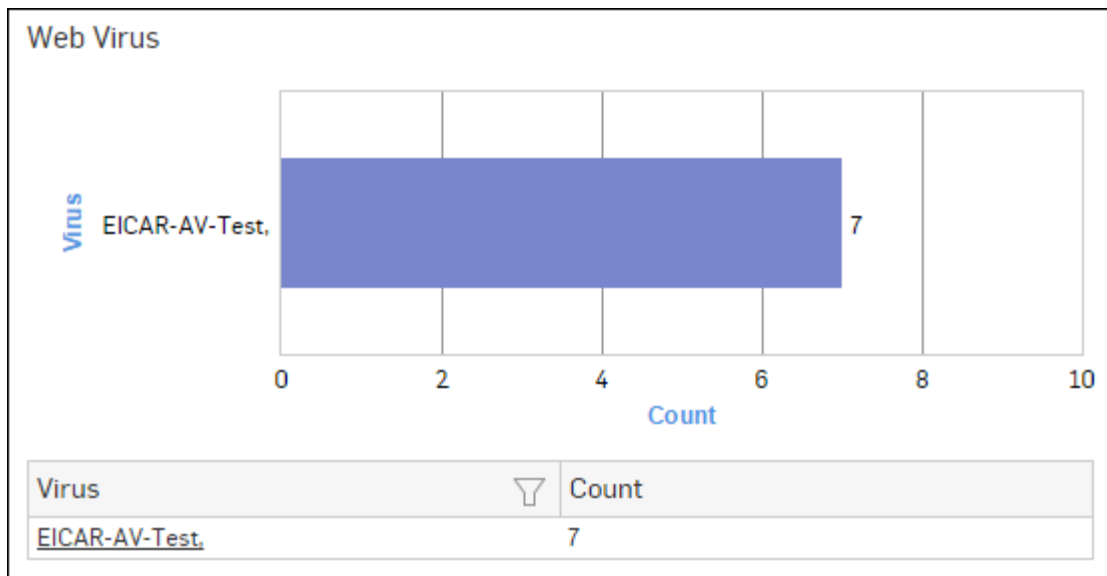


Figure 235: Web Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Virus Summary

This Report provides an overview of Virus traffic in your network, in terms of protocols through which viruses were introduced in the network as well as number of counts per protocol.

View the report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Virus Summary**.

The Report is displayed using a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays number of counts per protocol through which viruses were introduced in the network, while the tabular report contains following information:

- Application/Proto:Port: Name of the protocol through which viruses were introduced in the network.
- Count: Number of counts per protocol.

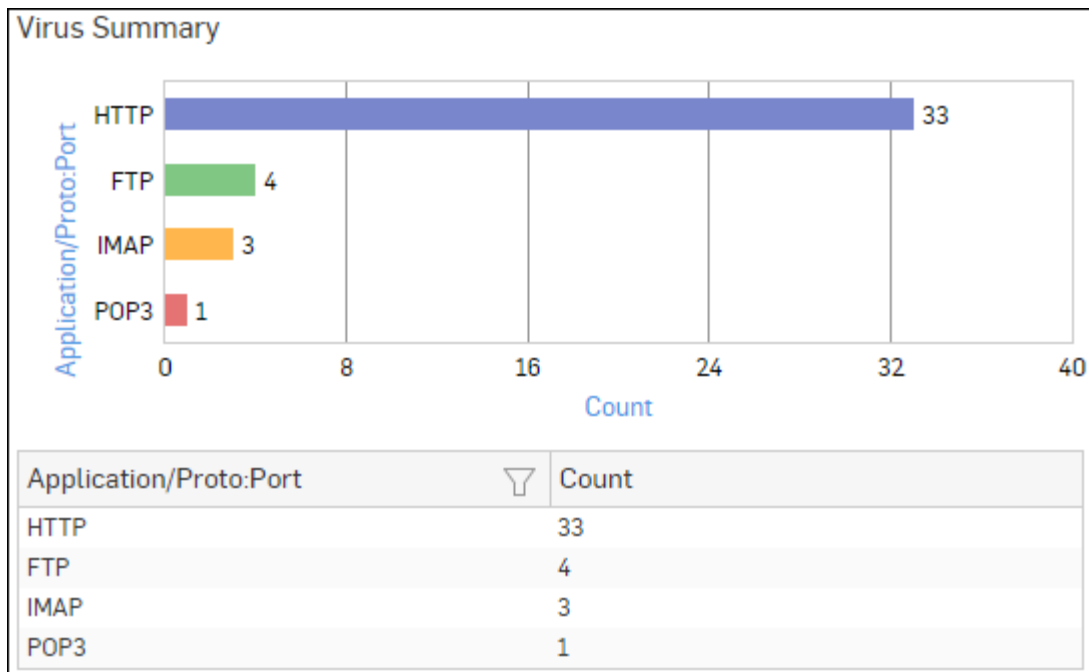


Figure 236: Virus Summary

Click Application hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Mail Virus

This Report displays Viruses detected in your network along with number of hits per Virus.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus while the tabular report contains the following information:

- Virus: Name of the virus.
- Count: Number of counts per mail virus.

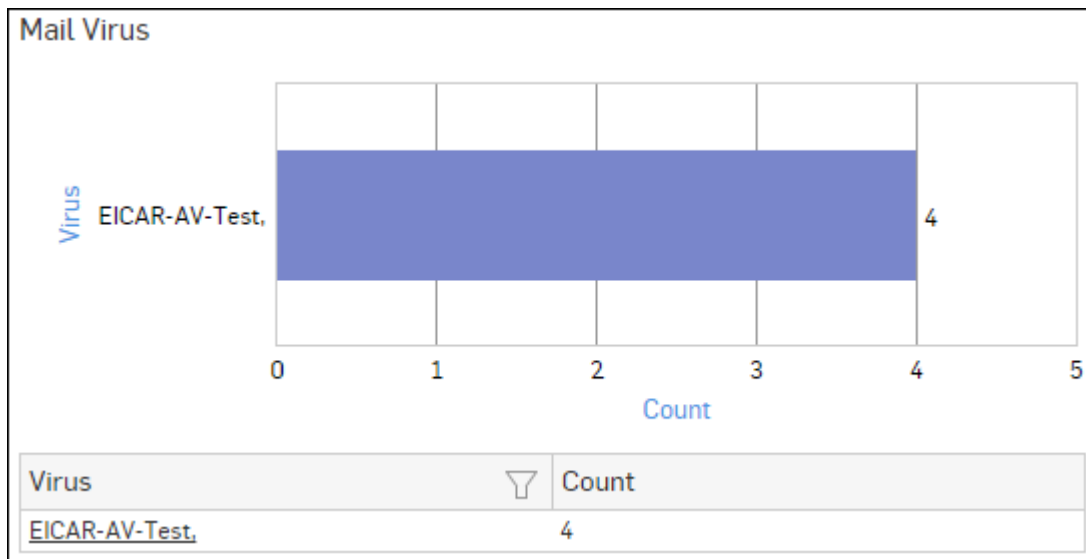


Figure 237: Mail Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Mail Virus by Application Type

This Report provides an overview of mail viruses by their application type.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus by Application Type**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of email viruses per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the application, as defined in the Device.If the application is not defined in the Device then this field displays the application identifier as combination of protocol and port number.
- Count: Number of email viruses per application.

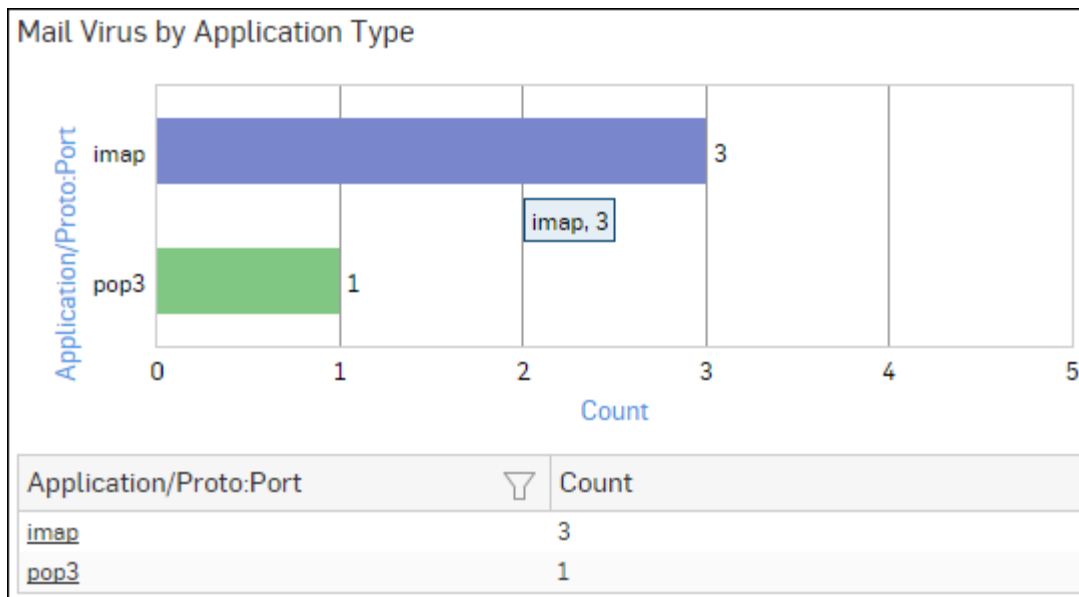


Figure 238: Mail Virus by Application Type

Click the Application hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Web Server Virus

This report displays a list of blocked viruses along with number of hits per virus.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Web Server Virus**.

The bar graph displays the list of viruses and number of hits while the tabular report contains the following information:

- Virus: Name of the Virus blocked by the Device.
- Hits: Number of hits per blocked virus.

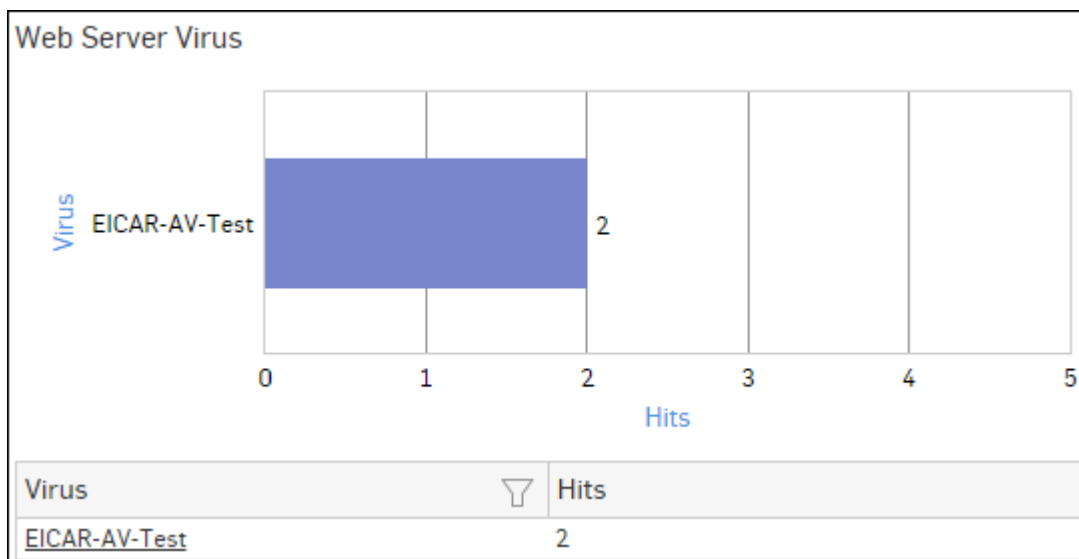


Figure 239: Web Server Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

FTP Virus

This Report displays a list of the FTP viruses and number of counts per virus.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > FTP Virus**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per virus while the tabular report contains the following information:

- Virus: Name of the FTP virus.
- Count: Number of counts for the virus.

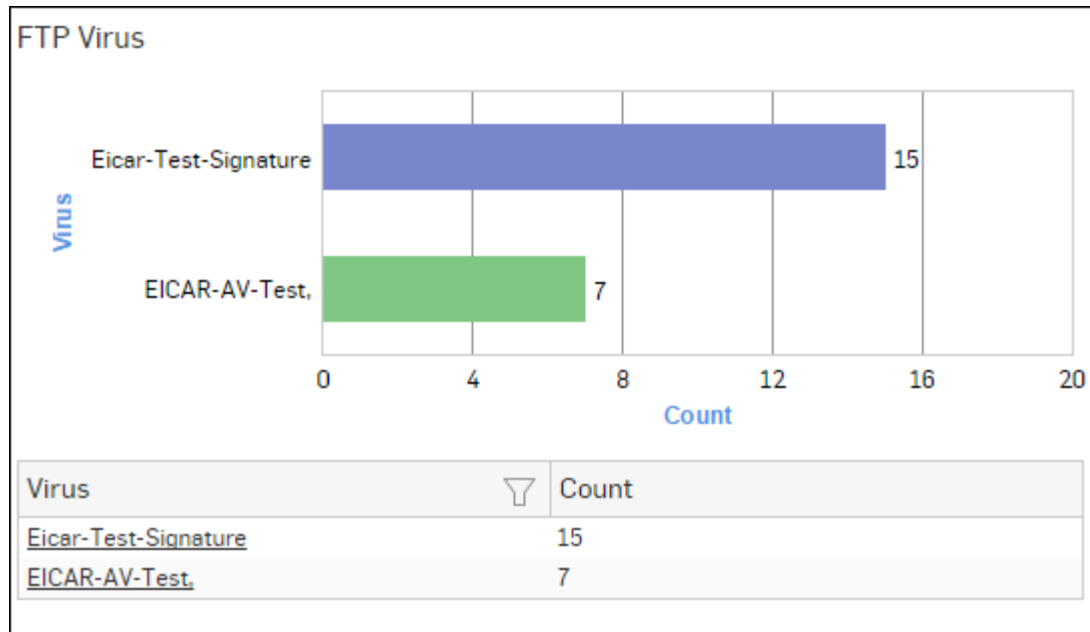


Figure 240: FTP Virus

Click the Virus hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Intrusion Attacks

The Report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Attacks**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Attacks** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each attack, while the tabular report contains the following information:

- Attack: Name of the attack launched.
- Hits: Number of hits for each attack.

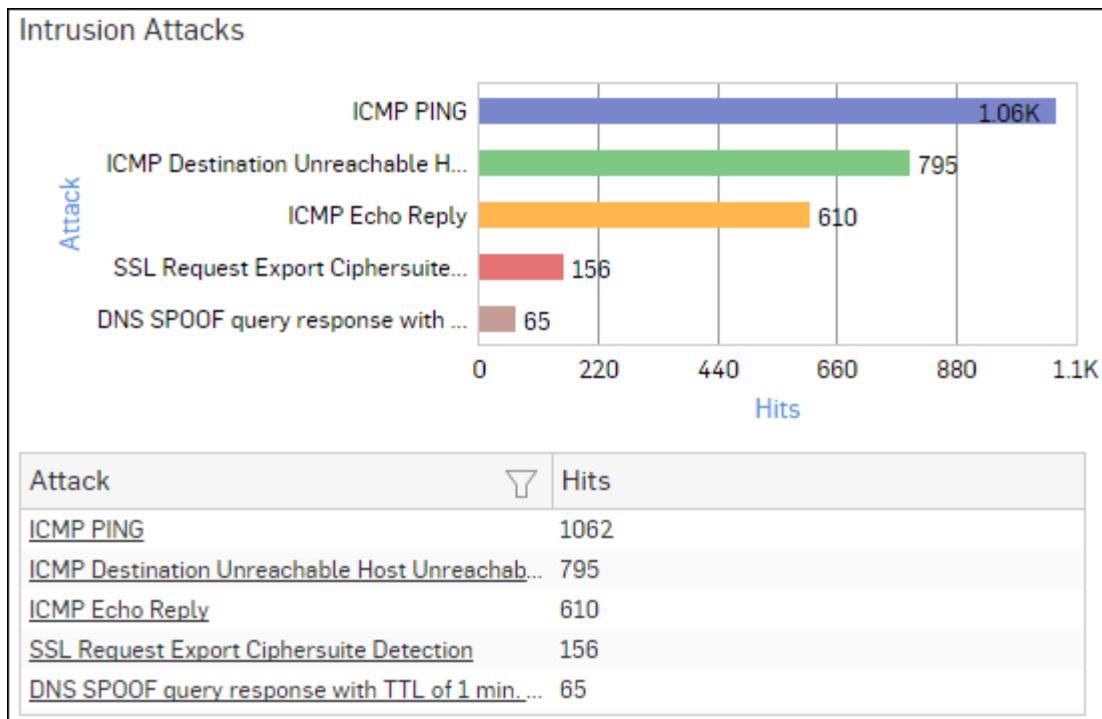


Figure 241: Intrusion Attacks

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Source

The Report enables to view the details of the attacker(s) who have hit the system and gives the detailed disintegration of attacks, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Source**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Source** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each attacker, while the tabular report contains the following information:

- Attacker: IP Address of the attacker.
- Hits: Number of hits for each attacker.

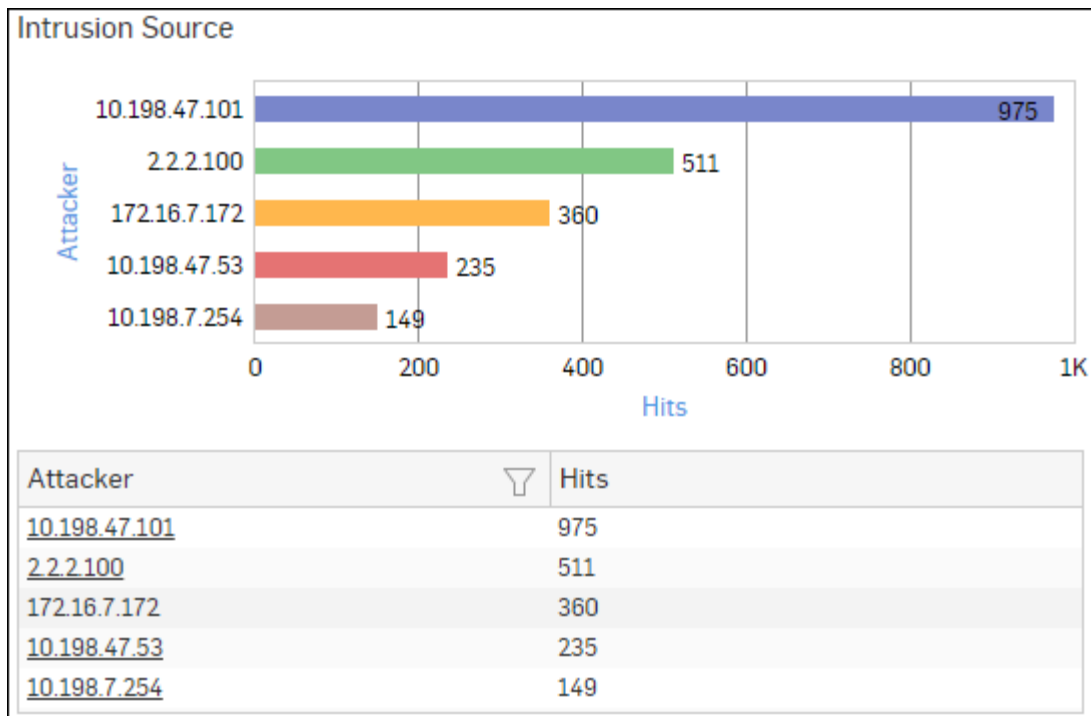


Figure 242: Intrusion Source

Click Attacker hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Web Server Users

This Report displays web server usage in terms of bandwidth utilization by users.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of domains along with bytes while the tabular report contains the following information:

- User: Username of the user, as defined in the Device.
- Bytes: Bandwidth used per user.
- Hits: Number of hits per user.

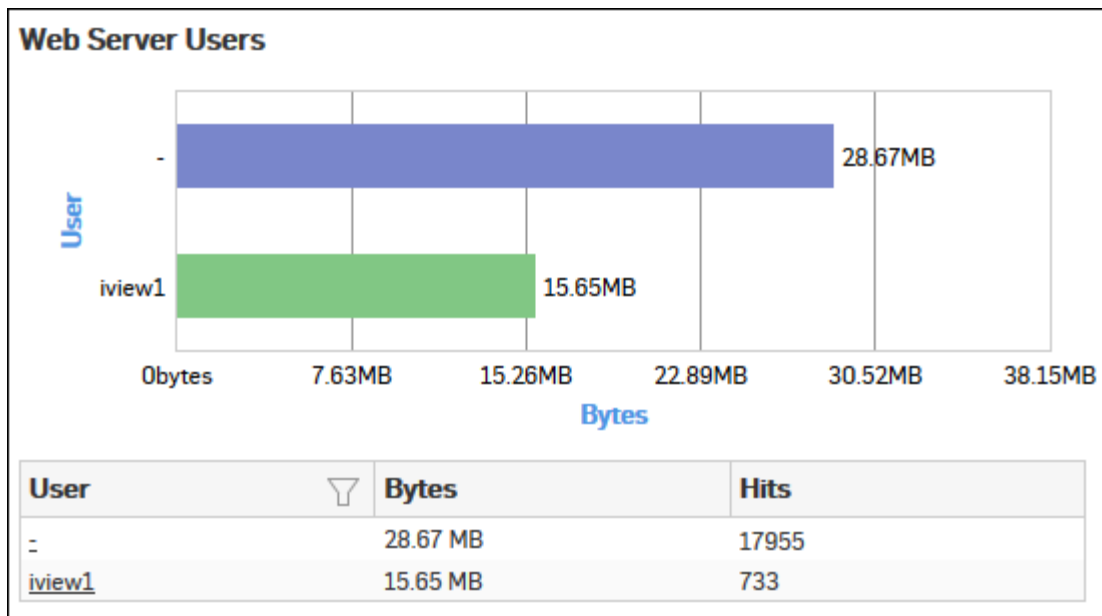


Figure 243: Web Server Users

Click the User hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Blocked Web Server Requests

This Report displays a list of reasons of attacks blocked by the Device, along with the number of hits per attack.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Blocked Web Server Requests**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Server Requests** as well.

The bar graph displays the list of blocked reasons along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

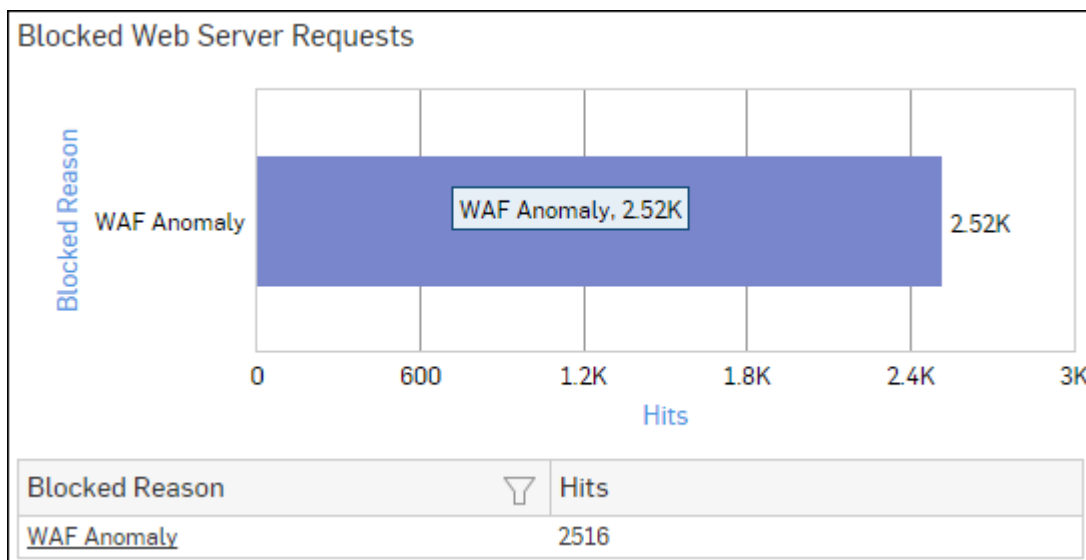


Figure 244: Blocked Web Server Requests

Click the Blocked Reason hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Admin Events

This Report displays the Admin Event details including time, event type, severity, message, username, source and status.

View report from **Monitor & Analyze > Reports > Compliance > Events > Admin Events**.

The tabular report contains the following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :
 - GUI
 - CLI
 - Console
 - SFM
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful






Admin Events						
Time	Event 	Severity	Mess... 	User 	Source 	Status 
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful
2015-12-1...	GUI	Information	User dhire...	dhiren	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	dhiren	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful

Figure 245: Admin Events

Authentication Events

This Report displays the Authentication Events detail including time, event type, severity, message, username, source and status.

View the report from **Monitor & Analyze > Reports > Compliance > Events > Authentication Events**.

Tabular report contains following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :

- Firewall Authentication
- My Account Authentication
- VPN Authentication
- SSL VPN Authentication
- Dial-in Authentication
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User Name: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful

Authentication Events						
Time	Event ▾	Severity	Mess... ▾	User ▾	Source ▾	Status ▾
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed

Figure 246: Authentication Events

Hosts - ATP

This report displays a comprehensive summary of host wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Hosts-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Hosts-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of events per host while the tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Threat Count: Number of threats per source host.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

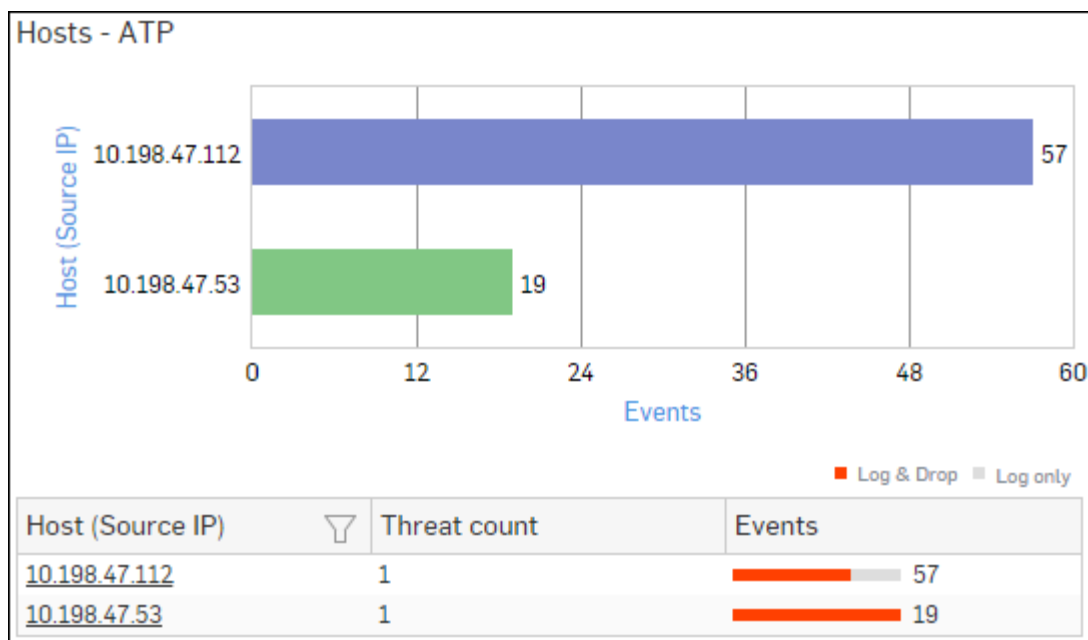


Figure 247: Hosts - ATP

Click Host hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Detailed View - Client Health

This report shows in-depth information regarding health status of endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Detailed View - Client Health**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Detailed View - Client Health** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Host Name: Name of the client.
- Health - Last Seen: Displays the latest health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.







Detailed View - Client Health				
Host (Source IP) 	Host Name 	Health - Last Seen		Last Health
10.20.41.8	TWIN8164BIT		Red	-
10.20.41.7	TWIN864		Yellow	-
10.198.38.8	TWIN764		Green	-
10.20.41.12	TWIN832		Green	-

Figure 248: Detailed View - Client Health

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Detailed View - ATP

This report provides a detailed summary of advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Detailed View - ATP**.

The report is displayed in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page..

The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- User: Username of the infected user.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Events: Total number of events. The number is summation of Log only and Log & Drop events.
- Action: Action performed by the Device when a threat is detected. Possible options:
 - Log & Drop: The data packet is logged and dropped.
 - Log only: The data packet is logged.

Detailed View - ATP										
Host (Source IP)		User		Threat		Threat URL/IP		Origin	Events	Action
10.198.47.112		dp		C2/Generic-A		46.161.30.47		Firewall	54	Log & Drop
10.198.47.112		dp		C2/Generic-A		213.21.21.170		Firewall	45	Log & Drop
10.198.47.112		atp1		C2/Generic-A		46.161.30.47		Firewall	27	Log & Drop
10.198.47.112		atp1		C2/Generic-A		213.21.21.170		Firewall	27	Log & Drop
10.198.47.112		atp1		C2/Generic-A		77.91.166.16		Firewall	18	Log & Drop

Figure 249: Detailed View - ATP

Security Heartbeat - ATP

This report provides an insight into advanced threats related to endpoints in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Security Heartbeat - ATP**.

The report is displayed in a tabular format. The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Login User: Username of the infected user.
- Process User: Username of the user owning the process.
- Executable: Name of the infected executable file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Event Last Seen: Time when the infected executed file was last found in the host.
- Events: Total number of events. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP							
Host (Source IP)	Login User	Process User	Executable	Threat	Threat URL/IP	Event Last Seen	Events
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1

Figure 250: Security Heartbeat - ATP

GLBA

GLBA report is the grouping of various network security reports which ensures compliance with Gramm-Leach Bliley Act (GLBA).

The GLBA security standards are mandatory to follow when an organization stores and transmits financial information of the users in electronic form.

View GLBA reports from **Monitor & Analyze > Reports > Compliance > GLBA**.

It enables to view the following reports:

- [Spam Recipients](#)
- [Spam Senders](#)
- [Web Virus](#)
- [Virus Summary](#)
- [Mail Virus](#)
- [Mail Virus by Application Type](#)
- [Web Server Virus](#)
- [FTP Virus](#)
- [Intrusion Attacks](#)
- [Intrusion Source](#)
- [Web Server Users](#)
- [Blocked Web Server Requests](#)
- [Admin Events](#)
- [Authentication Events](#)
- [Hosts - ATP](#)
- [Detailed View - Client Health](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)

Spam Recipients

This Report displays a list of Spam Recipients along with number of emails and percent distribution among the spam recipients.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Recipients**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Recipients** as well.

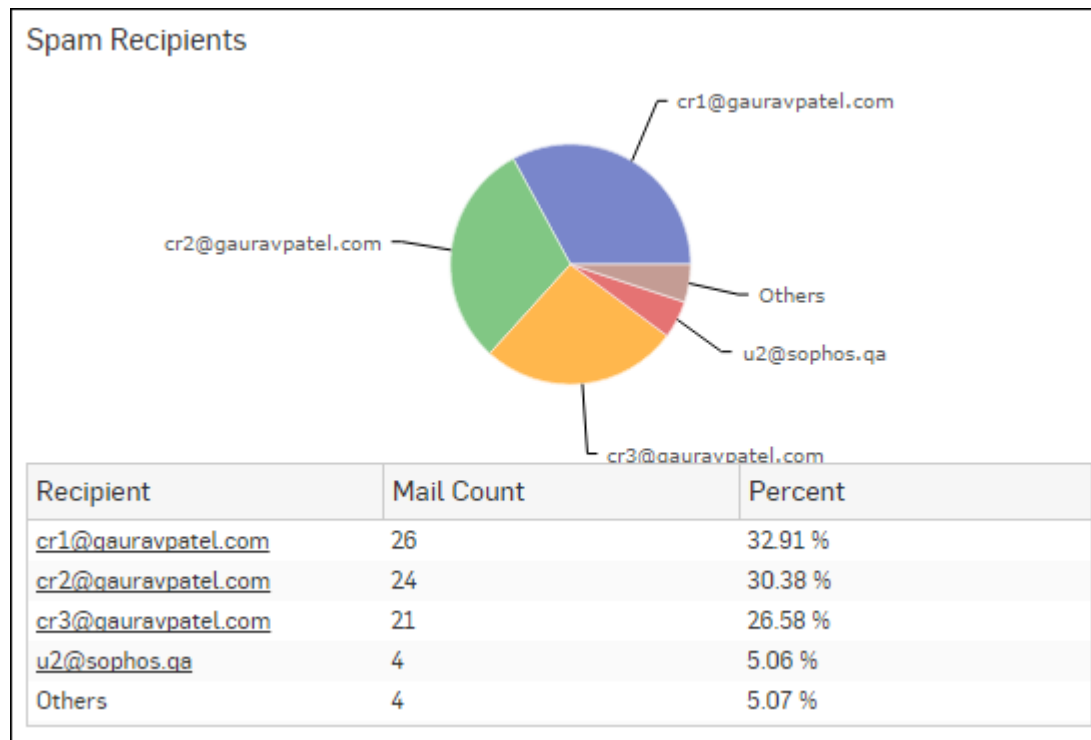
The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per recipient while the tabular report contains the following information:

- Recipient: Email ID of the recipient.
- Mail Count: Number of spam emails received.
- Percent: Relative percent distribution among the spam recipients.

Figure 251: Spam Recipients



Click the Recipient hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Spam Senders

This Report displays a list of Spam Senders along with number of emails and percent distribution among the spam senders.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Spam Senders**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Spam Senders** as well.

The Report is displayed as a pie chart as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Pie chart displays a percentage-wise distribution of spam per sender while the tabular report contains the following information:

- Sender: Email ID of the sender.
- Mail Count: Number of spam emails sent.
- Percent: Relative percent distribution among the spam sender.

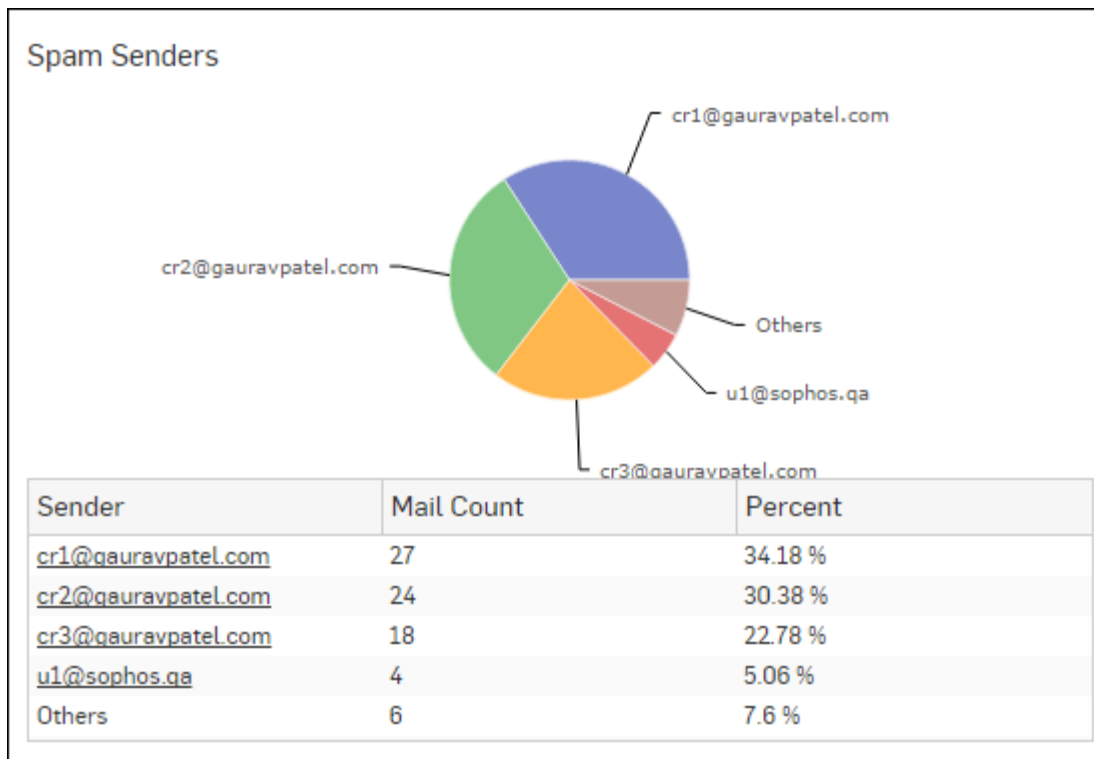


Figure 252: Spam Senders

Click the Sender hyperlink in the table or pie chart to view the [Filtered Spam Reports](#).

Web Virus

This Report lists viruses blocked by the Device as well as number of occurrence per blocked virus.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked web viruses along with number of counts per virus while the tabular report contains the following information:

- Virus: Name of the blocked web virus.
- Count: Number of times a virus was blocked.

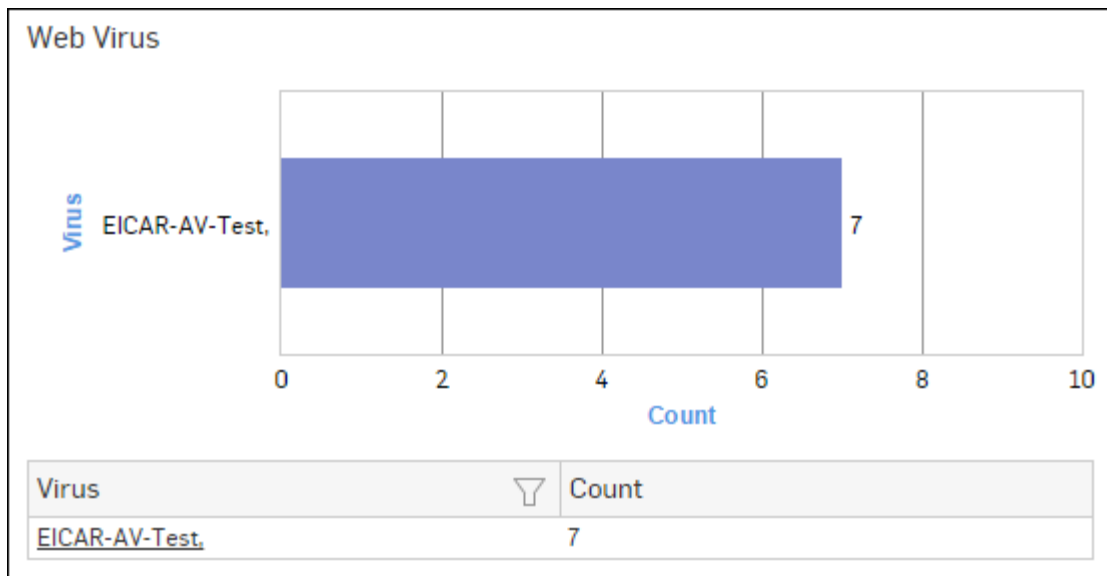


Figure 253: Web Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Virus Summary

This Report provides an overview of Virus traffic in your network, in terms of protocols through which viruses were introduced in the network as well as number of counts per protocol.

View the report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Virus Summary**.

The Report is displayed using a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays number of counts per protocol through which viruses were introduced in the network, while the tabular report contains following information:

- Application/Proto:Port: Name of the protocol through which viruses were introduced in the network.
- Count: Number of counts per protocol.

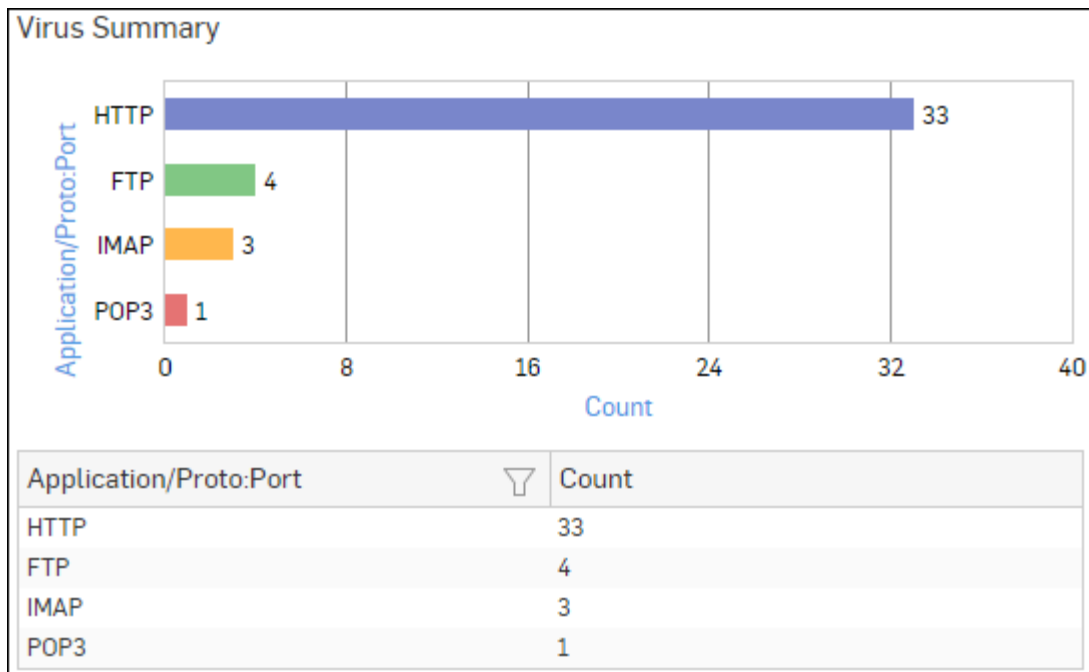


Figure 254: Virus Summary

Click Application hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Mail Virus

This Report displays Viruses detected in your network along with number of hits per Virus.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus while the tabular report contains the following information:

- Virus: Name of the virus.
- Count: Number of counts per mail virus.

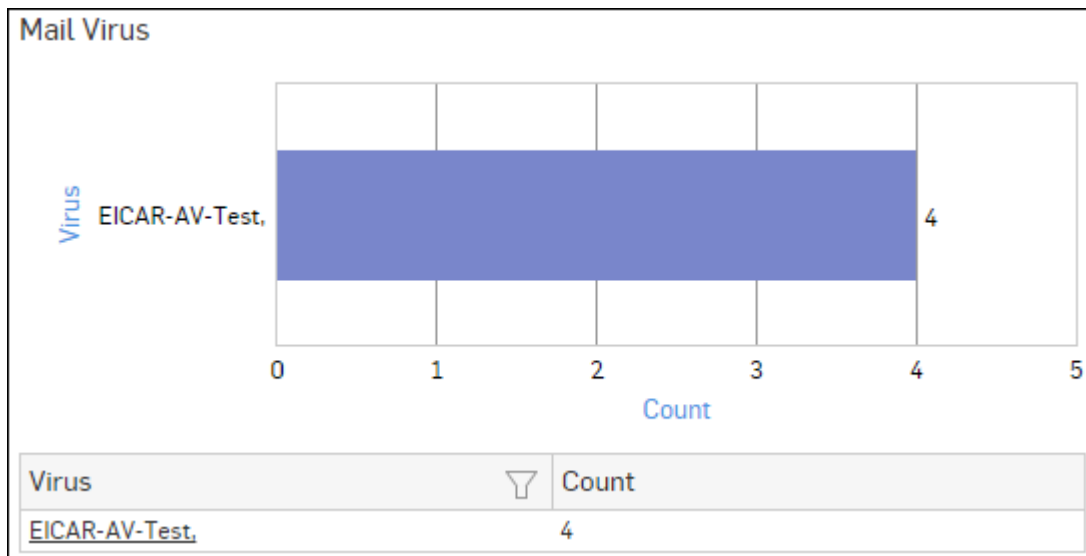


Figure 255: Mail Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Mail Virus by Application Type

This Report provides an overview of mail viruses by their application type.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus by Application Type**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of email viruses per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the application, as defined in the Device.If the application is not defined in the Device then this field displays the application identifier as combination of protocol and port number.
- Count: Number of email viruses per application.

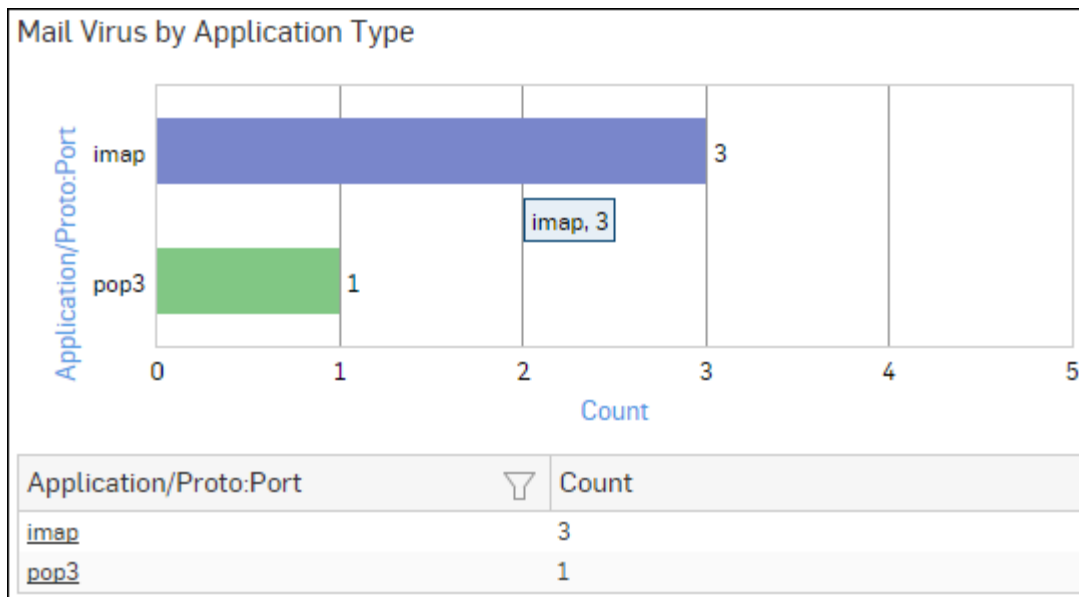


Figure 256: Mail Virus by Application Type

Click the Application hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Web Server Virus

This report displays a list of blocked viruses along with number of hits per virus.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Web Server Virus**.

The bar graph displays the list of viruses and number of hits while the tabular report contains the following information:

- Virus: Name of the Virus blocked by the Device.
- Hits: Number of hits per blocked virus.

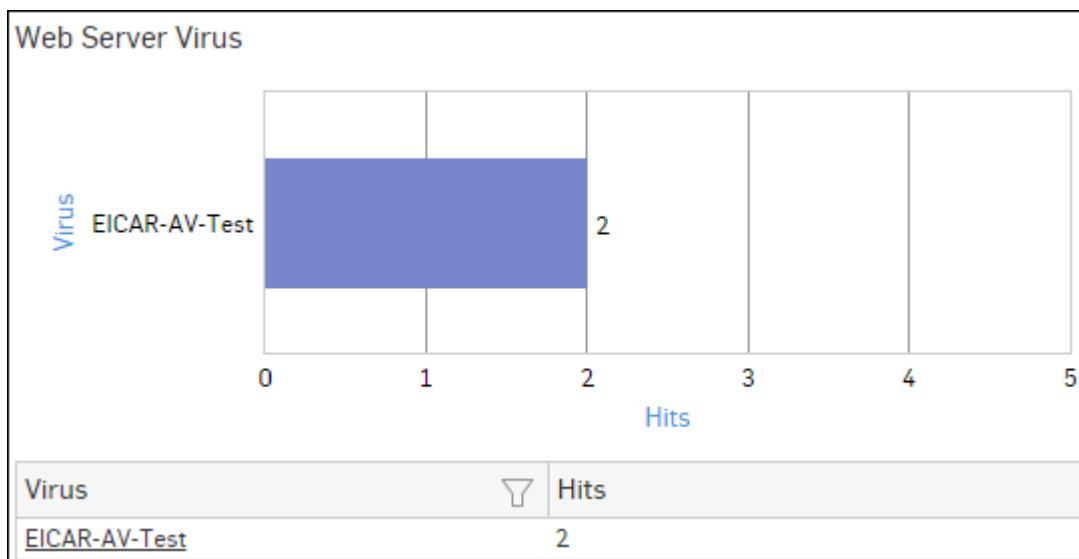


Figure 257: Web Server Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

FTP Virus

This Report displays a list of the FTP viruses and number of counts per virus.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > FTP Virus**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per virus while the tabular report contains the following information:

- Virus: Name of the FTP virus.
- Count: Number of counts for the virus.

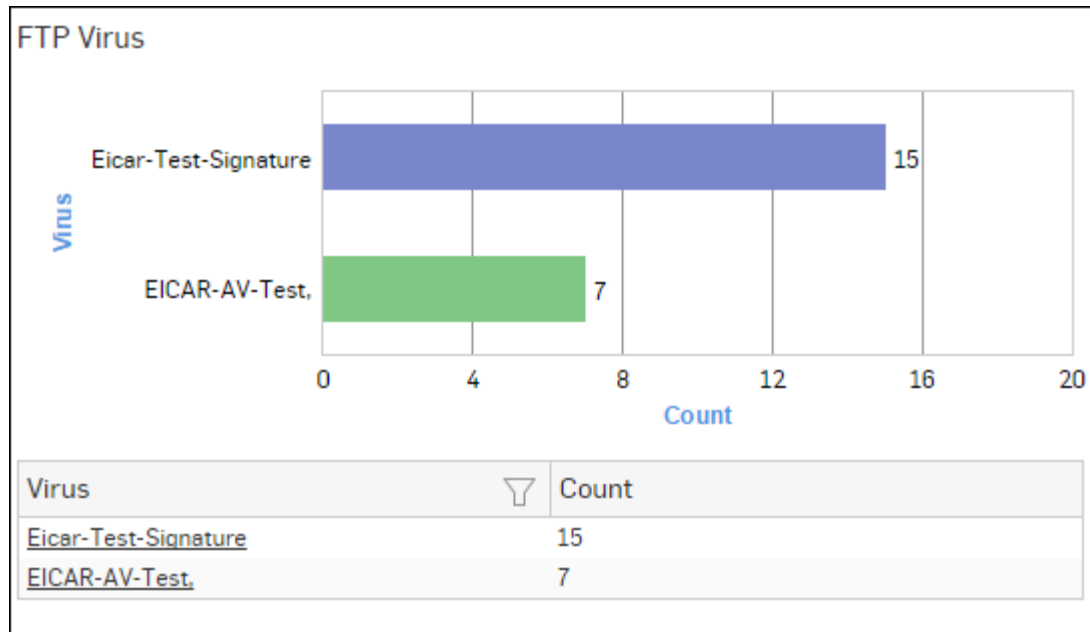


Figure 258: FTP Virus

Click the Virus hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Intrusion Attacks

The Report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Attacks**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Attacks** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each attack, while the tabular report contains the following information:

- Attack: Name of the attack launched.
- Hits: Number of hits for each attack.

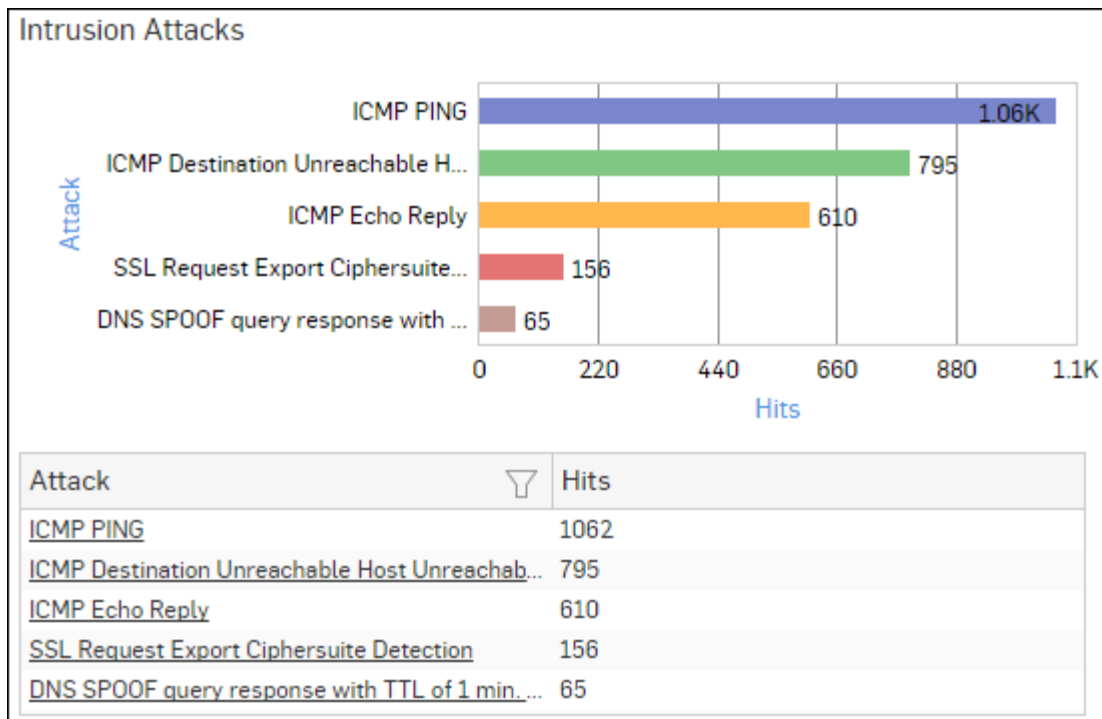


Figure 259: Intrusion Attacks

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Source

The Report enables to view the details of the attacker(s) who have hit the system and gives the detailed disintegration of attacks, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Source**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Source** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each attacker, while the tabular report contains the following information:

- Attacker: IP Address of the attacker.
- Hits: Number of hits for each attacker.

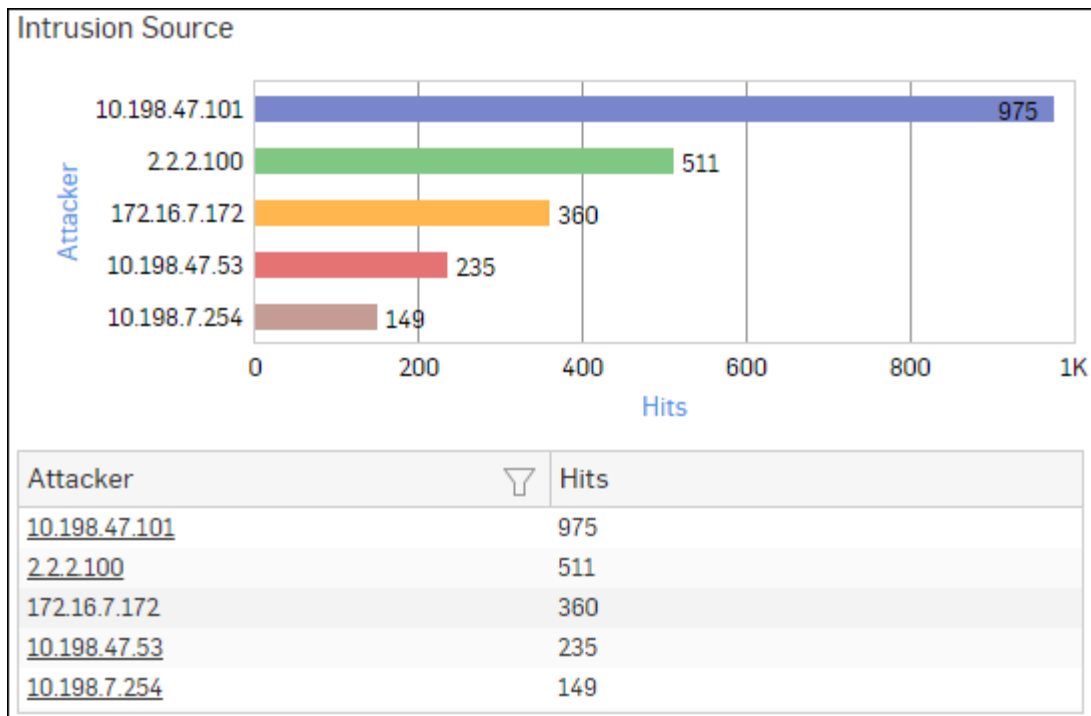


Figure 260: Intrusion Source

Click Attacker hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Web Server Users

This Report displays web server usage in terms of bandwidth utilization by users.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of domains along with bytes while the tabular report contains the following information:

- User: Username of the user, as defined in the Device.
- Bytes: Bandwidth used per user.
- Hits: Number of hits per user.

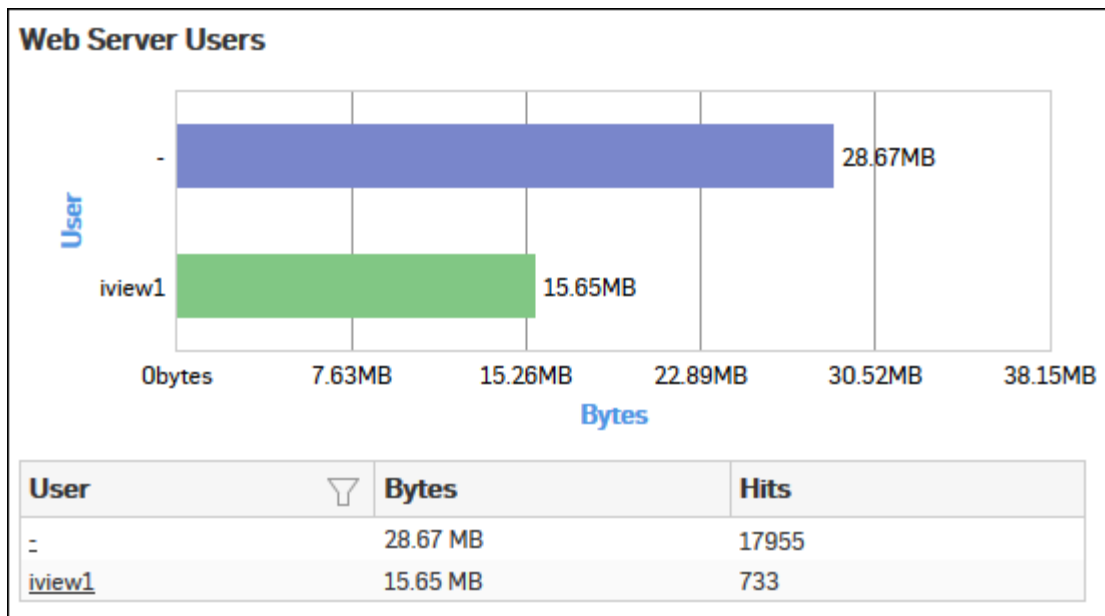


Figure 261: Web Server Users

Click the User hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Blocked Web Server Requests

This Report displays a list of reasons of attacks blocked by the Device, along with the number of hits per attack.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Blocked Web Server Requests**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Server Requests** as well.

The bar graph displays the list of blocked reasons along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

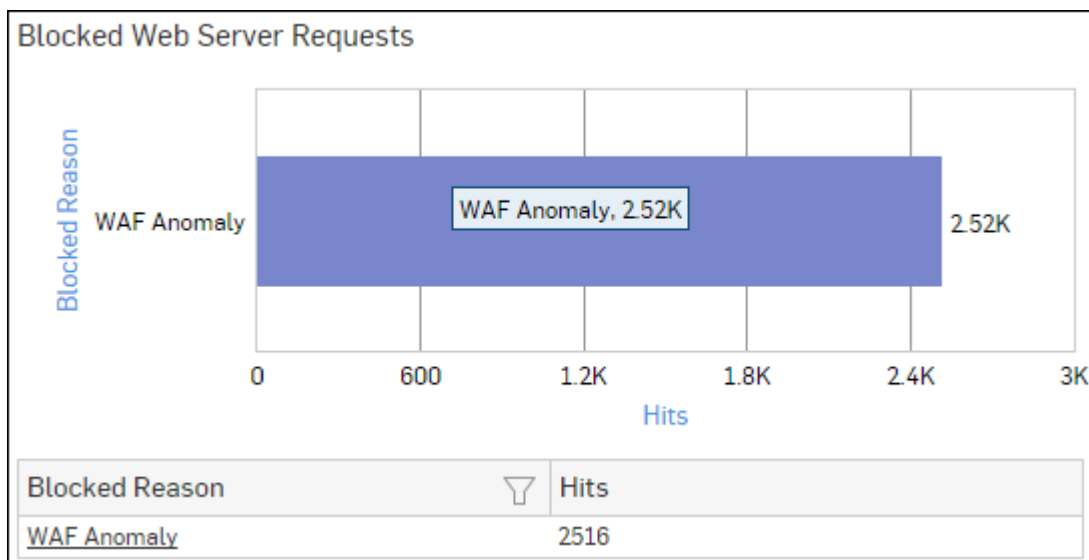


Figure 262: Blocked Web Server Requests

Click the Blocked Reason hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Admin Events

This Report displays the Admin Event details including time, event type, severity, message, username, source and status.

View report from **Monitor & Analyze > Reports > Compliance > Events > Admin Events**.

The tabular report contains the following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :
 - GUI
 - CLI
 - Console
 - SFM
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful






Admin Events						
Time	Event 	Severity	Mess... 	User 	Source 	Status 
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful
2015-12-1...	GUI	Information	User dhire...	dhiren	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	dhiren	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful

Figure 263: Admin Events

Authentication Events

This Report displays the Authentication Events detail including time, event type, severity, message, username, source and status.

View the report from **Monitor & Analyze > Reports > Compliance > Events > Authentication Events**.

Tabular report contains following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :

- Firewall Authentication
- My Account Authentication
- VPN Authentication
- SSL VPN Authentication
- Dial-in Authentication
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User Name: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful

Authentication Events						
Time	Event ▾	Severity	Mess... ▾	User ▾	Source ▾	Status ▾
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed

Figure 264: Authentication Events

Hosts - ATP

This report displays a comprehensive summary of host wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Hosts-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Hosts-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of events per host while the tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Threat Count: Number of threats per source host.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

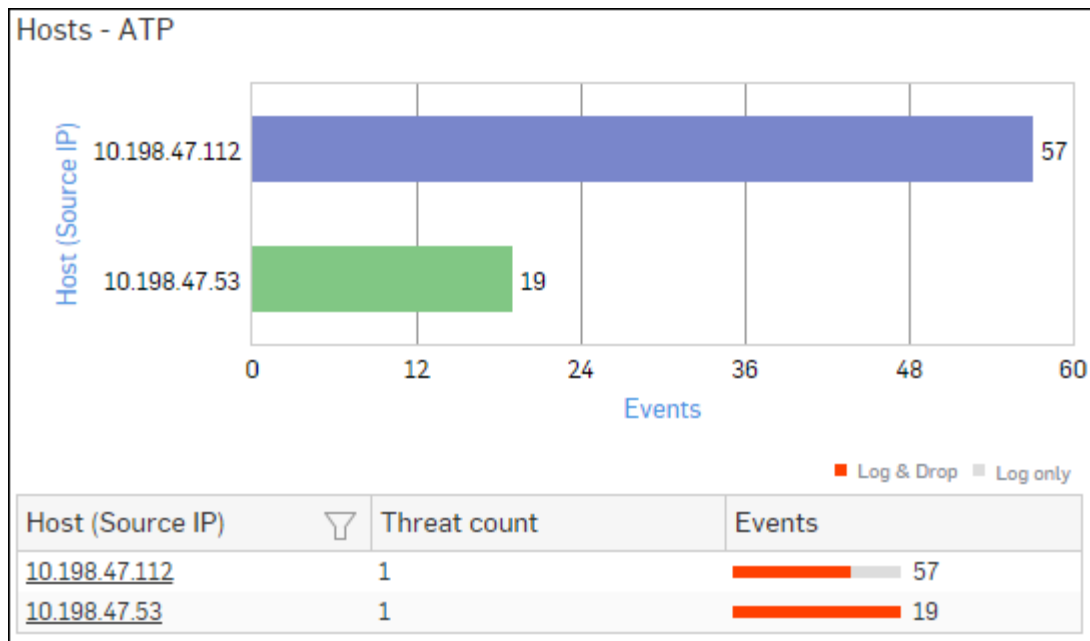


Figure 265: Hosts - ATP

Click Host hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Detailed View - Client Health

This report shows in-depth information regarding health status of endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Detailed View - Client Health**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Detailed View - Client Health** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Host Name: Name of the client.
- Health - Last Seen: Displays the latest health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.





Detailed View - Client Health				
Host (Source IP) ▾	Host Name ▾		Health - Last Seen	Last Health
10.20.41.8	TWIN8164BIT		Red	-
10.20.41.7	TWIN864		Yellow	-
10.198.38.8	TWIN764		Green	-
10.20.41.12	TWIN832		Green	-

Figure 266: Detailed View - Client Health

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Detailed View - ATP

This report provides a detailed summary of advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Detailed View - ATP**.

The report is displayed in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page..

The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- User: Username of the infected user.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Origin: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - Web
 - Combination of any of the above
- Events: Total number of events. The number is summation of Log only and Log & Drop events.
- Action: Action performed by the Device when a threat is detected. Possible options:
 - Log & Drop: The data packet is logged and dropped.
 - Log only: The data packet is logged.

Detailed View - ATP									
Host (Source IP) ▾	User ▾	Threat ▾	Threat URL/IP ▾	Origin	Events	Action			
10.198.47.112	dp	C2/Generic-A	46.161.30.47	Firewall	54	Log & Drop			
10.198.47.112	dp	C2/Generic-A	213.21.21.170	Firewall	45	Log & Drop			
10.198.47.112	atp1	C2/Generic-A	46.161.30.47	Firewall	27	Log & Drop			
10.198.47.112	atp1	C2/Generic-A	213.21.21.170	Firewall	27	Log & Drop			
10.198.47.112	atp1	C2/Generic-A	77.91.166.16	Firewall	18	Log & Drop			

Figure 267: Detailed View - ATP

Security Heartbeat - ATP

This report provides an insight into advanced threats related to endpoints in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Security Heartbeat - ATP**.

The report is displayed in a tabular format. The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Login User: Username of the infected user.
- Process User: Username of the user owning the process.
- Executable: Name of the infected executable file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Event Last Seen: Time when the infected executed file was last found in the host.
- Events: Total number of events. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP							
Host (Source IP)	Login User	Process User	Executable	Threat	Threat URL/IP	Event Last Seen	Events
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1

Figure 268: Security Heartbeat - ATP

SOX

SOX report is the grouping of various network security reports which ensures compliance with Sarbanes-Oxley (SOX).

SOX mandates financial public companies to assess risk associated with their organization's network.

View SOX reports from **Monitor & Analyze > Reports > Compliance > SOX**.

It enables to view the following reports:

- [Spam Recipients](#)
- [Spam Senders](#)
- [Web Virus](#)
- [Virus Summary](#)
- [Mail Virus](#)
- [Mail Virus by Application Type](#)
- [Web Server Virus](#)
- [FTP Virus](#)
- [Intrusion Attacks](#)
- [Intrusion Source](#)
- [Web Server Users](#)
- [Blocked Web Server Requests](#)
- [Admin Events](#)
- [Authentication Events](#)
- [Hosts - ATP](#)
- [Detailed View - Client Health](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)

FISMA

FISMA report is the grouping of various network security reports which ensures compliance with Federal Information Security Management Act (FISMA).

FISMA makes sure that each federal company should have information security solution in place.

View FISMA reports from **Monitor & Analyze > Reports > Compliance > FISMA**.

It enables to view the following reports:

- [Web Virus](#)
- [Virus Summary](#)
- [Mail Virus](#)

- [Mail Virus by Application Type](#)
- [Web Server Virus](#)
- [FTP Virus](#)
- [Intrusion Attacks](#)
- [Intrusion Source](#)
- [Web Server Users](#)
- [Blocked Web Server Requests](#)
- [Admin Events](#)
- [Authentication Events](#)
- [Hosts - ATP](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)

Web Virus

This Report lists viruses blocked by the Device as well as number of occurrence per blocked virus.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked web viruses along with number of counts per virus while the tabular report contains the following information:

- Virus: Name of the blocked web virus.
- Count: Number of times a virus was blocked.

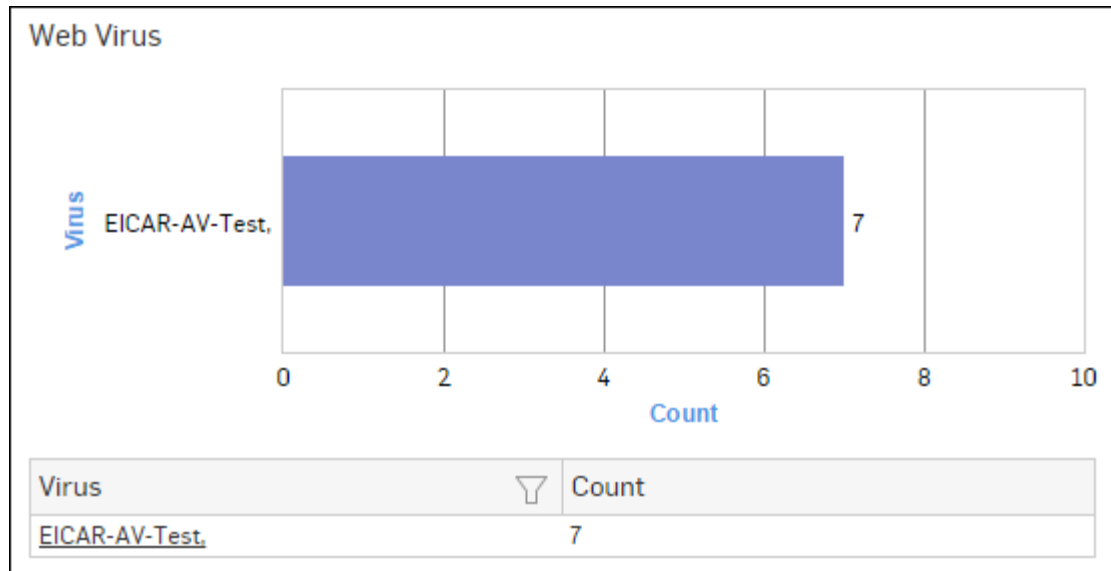


Figure 269: Web Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Virus Summary

This Report provides an overview of Virus traffic in your network, in terms of protocols through which viruses were introduced in the network as well as number of counts per protocol.

View the report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Virus Summary**.

The Report is displayed using a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays number of counts per protocol through which viruses were introduced in the network, while the tabular report contains following information:

- Application/Proto:Port: Name of the protocol through which viruses were introduced in the network.
- Count: Number of counts per protocol.

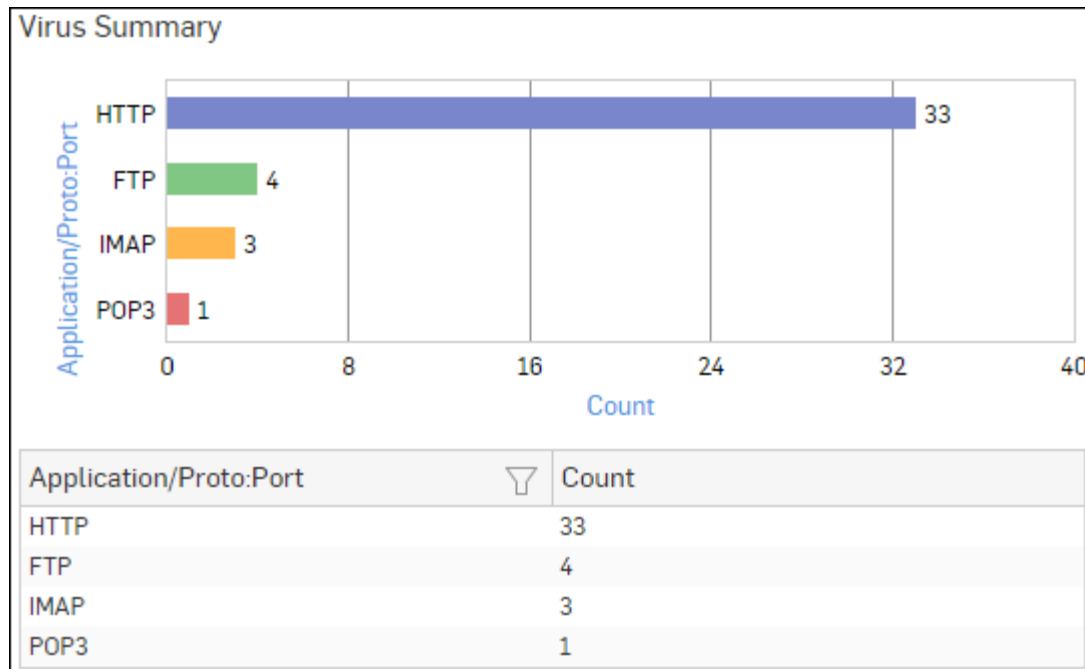


Figure 270: Virus Summary

Click Application hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Mail Virus

This Report displays Viruses detected in your network along with number of hits per Virus.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus while the tabular report contains the following information:

- Virus: Name of the virus.
- Count: Number of counts per mail virus.

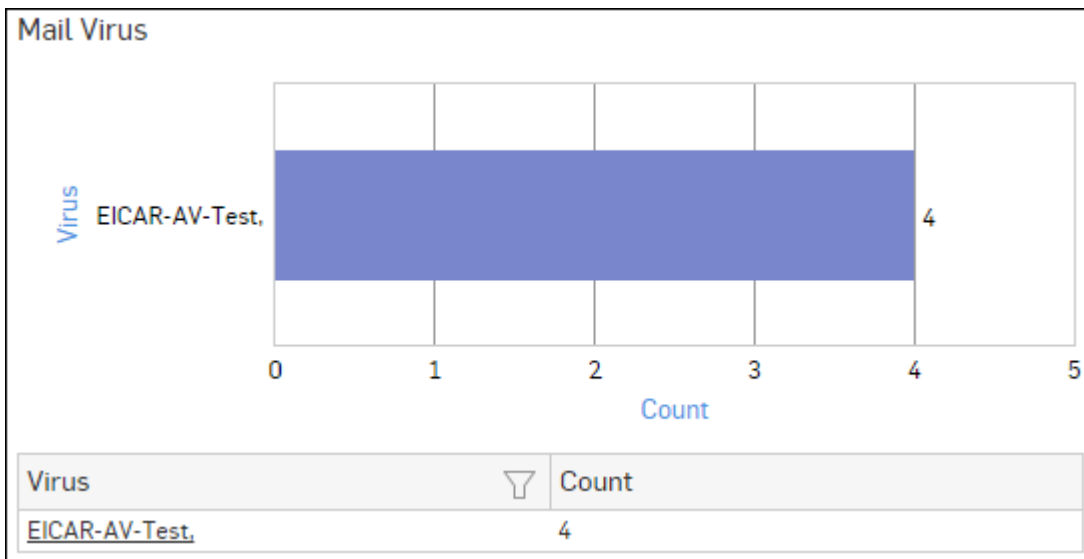


Figure 271: Mail Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Mail Virus by Application Type

This Report provides an overview of mail viruses by their application type.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus by Application Type**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of email viruses per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the application, as defined in the Device. If the application is not defined in the Device then this field displays the application identifier as combination of protocol and port number.
- Count: Number of email viruses per application.

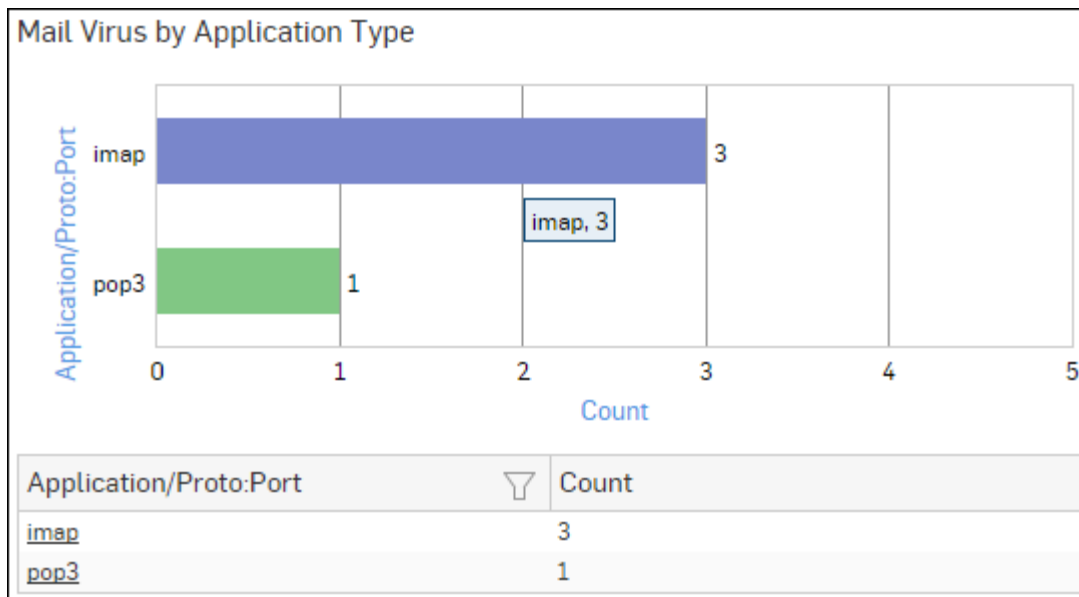


Figure 272: Mail Virus by Application Type

Click the Application hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Web Server Virus

This report displays a list of blocked viruses along with number of hits per virus.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Web Server Virus**.

The bar graph displays the list of viruses and number of hits while the tabular report contains the following information:

- Virus: Name of the Virus blocked by the Device.
- Hits: Number of hits per blocked virus.

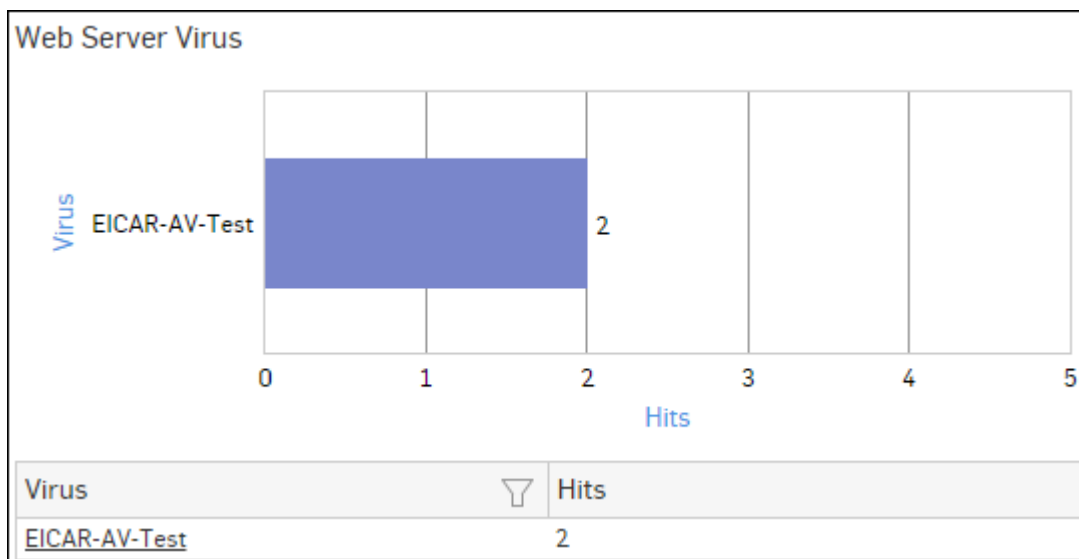


Figure 273: Web Server Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

FTP Virus

This Report displays a list of the FTP viruses and number of counts per virus.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > FTP Virus**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per virus while the tabular report contains the following information:

- Virus: Name of the FTP virus.
- Count: Number of counts for the virus.

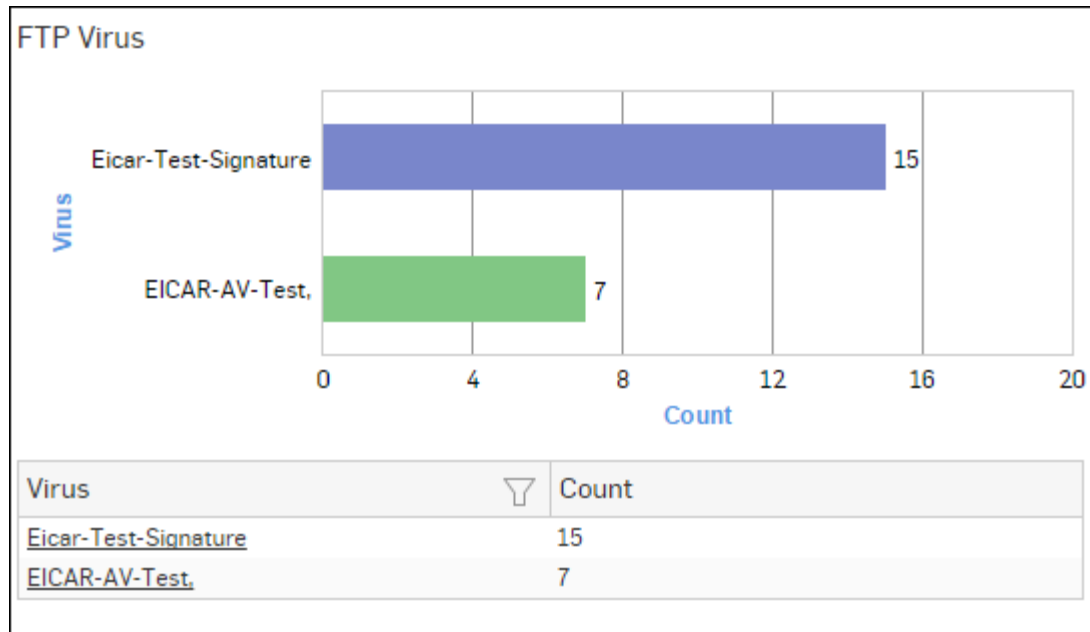


Figure 274: FTP Virus

Click the Virus hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Intrusion Attacks

The Report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Attacks**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Attacks** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each attack, while the tabular report contains the following information:

- Attack: Name of the attack launched.
- Hits: Number of hits for each attack.

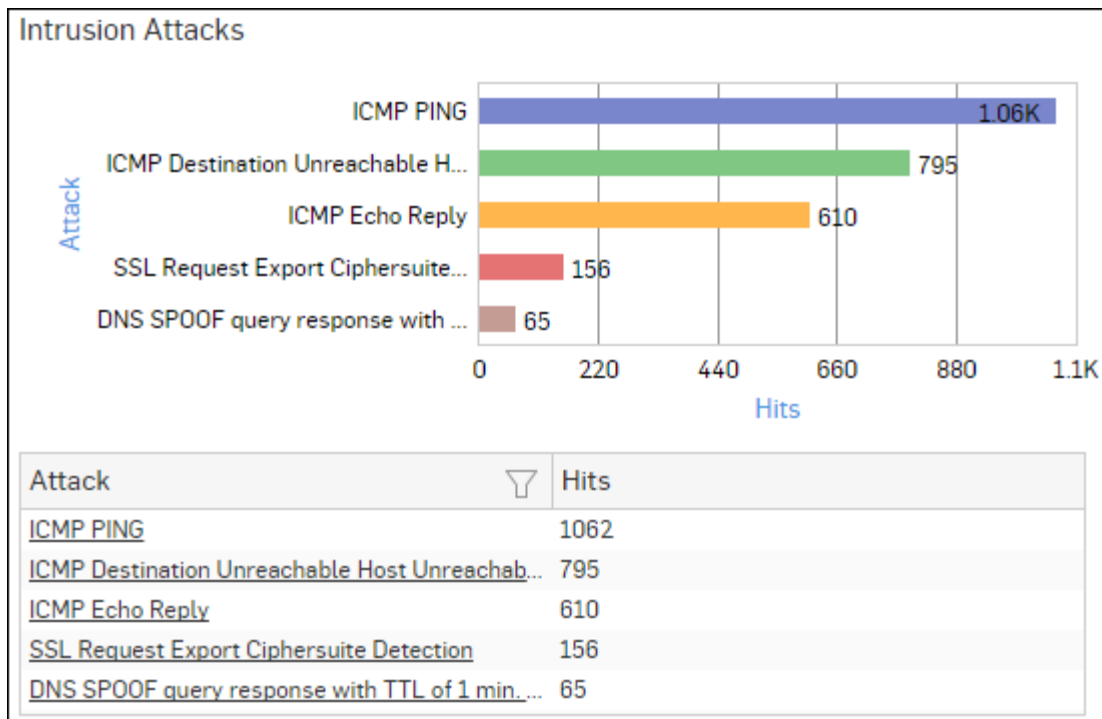


Figure 275: Intrusion Attacks

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Source

The Report enables to view the details of the attacker(s) who have hit the system and gives the detailed disintegration of attacks, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Source**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Source** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each attacker, while the tabular report contains the following information:

- Attacker: IP Address of the attacker.
- Hits: Number of hits for each attacker.

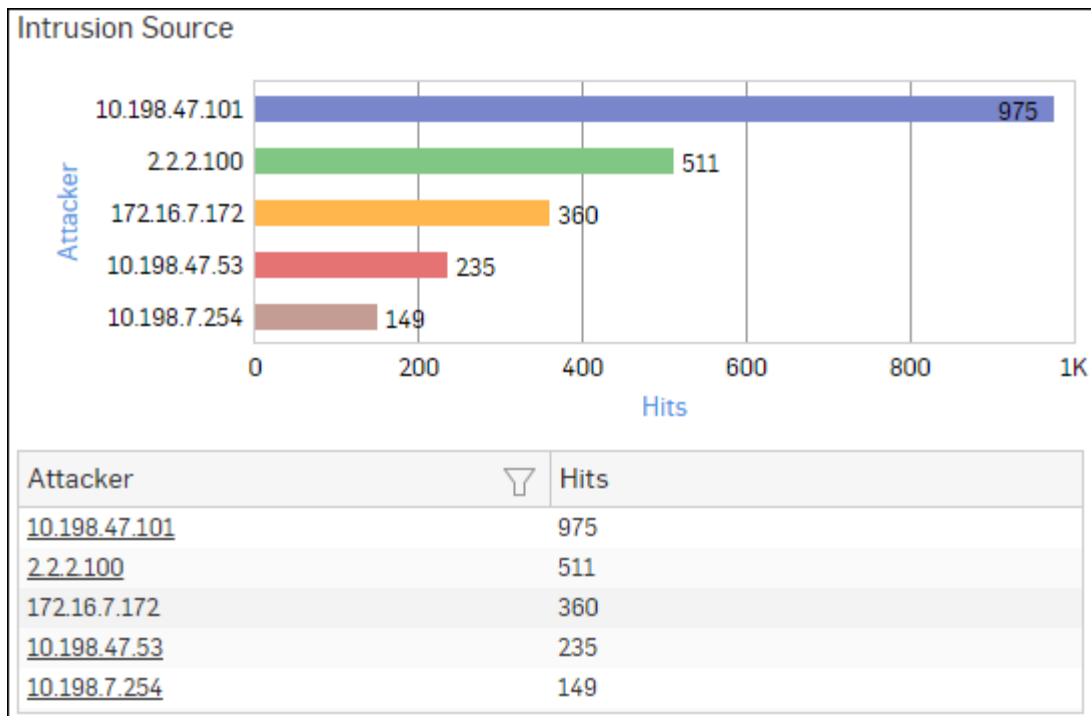


Figure 276: Intrusion Source

Click Attacker hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Web Server Users

This Report displays web server usage in terms of bandwidth utilization by users.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of domains along with bytes while the tabular report contains the following information:

- User: Username of the user, as defined in the Device.
- Bytes: Bandwidth used per user.
- Hits: Number of hits per user.

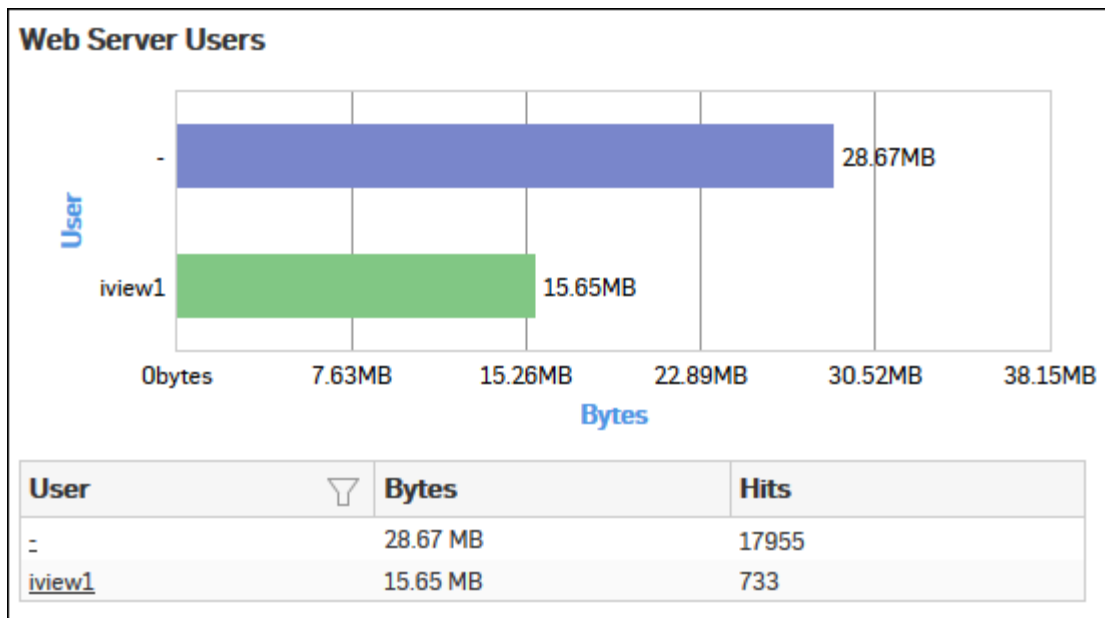


Figure 277: Web Server Users

Click the User hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Blocked Web Server Requests

This Report displays a list of reasons of attacks blocked by the Device, along with the number of hits per attack.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Blocked Web Server Requests**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Server Requests** as well.

The bar graph displays the list of blocked reasons along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

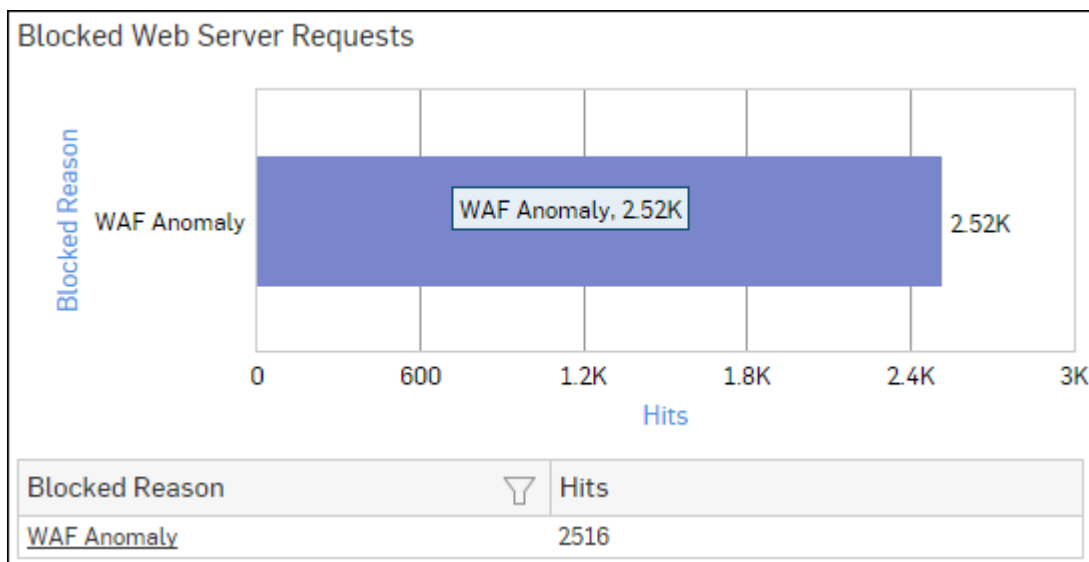


Figure 278: Blocked Web Server Requests

Click the Blocked Reason hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Admin Events

This Report displays the Admin Event details including time, event type, severity, message, username, source and status.

View report from **Monitor & Analyze > Reports > Compliance > Events > Admin Events**.

The tabular report contains the following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :
 - GUI
 - CLI
 - Console
 - SFM
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful






Admin Events						
Time	Event 	Severity	Mess... 	User 	Source 	Status 
2015-12-1...	GUI	Information	Administra...	admin	10.198.47....	Successful
2015-12-1...	GUI	Information	User dhire...	dhiren	10.198.47....	Successful
2015-12-1...	GUI	Information	Administra...	dhiren	10.198.47....	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47....	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47....	Successful

Figure 279: Admin Events

Authentication Events

This Report displays the Authentication Events detail including time, event type, severity, message, username, source and status.

View the report from **Monitor & Analyze > Reports > Compliance > Events > Authentication Events**.

Tabular report contains following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :

- Firewall Authentication
- My Account Authentication
- VPN Authentication
- SSL VPN Authentication
- Dial-in Authentication
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User Name: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful

Authentication Events						
Time	Event ▾	Severity	Mess... ▾	User ▾	Source ▾	Status ▾
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed

Figure 280: Authentication Events

Hosts - ATP

This report displays a comprehensive summary of host wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Hosts-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Hosts-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of events per host while the tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Threat Count: Number of threats per source host.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

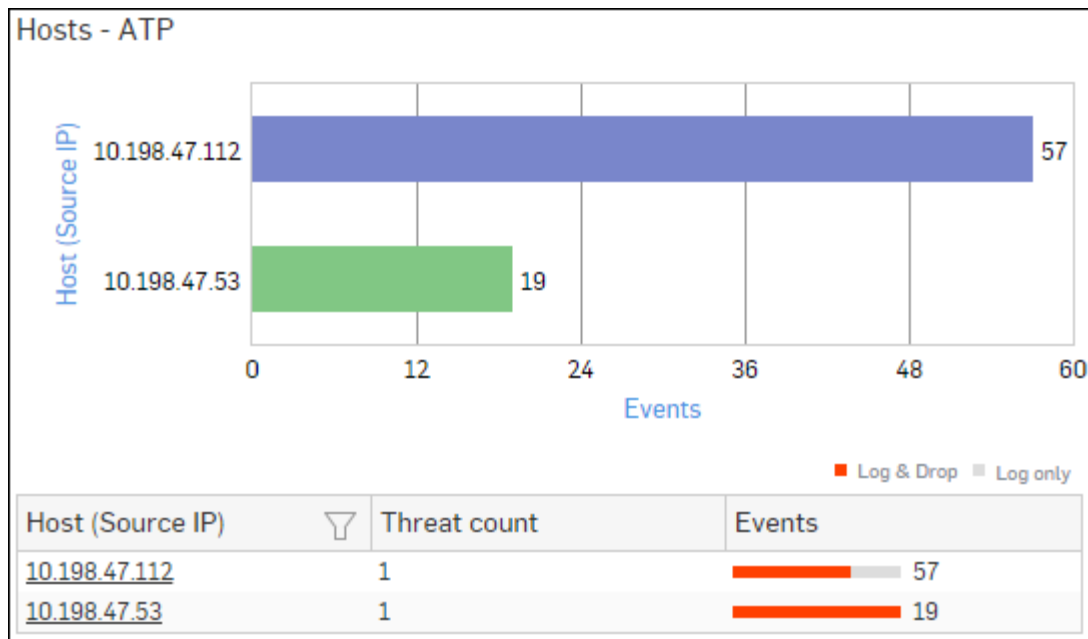


Figure 281: Hosts - ATP

Click Host hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Detailed View - Client Health

This report shows in-depth information regarding health status of endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Detailed View - Client Health**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Detailed View - Client Health** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Host Name: Name of the client.
- Health - Last Seen: Displays the latest health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.





Detailed View - Client Health				
Host (Source IP) ▾	Host Name ▾		Health - Last Seen	Last Health
10.20.41.8	TWIN8164BIT		Red	-
10.20.41.7	TWIN864		Yellow	-
10.198.38.8	TWIN764		Green	-
10.20.41.12	TWIN832		Green	-

Figure 282: Detailed View - Client Health

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Security Heartbeat - ATP

This report provides an insight into advanced threats related to endpoints in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Security Heartbeat - ATP**.

The report is displayed in a tabular format. The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Login User: Username of the infected user.
- Process User: Username of the user owning the process.
- Executable: Name of the infected executable file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Event Last Seen: Time when the infected executed file was last found in the host.
- Events: Total number of events. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP									
Host (Source IP) ▾	Login User ▾	Process User ▾	Executable ▾	Threat ▾	Threat URL/IP ▾	Event Last Seen	Events		
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1		

Figure 283: Security Heartbeat - ATP

PCI

PCI report is the grouping of various network security reports which ensures compliance with Payment Card Industry (PCI).

PCI applies to an organization that processes, stores or transmits credit card data and consequently affects merchants with physical stores, hospitality industry as well as banks, bureau and service providers.

View PCI reports from **Monitor & Analyze > Reports > Compliance > PCI**.

It enables to view the following reports:

- [Web Virus](#)
- [Virus Summary](#)
- [Mail Virus](#)
- [Mail Virus by Application Type](#)
- [Web Server Virus](#)
- [FTP Virus](#)
- [Intrusion Attacks](#)
- [Intrusion Source](#)
- [Web Server Users](#)
- [Blocked Web Server Requests](#)
- [Admin Events](#)

- [Authentication Events](#)
- [Hosts - ATP](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)

Web Virus

This Report lists viruses blocked by the Device as well as number of occurrence per blocked virus.

View the report from Blocked Web Attempts reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Blocked Web Attempts > Web Virus**.

This Report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays blocked web viruses along with number of counts per virus while the tabular report contains the following information:

- Virus: Name of the blocked web virus.
- Count: Number of times a virus was blocked.

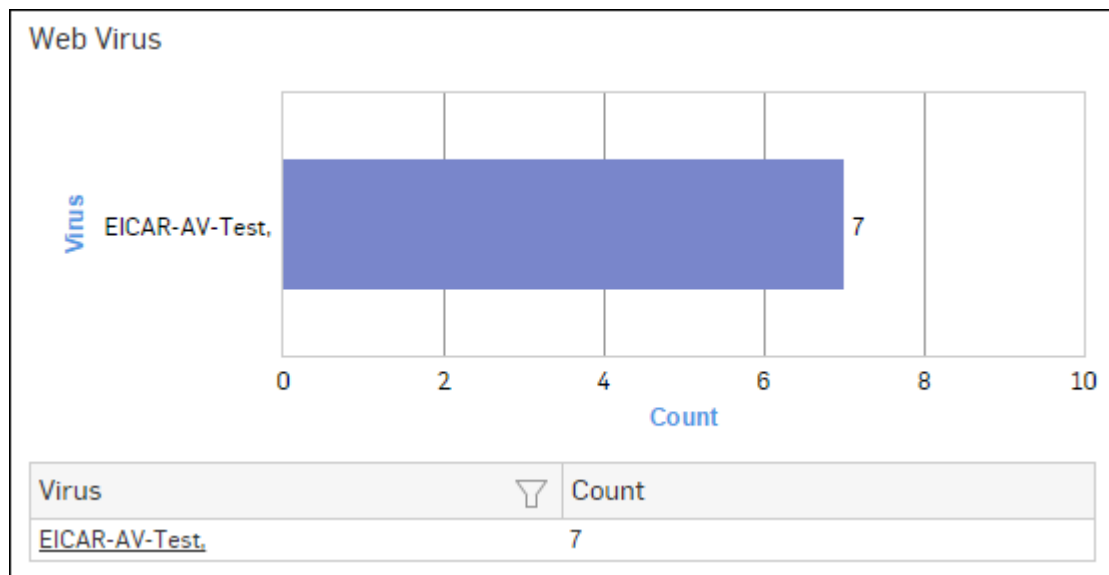


Figure 284: Web Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Blocked Web Attempts Reports - Virus](#).

Virus Summary

This Report provides an overview of Virus traffic in your network, in terms of protocols through which viruses were introduced in the network as well as number of counts per protocol.

View the report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Virus Summary**.

The Report is displayed using a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays number of counts per protocol through which viruses were introduced in the network, while the tabular report contains following information:

- Application/Proto:Port: Name of the protocol through which viruses were introduced in the network.
- Count: Number of counts per protocol.

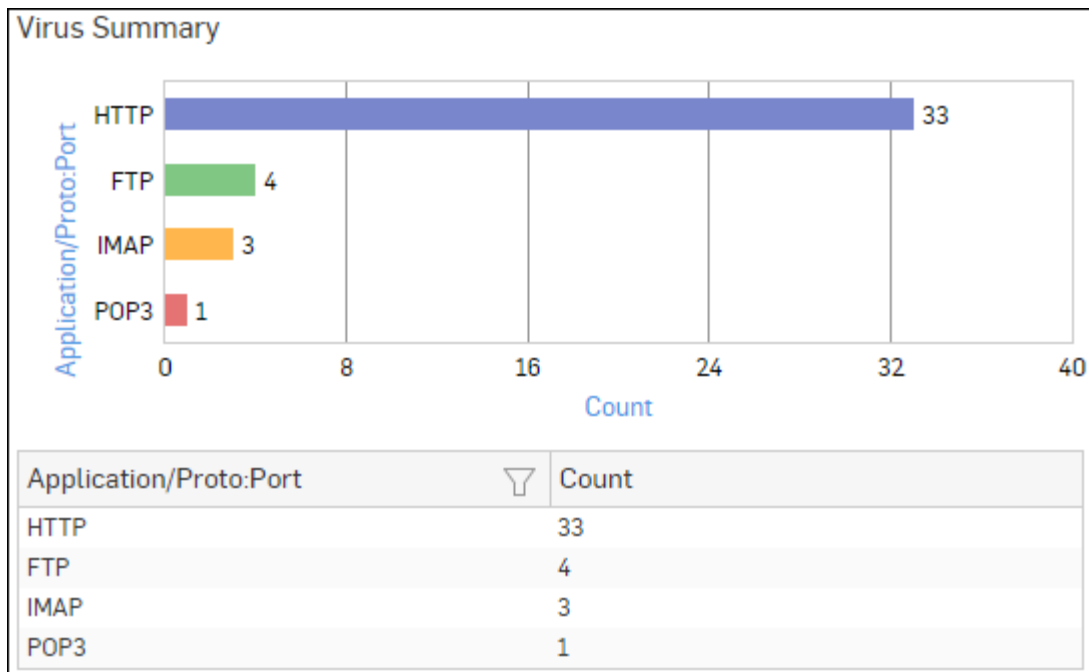


Figure 285: Virus Summary

Click Application hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Mail Virus

This Report displays Viruses detected in your network along with number of hits per Virus.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of counts per mail virus while the tabular report contains the following information:

- Virus: Name of the virus.
- Count: Number of counts per mail virus.

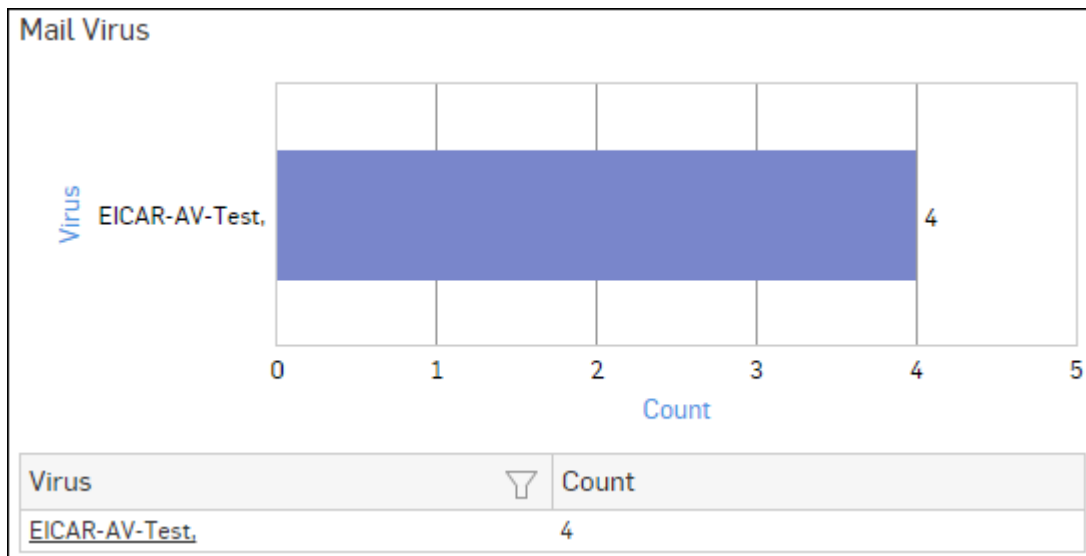


Figure 286: Mail Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Mail Virus by Application Type

This Report provides an overview of mail viruses by their application type.

View the report from Email Protection reports dashboard or from **Monitor & Analyze > Reports > Email > Email Protection > Mail Virus by Application Type**.

The Report is displayed as a bar graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of email viruses per application while the tabular report contains the following information:

- Application/Proto:Port: Name of the application, as defined in the Device. If the application is not defined in the Device then this field displays the application identifier as combination of protocol and port number.
- Count: Number of email viruses per application.

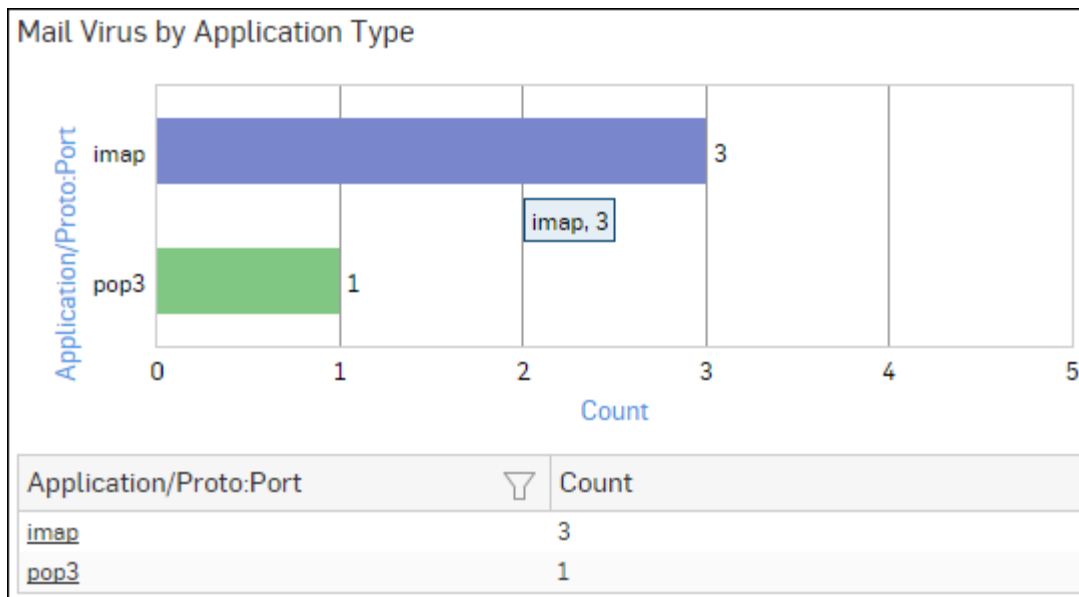


Figure 287: Mail Virus by Application Type

Click the Application hyperlink in the table or graph to view the [Filtered Virus Reports](#).

Web Server Virus

This report displays a list of blocked viruses along with number of hits per virus.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Web Server Virus**.

The bar graph displays the list of viruses and number of hits while the tabular report contains the following information:

- Virus: Name of the Virus blocked by the Device.
- Hits: Number of hits per blocked virus.

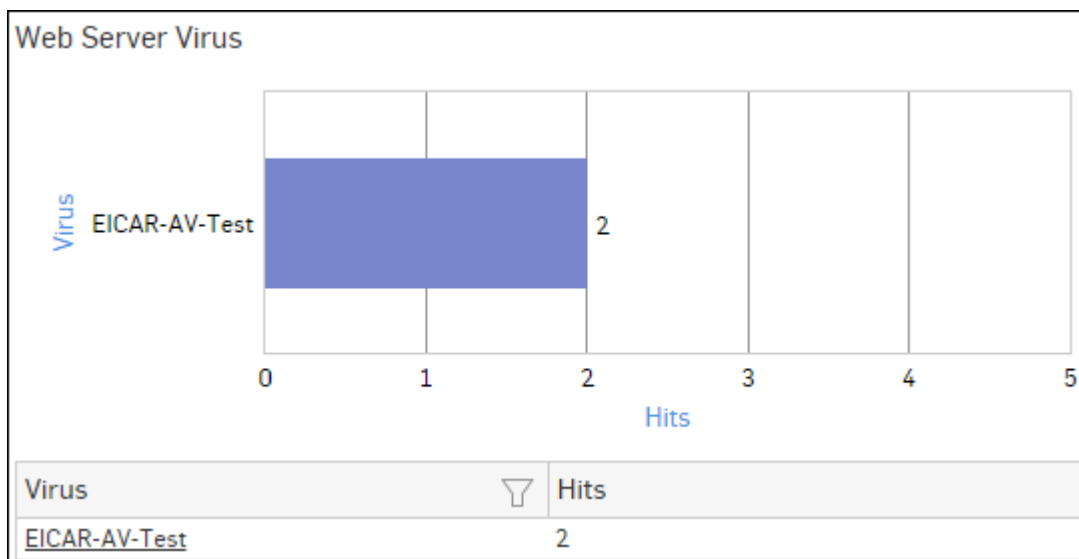


Figure 288: Web Server Virus

Click the Virus hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

FTP Virus

This Report displays a list of the FTP viruses and number of counts per virus.

View the report from FTP Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > FTP Protection > FTP Virus**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of virus counts per virus while the tabular report contains the following information:

- Virus: Name of the FTP virus.
- Count: Number of counts for the virus.

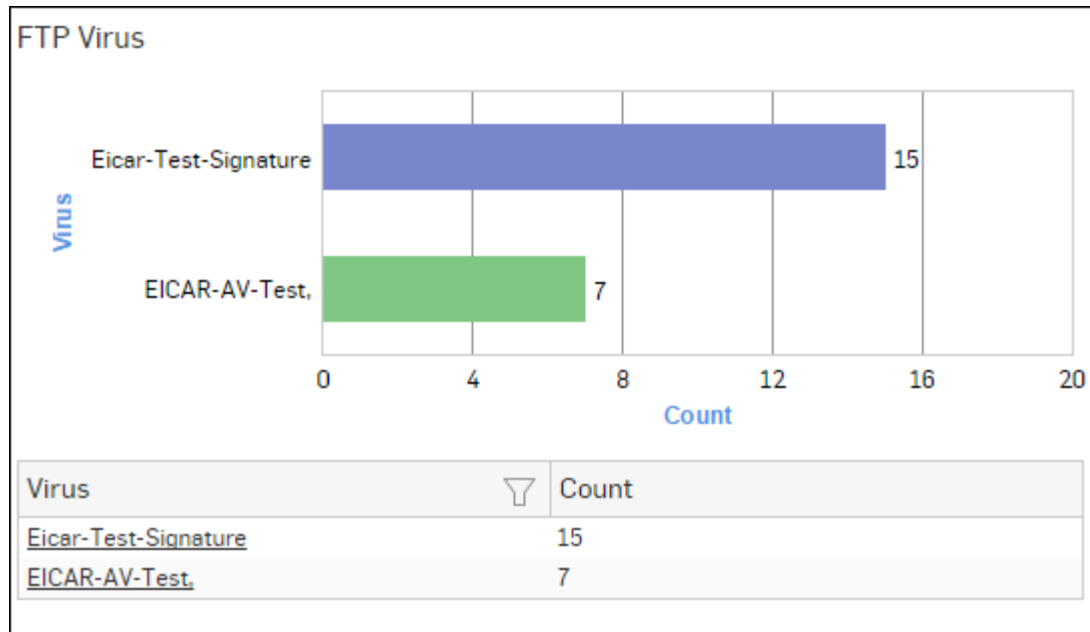


Figure 289: FTP Virus

Click the Virus hyperlink in the table or graph to view the [Filtered FTP Protection Reports](#).

Intrusion Attacks

The Report enables to view the details of the attack that has hit the system and gives the detailed disintegration of attackers, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Attacks**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Attacks** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits under each attack, while the tabular report contains the following information:

- Attack: Name of the attack launched.
- Hits: Number of hits for each attack.

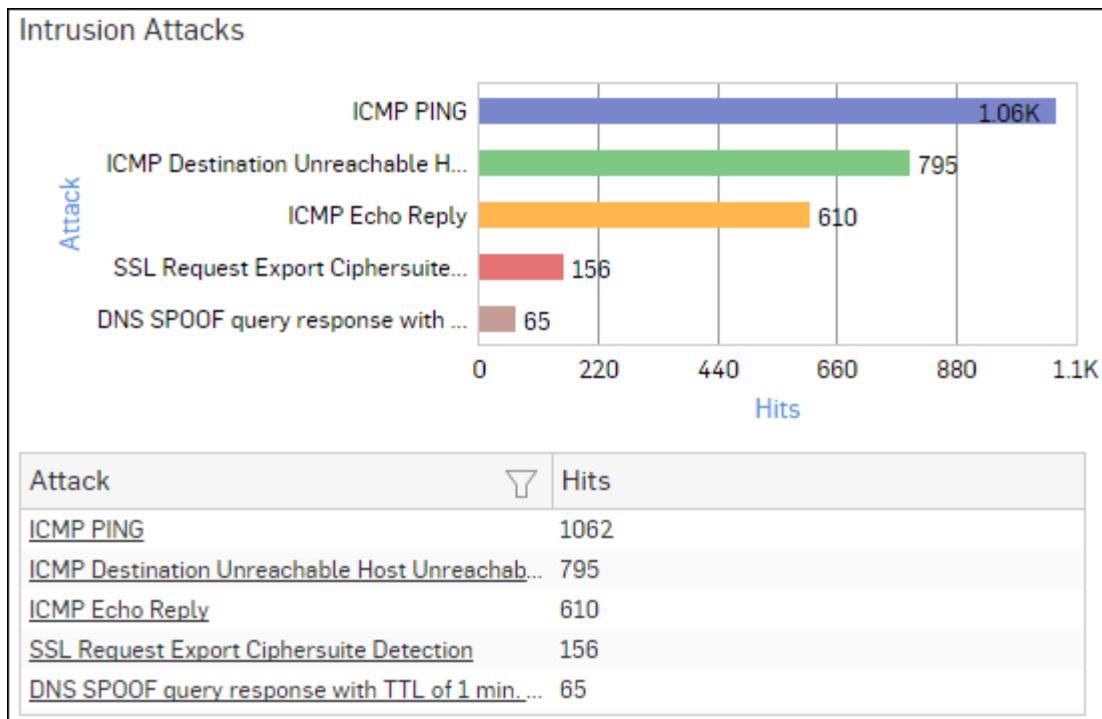


Figure 290: Intrusion Attacks

Click the Attack hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Intrusion Source

The Report enables to view the details of the attacker(s) who have hit the system and gives the detailed disintegration of attacks, victims and applications through individual reports.

View the reports from Intrusion Attacks reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Intrusion Attacks > Intrusion Source**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Intrusion Source** as well.

The Report is displayed as a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the number of hits by each attacker, while the tabular report contains the following information:

- Attacker: IP Address of the attacker.
- Hits: Number of hits for each attacker.

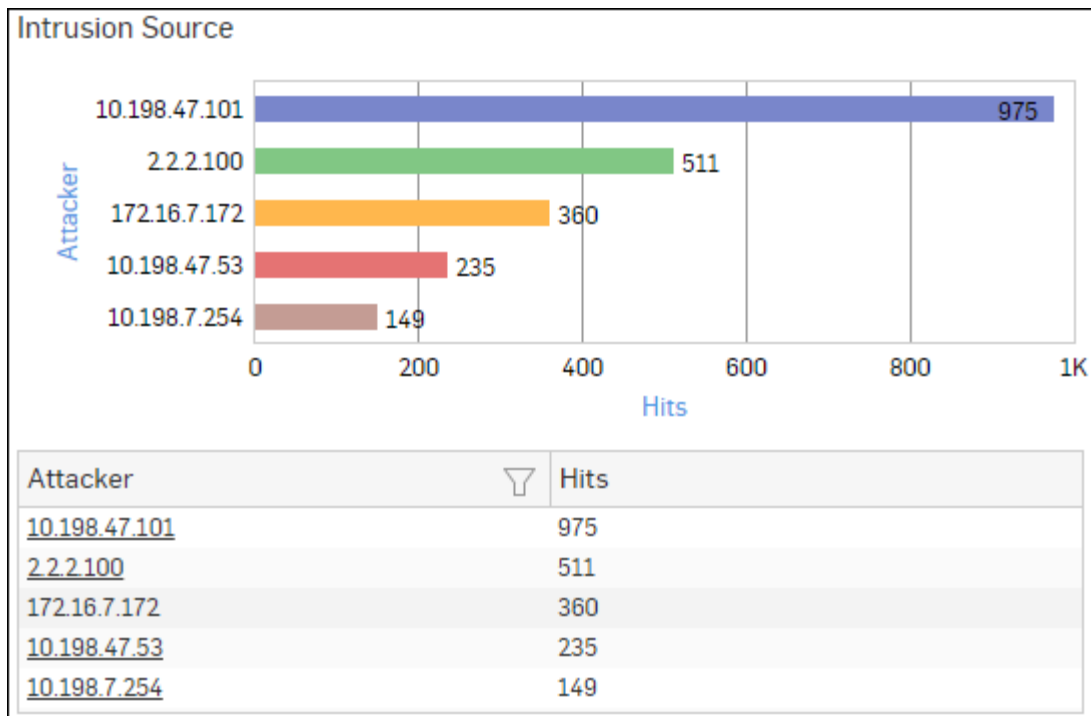


Figure 291: Intrusion Source

Click Attacker hyperlink in the table or graph to view the [Filtered Intrusion Attacks Reports](#).

Web Server Users

This Report displays web server usage in terms of bandwidth utilization by users.

View the report from Web Server Usage reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Usage > Web Server Users**.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays a list of domains along with bytes while the tabular report contains the following information:

- User: Username of the user, as defined in the Device.
- Bytes: Bandwidth used per user.
- Hits: Number of hits per user.

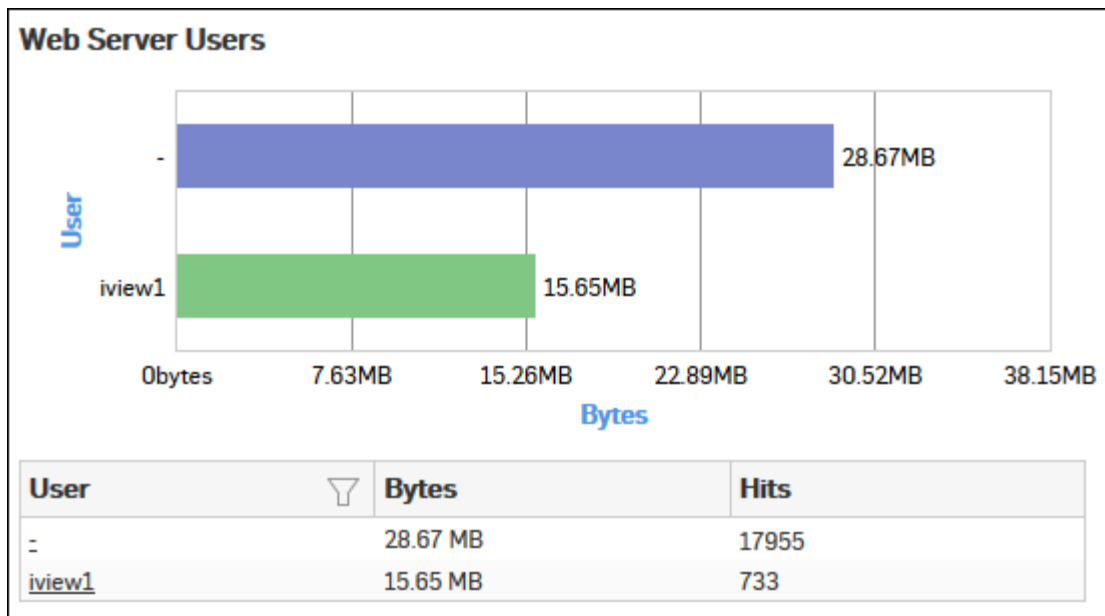


Figure 292: Web Server Users

Click the User hyperlink in the table or graph to view the [Filtered Web Server Usage Reports](#).

Blocked Web Server Requests

This Report displays a list of reasons of attacks blocked by the Device, along with the number of hits per attack.

View the report from Web Server Protection reports dashboard or from **Monitor & Analyze > Reports > Applications & Web > Web Server Protection > Blocked Web Server Requests**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Blocked Web Server Requests** as well.

The bar graph displays the list of blocked reasons along with the number of hits per attack, while the tabular report contains the following information:

- Blocked Reason: Reason of attack blocked by the Device.
- Hits: Number of hits per attack.

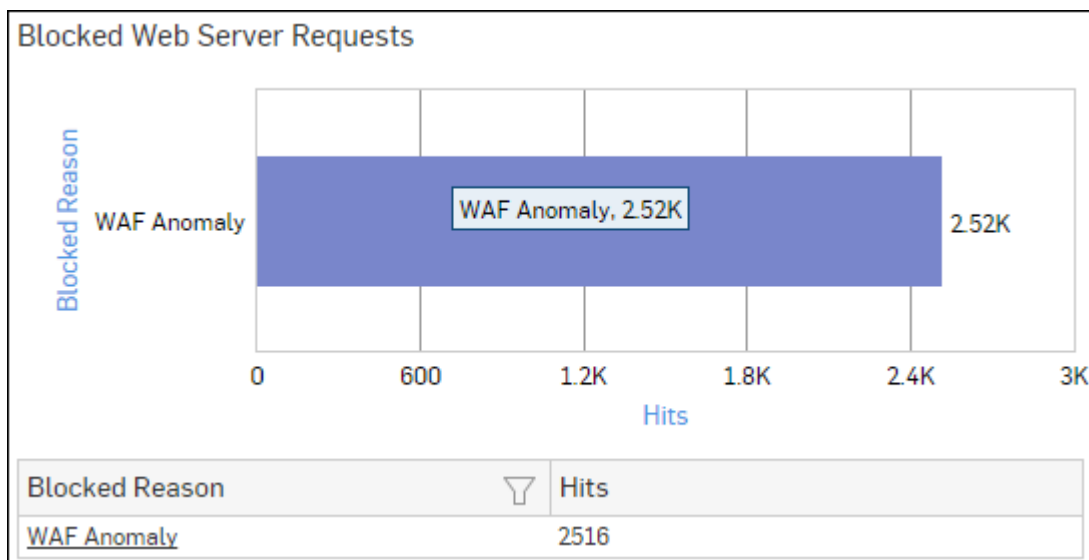


Figure 293: Blocked Web Server Requests

Click the Blocked Reason hyperlink in the table or graph to view the [Filtered Web Server Protection Reports](#).

Admin Events

This Report displays the Admin Event details including time, event type, severity, message, username, source and status.

View report from **Monitor & Analyze > Reports > Compliance > Events > Admin Events**.

The tabular report contains the following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :
 - GUI
 - CLI
 - Console
 - SFM
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful






Admin Events						
Time	Event 	Severity	Mess... 	User 	Source 	Status 
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful
2015-12-1...	GUI	Information	User dhire...	dhiren	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	dhiren	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47	Successful

Figure 294: Admin Events

Authentication Events

This Report displays the Authentication Events detail including time, event type, severity, message, username, source and status.

View the report from **Monitor & Analyze > Reports > Compliance > Events > Authentication Events**.

Tabular report contains following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :

- Firewall Authentication
- My Account Authentication
- VPN Authentication
- SSL VPN Authentication
- Dial-in Authentication
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User Name: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful

Authentication Events						
Time	Event ▾	Severity	Mess... ▾	User ▾	Source ▾	Status ▾
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed

Figure 295: Authentication Events

Hosts - ATP

This report displays a comprehensive summary of host wise advanced threats in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Hosts-ATP**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Hosts-ATP** as well.

The report is displayed using a graph as well as in a tabular format. By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of hosts along with number of events per host while the tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Threat Count: Number of threats per source host.
- Events: Total number of events per host. The number is summation of Log only and Log & Drop events.

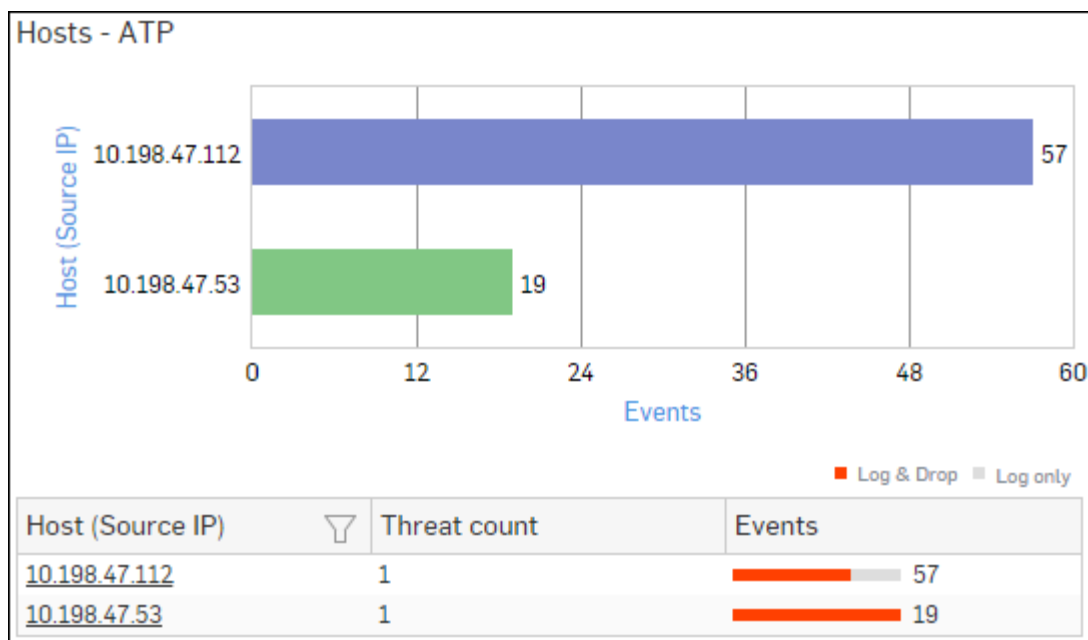


Figure 296: Hosts - ATP

Click Host hyperlink in the graph or table to view the [Filtered ATP Reports](#).

Detailed View - Client Health

This report shows in-depth information regarding health status of endpoints in your network.

View the reports from Security Heartbeat reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Security Heartbeat > Detailed View - Client Health**.



Note: You can view this report from **Monitor & Analyze > Reports > Dashboards > Security Dashboard > Detailed View - Client Health** as well.

The Report is displayed in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The tabular report contains the following information:

- Host (Source IP): IP Address of the endpoint.
- Host Name: Name of the client.
- Health - Last Seen: Displays the latest health status. Possible options are:
 - Green: The client is healthy, i.e. not infected with any malicious files.
 - Yellow: The client is potentially Objectionable, i.e. it may be infected with some malicious content.
 - Red: The client is Objectionable and is infected with some malicious content.
- Last Health: Displays the date in YYYY-MM-DD HH:MM:SS format when the health of the host was last changed.





Detailed View - Client Health				
Host (Source IP) ▾	Host Name ▾		Health - Last Seen	Last Health
10.20.41.8	TWIN8164BIT		Red	-
10.20.41.7	TWIN864		Yellow	-
10.198.38.8	TWIN764		Green	-
10.20.41.12	TWIN832		Green	-

Figure 297: Detailed View - Client Health

Click the Host hyperlink in the table to view the [Filtered Security Heartbeat Reports](#).

Security Heartbeat - ATP

This report provides an insight into advanced threats related to endpoints in your network.

View the report from ATP reports dashboard or from **Monitor & Analyze > Reports > Network & Threats > Advanced Threat Protection > Security Heartbeat - ATP**.

The report is displayed in a tabular format. The tabular report contains the following information:

- Host (Source IP): IP Address of the source host.
- Login User: Username of the infected user.
- Process User: Username of the user owning the process.
- Executable: Name of the infected executable file.
- Threat: Name of the threat.
- Threat URL/IP: IP Address of the infected destination.
- Event Last Seen: Time when the infected executed file was last found in the host.
- Events: Total number of events. The number is summation of Log only and Log & Drop events.

Security Heartbeat - ATP									
Host (Source IP) ▾	Login User ▾	Process User ▾	Executable ▾	Threat ▾	Threat URL/IP ▾	Event Last Seen	Events		
10.20.41.7	TWIN864\Administrator	TWIN864\Administrator	C:\program files (x86)\...	C2/Generic-A	92.240.99.70	2015-10-31 17:21:09	1		

Figure 298: Security Heartbeat - ATP

NERC CIP v3

NERC CIP v3 report is the grouping of various network security reports that helps organizations with critical infrastructures like ICS, Power Systems etc. to match some of the key cyber security requirements of NERC's CIP v3 standards.

To mitigate the security risks associated with critical infrastructures North American Electric Reliability Corporation (NERC) has established various standards to be followed by all users which are part of eco-system of these critical infrastructures.

Critical Infrastructure Protection Version 3 (CIP 001 to 009) standard is one of mandatory standards of NERC which deals with physical and cyber security of components which are functional in operating Bulk Power Systems.

View NERC CIP v3 reports from **Monitor & Analyze > Reports > Compliance > NERC CIP v3**.

It enables to view the following reports:

- [Applications](#)
- [Application Users](#)
- [Blocked Applications](#)
- [Blocked Application Users](#)
- [Intrusion Attacks](#)
- [Intrusion Source](#)
- [Web Server Users](#)

- [Blocked Web Server Requests](#)
- [Hosts - ATP](#)
- [Detailed View - ATP](#)
- [Security Heartbeat - ATP](#)
- [Detailed View - Client Health](#)
- [Virus Summary](#)
- [Mail Virus by Application Type](#)
- [Web Server Virus](#)
- [FTP Virus](#)
- [Admin Events](#)
- [Authentication Events](#)

CIPA

CIPA report is the grouping of various network security reports which ensures compliance with Children's Internet Protection Act (CIPA) criteria.

In 2000, United States' Congress enacted CIPA to try and stop kids from accessing obscene or harmful content via the Internet. CIPA is required for schools or libraries that receive E-rate discounts for Internet access or internal connections through the E-rate program.

View CIPA reports from **Monitor & Analyze > Reports > Compliance > CIPA**.

It enables to view the following reports:

- [Blocked Web Users](#)
- [Blocked Web Categories](#)
- [Blocked Web Domains](#)
- [Blocked Web Hosts](#)
- [Blocked Applications](#)
- [Google Search](#)
- [Yahoo Search](#)
- [Bing Search](#)
- [Wikipedia Search](#)
- [Rediff Search](#)
- [eBay Search](#)
- [Yandex Search](#)

Events

Events provide a snapshot of the network events along with their severity. It helps identify events which are critical to the network.

These reports can help assessing risk on the network and help to take corrective action.

View Event reports from **Monitor & Analyze > Reports > Compliance > Events**.

It enables to view below event details:

- [Event Summary](#)
- [Admin Events](#)
- [Authentication Events](#)
- [System Events](#)

Event Summary

This Report displays the list of Events along with the number of counts with the details event.

View the report from **Monitor & Analyze > Reports > Compliance > Events > Event Summary**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The Bar graph displays the number of counts per event while the tabular report contains the following information:

- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Count: Number of counts per event.

To view the [Event Summary Details](#) for a particular event drill down by clicking severity in the graph or the severity hyperlink in the table.

Event Summary Details

This Report displays the event details including time, event type, message, username, source and status.

View report from **Monitor & Analyze > Reports > Compliance > Events > Event Summary > Severity**.

The tabular report contains the following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :
 - DHCP Server
 - Firewall Authentication
 - My Account Authentication
 - VPN Authentication
 - SSL VPN Authentication
 - IPSec
 - L2TP
 - PPTP
 - GUI
 - Device
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User Name: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful

Admin Events

This Report displays the Admin Event details including time, event type, severity, message, username, source and status.

View report from **Monitor & Analyze > Reports > Compliance > Events > Admin Events**.

The tabular report contains the following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :

- GUI
- CLI
- Console
- SFM
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition
 - WARNING - Warning condition
 - NOTICE - Normal but significant condition
 - INFORMATION - Informational
 - DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful






Admin Events						
Time	Event 	Severity	Mess... 	User 	Source 	Status 
2015-12-1...	GUI	Information	Administra...	admin	10.198.47....	Successful
2015-12-1...	GUI	Information	User dhire...	dhiren	10.198.47....	Successful
2015-12-1...	GUI	Information	Administra...	dhiren	10.198.47....	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47....	Successful
2015-12-1...	GUI	Information	Administra...	admin	10.198.47....	Successful

Figure 299: Admin Events

Authentication Events

This Report displays the Authentication Events detail including time, event type, severity, message, username, source and status.

View the report from **Monitor & Analyze > Reports > Compliance > Events > Authentication Events**.

Tabular report contains following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :
 - Firewall Authentication
 - My Account Authentication
 - VPN Authentication
 - SSL VPN Authentication
 - Dial-in Authentication
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition

- ERROR - Error condition
- WARNING - Warning condition
- NOTICE - Normal but significant condition
- INFORMATION - Informational
- DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.
- User Name: Name of the user associated with the event.
- Source: IP Address of the event generator.
- Status: Status of the event. Possible status are:
 - Failed
 - Successful

Authentication Events						
Time	Event ▾	Severity	Mess... ▾	User ▾	Source ▾	Status ▾
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed
2015-12-0...	Not Availa...	Information	NTLM ena...	Unidentified	0.0.0.0	Failed

Figure 300: Authentication Events

System Events

This Report displays the System Events detail including time, event type, severity and message.

View report from **Monitor & Analyze > Reports > Compliance > Events > System Events**.

Tabular report contains following information:

- Time: Date and time of the event.
- Event Type: Type of the event. Possible event types are :
 - Device
 - Interface
 - Gateway
 - DDNS
 - Quarantine
 - DHCP Server
 - HA
 - IPSec
 - L2TP
 - PPTP
 - Webcat
 - IPS
 - AV
 - Dial-in
- Severity: Severity level of the events. Predefined level are:
 - EMERGENCY - System is not usable
 - ALERT - Action must be taken immediately
 - CRITICAL - Critical condition
 - ERROR - Error condition

- WARNING - Warning condition
- NOTICE - Normal but significant condition
- INFORMATION - Informational
- DEBUG - Debug - level messages
- Message: Message associated with event. Complete message can be viewed by placing cursor on the message.

System Events			
Time	Event Type	Severity	Message
2015-12-10 18:14:23	IPSec	Information	"sophos2copernicus-...
2015-12-10 18:14:03	IPSec	Information	"sophos2copernicus-...
2015-12-10 18:13:53	IPSec	Information	"sophos2copernicus-...
2015-12-10 18:13:53	IPSec	Information	"sophos2copernicus-...
2015-12-10 18:13:53	IPSec	Information	"sophos2copernicus-...

Figure 301: System Events

Bookmarks

This page displays list of Bookmark Groups configured in the device, in addition to the Default bookmark group.



Note: The Reports navigation pane displays Bookmarks menu only if at least one Report is bookmarked.

Use the [Bookmark Management](#) page to create and manage bookmark groups.

Click Bookmark hyperlink given at the top right of a report to save it as a bookmark. The bookmarked report is placed under the Default bookmark group, unless specified otherwise .

Custom

This section lets you to generate and view custom reports i.e. as per your requirement, you can customize the existing reports based on a set of filtering criteria.



Note: The Custom report sub sections can be accessed by selecting drop-down 1 given at the upper left corner of the page.

Custom report sections allows you to view following reports:

- [Custom Web Report](#) - Search web surfing and web virus reports based on user, domain and other criteria.
- [Custom Mail Report](#) - Search mail usage, mail protection and mail virus reports based on recipient and sender.
- [Custom FTP Report](#) - Search FTP usage and FTP virus reports based on user and other criteria.
- [Custom User Report](#) - Search usage and risk reports based on Username, IP Address, Sender's and Recipient's Email Addresses.
- [Custom Web Server Report](#) - Search Business application reports based on user, web server, attack and other criteria.

Custom Web Report

Use the **Monitor & Analyze > Reports > Custom > Custom Web Report** to perform a search in the Web Surfing Reports.

1. Go to **Monitor & Analyze > Reports > Custom > Custom Web Report** .
2. Specify the 'Search Type' value. Possible values are:
 - Web Surfing Reports

- Web Virus Reports
3. Specify the 'Report Type' value. Possible values are:
 - Summary
 - Detail
 4. Specify 'Search In' value. Possible values are:
 - Domain
 - URL
 - Category
 - IP Address
 5. Specify 'Search For' value. Possible values are:
 - User
 - Group

User Name/ Group Name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”. If the User Name/ Group Name is not specified, then search result will be displayed for all the defined Users/ Groups.

6. Specify the Domain/URL/Category Name/IP Address. If this is not specified, then the result will be displayed for all the Domain/URL/Category/IP Address.
7. Click Search.

Given below is the list of available Search Web Surfing reports:

- *Summary Web Surfing Reports by Domain and User*
- *Summary Web Surfing Reports by Domain and Group*
- *Summary Web Surfing Reports by Category and User*
- *Summary Web Surfing Reports by IP Address and User*
- *Detailed Web Surfing Reports by Domain and User*
- *Detailed Web Surfing Reports by Domain and Group*
- *Detailed Web Surfing Reports by URL and User*
- *Detailed Web Surfing Reports by URL and Group*
- *Detailed Web Surfing Reports by Category and User*
- *Detailed Web Surfing Reports by IP Address and User*
- *Detailed Web Virus Search Reports*

Summary Web Surfing Reports by Domain and User

This Report displays the number of hits and the amount of data transferred for the selected domain and user along with the web site name.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Web Surfing Reports
 - Report Type: Summary
 - Search In: Domain
 - Search For: User
 - User Name
 - Domain

The Tabular Report contains the following information:

- User Name: Username of the user as defined in the Device. If the User is unauthenticated or a clientless user, then it will be considered as traffic generated by an 'Unidentified' user.
- Domain: URLs of the website visited by the user.
- Hits: Number of hits to the user.

- Bytes: Amount of data transferred, in bytes.

Summary Web Surfing Reports by Domain and Group

This Report displays the number of hits and the amount of data transferred for the selected domain and group along with the web site name.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Web Surfing Reports
 - Report Type: Summary
 - Search In: Domain
 - Search For: Group
 - Group Name
 - Domain

The Tabular Report contains the following information:

- User Group: Group name of the user group as defined in the Device. If the group is unauthenticated, then it will be considered as traffic generated by an 'Unidentified' group.
- Domain: URLs of the website visited by the user group.
- Hits: Number of hits to the user group.
- Bytes: Amount of data transferred.

Summary Web Surfing Reports by Category and User

This Report displays the number of hits and amount of data transferred for the selected category and user.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Web Surfing Reports
 - Report Type: Summary
 - Search In: Category
 - Search For: User
 - User Name
 - Category Name

The Tabular Report contains the following information:

- User Name: Username of the user as defined in the Device. If the User is unauthenticated, then it will be considered as traffic generated by an 'Unidentified' user.
- Category: Name of the category as defined in the Device.
- Hits: Number of hits to the user.
- Bytes: Amount of data transferred.

Summary Web Surfing Reports by IP Address and User

This Report displays the number of hits and amount of data transferred for the selected category and user.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Web Surfing Reports
 - Report Type: Summary
 - Search In: IP Address
 - Search For: User
 - User Name
 - IP Address

The Tabular Report contains the following information:

- User Name: Username of the user as defined in the Device. If the User is not defined, then it will be considered as traffic generated by an 'Unknown' user.
- Host: IP Address of the host.
- Hits: Number of hits to the user.
- Bytes: Amount of data transferred.

Detailed Web Surfing Reports

This Report displays the number of hits and amount of data transferred for the selected domain and user along with the web site name.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Web Surfing Reports
 - Report Type: Detail
 - Search In: Domain / URL / Category / IP Address
 - Search For: User / Group
 - Domain
 - User Name / Group Name

The Tabular Report contains the following information:

- Time: Time of the Internet activity in YYYY-MM-DD HH:MM:SS format.
- User Name: Username of the user as defined in the Device. If the User is unauthenticated , then it will be considered as traffic generated by an 'Unidentified' user.
- User Group: Group name of the User Group as defined in the Device. If the group is unauthenticated , then it will be considered as traffic generated by an 'Unidentified' User Group.
- Domain: Domain name of the website visited by the user.
- URL: Complete URL path of the website visited by the user.
- Category: Name of the web category, as defined in the Device.
- IP Address: IP Address from which the user accessed the website.
- Policy Rule: Number displaying firewall rule ID.

Detailed Web Virus Search Reports

This Report displays the number of hits and amount of data transferred for the selected domain and user along with the web site name.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Web Virus Reports
 - Search In: Domain / URL / IP Address
 - User Name
 - Domain / URL / IP Address
 - Virus Name
 - Virus Search: HTTP / HTTPS

The Tabular Report contains the following information:

- Time: Time of the Internet activity in YYYY-MM-DD HH:MM:SS format.
- User Name: Username of the user as defined in the Device. If the User is unauthenticated, then it will be considered as traffic generated by an 'Unidentified' user.
- Domain: Domain name of the website visited by the user.
- URL: Complete URL path of the website visited by the user.
- Virus: Name of the virus identified by the Device.
- Protocol: Protocol name. Possible values are:
 - HTTP

- HTTPS
- Source IP: IP Address of the user.
- Destination IP: IP Address of the domain.

Custom Mail Report

Use the **Monitor & Analyze > Reports > Custom > Custom Mail Report** to search Mail Reports.

1. Go to **Monitor & Analyze > Reports > Custom > Custom Mail Report**.
2. Specify the search type. Available options are:
 - Mail Usage
 - Spam
 - Mail Virus
3. Specify the protocol. Available options are:
 - SMTP
 - SMTPS
 - POP3
 - POP3S
 - IMAP
 - IMAPS
4. Specify user type: Available User Types are:
 - Recipient
 - Sender
 - Any
5. Specify the User Email Address to be searched. Email Address can be any combination of alphanumeric characters and special characters “_”, “@” and “.”. If the Email Address is not specified then the search result will be displayed for all the Email Addresses.
6. Specify the Subject line to be searched. If the subject line is not specified then the search result will be displayed for all the subjects.
7. Click Search.

Given below is the list of available Search Mail reports:

- [Mail Usage Report](#)
- [Spam Report](#)
- [Mail Virus Report](#)

Mail Usage Report

This Report displays an overview of Mail Usage in your network.

1. To view the report go to **Monitor & Analyze > Reports > Custom > Custom Mail Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Mail Usage
 - Protocol: SMTP / SMTPS / POP3/ POP3S / IMAP / IMAPS
 - User Type: Recipient / Sender / Any
 - User Email Address (optional)
 - Subject (optional)

The Tabular report contains the following information:

- Time: Time of email activity in YYYY-MM-DD HH:MM:SS format.
- User Name: User Name of the user as defined in the Device.
- From: From Email ID.
- To: To Email ID.

- Subject: Subject line of the Email.
- Source IP: Source IP Address of the Email.
- Destination IP: Destination IP Address of the Email.
- Mail Size: Amount of data transferred, in bytes.

Spam Report

This Report displays an overview of Spam emails in your network.

1. To view the report go to **Monitor & Analyze > Reports > Custom > Custom Mail Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Spam
 - Protocol: SMTP / SMTPS / POP3/ POP3S / IMAP / IMAPS
 - User Type: Recipient / Sender / Any
 - User Email Address (optional)
 - Subject (optional)

The Tabular report contains the following information:

- Time: Time of email activity in YYYY-MM-DD HH:MM:SS format.
- From: From Email ID.
- To: To Email ID.
- Subject: Subject line of the Email.
- Rule Name : Applicable spam rule name.
- Action: Action taken on the spam: Possible actions:
 - Reject
 - Drop
 - Accept
 - Change Recipient
 - Prefix Subject
 - Quarantine

Mail Virus Report

This Report displays an overview of Virus emails in your network.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Mail Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: Mail Virus
 - Protocol: SMTP / SMTPS / POP3/ POP3S / IMAP / IMAPS
 - User Type: Recipient / Sender / Any
 - User Email Address (optional)
 - Subject (optional)
 - Virus (optional)

The Tabular report contains the following information:

- Time: Time of email activity in YYYY-MM-DD HH:MM:SS format.
- From: From Email ID.
- To: To Email ID.
- Subject: Subject line of the Email.
- Virus: Name of the virus.
- Protocol: Protocol name.
- Source IP: Source IP Address of the Email.
- Destination IP: Destination IP Address of the Email.
- Action: Action taken on the virus: Possible actions:

- Reject
- Drop
- Accept
- Change Recipient
- Prefix Subject
- Quarantine
- Rule Name : Applicable spam rule name.

Custom FTP Report

Use **Monitor & Analyze > Reports > Custom > Custom FTP Report** to perform a search in the FTP reports.

1. Go to **Monitor & Analyze > Reports > Custom > Custom FTP Report**.
2. Specify the 'Search Type'. Available options are:
 - FTP Usage
 - FTP Virus
3. Specify the file 'Transfer Type'. Available options are:
 - Download
 - Upload
 - Any
4. Specify the 'Search For' criteria: Available options:
 - User
 - File
 - Source IP
5. Specify the User Name / File Name or Source IP Address to be searched. If none of the parameters is specified, then search result will be displayed for all the users, files and source IP Addresses.
6. Click Search.

Given below is the list of available Search Mail reports:

- [FTP Usage Search Report](#)
- [FTP Virus Search Report](#)

FTP Usage Search Report

This Report provides an overview of FTP Usage in your network.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom FTP Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: FTP Usage
 - Transfer Type: Upload / Download / Any
 - Search For: User / File / Source IP
 - User Name / File Name / Source IP Address (optional)

The Tabular Report contains the following information:

- Time: Time in YYYY-MM-DD HH:MM:SS format.
- Client IP: IP Address of the machine from where the file transfer is done.
- Server IP: IP Address of the server where the file transfer is done.
- User: User name as defined in the Device.
- File: Name of the file.
- Direction: Upload / Download.
- Bytes: Amount of data transferred.

FTP Virus Search Report

This Report provides an overview of FTP Usage in your network.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom FTP Report**.
2. Specify the search parameters as mentioned below:
 - Search Type: FTP Virus
 - Transfer Type: Upload / Download / Any
 - Search For: User / File / Source IP
 - User Name (optional)
 - Virus Name (optional)

The Tabular Report contains the following information:

- Time: Time in YYYY-MM-DD HH:MM:SS format.
- Virus: Name of the virus.
- Protocol: Protocol name.
- File: Name of the file.
- User: User name as defined in the Device.
- Source IP: Source IP Address from where the file transfer is done.
- Destination IP: Destination IP Address where the file transfer is done.
- Direction: Upload / Download.

Custom User Report

Use **Monitor & Analyze > Reports > Custom > Custom User Report** to view custom reports by Username, Source Host, Sender's Email Address and Recipient's Email Address.

Custom User Report contains following dashboards:

- [Username](#)
- [Source Host](#)
- [Sender's Email Address](#)
- [Recipient's Email Address](#)

Select the criteria (username, source host, sender's Email Address and Recipient's Email Address) to view respective Custom User Reports dashboards.

Custom User Report by Username

The **Custom User Report by Username** dashboard provides a snapshot of network activities by the specified user.

To view the **Custom User Report by Username** dashboard:

- Go to **Monitor & Analyze > Reports > Custom > Custom User Report**.
- Select the criteria Username and specify it in the adjacent space provided.
- Click Go to view the customized dashboard.

The dashboard consists of the following reports in widget form:

- [Relative UTQ Score](#)
- [High Risk Applications](#)
- [Objectionable Web Domains](#)
- [Web Categories](#)
- [Virus Summary](#)
- [Unproductive Web Domains](#)
- [Applications](#)
- [Web Domains](#)
- [Spam Senders](#)
- [Spam Recipients](#)

- [Advanced Threats](#)
- [Web Server Usage](#)
- [Files Uploaded via FTP](#)
- [Files Downloaded via FTP](#)
- [Severity Level](#)
- [Web Virus](#)
- [User Data Transfer](#)

Relative UTQ Score

The widget report displays day-wise User Threat Quotient (UTQ) score of the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph and the tabular report contains the following information:

- Username: Name of the user, specified against the Username parameter.
- Days: Displays day out of the following options:
 - Last 14 Days
 - Last 7 Days
 - Last 1 Day
- Relative Score: Average threat posed by the user (in number), relative to the web behaviour of all other users, for the selected period.

High Risk Applications

The widget report displays applications with high risk level, accessed by the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per application while the tabular report contains the following information:

- Application/Proto:Port: Displays name of the Application as defined in the Device. If the application is not defined in the Device, then this field will display the application identifier as a combination of the protocol and port number associated with the application.
- Risk: Level of risk associated with the application.
- Hits: Number of hits per application.
- Bytes: Amount of data transferred through the application, in bytes.



Note: Click on an application to view the [Filtered User App Risks & Usage Reports](#).

Objectionable Web Domains

The widget report displays, for the selected user, details on frequently accessed web domains falling under a web category that is classified as 'Objectionable' in the Device.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per domain while the tabular graph displays following information:

- Domain: Domain name or IP Address of the domain.
- Category: Name of the web category, classified as Objectionable in the Device.
- Hits: Number of hits to the web domain.
- Bytes: Amount of data transferred through the web domain, in bytes.



Note: Click on a web domain to view the [Filtered Blocked Web Attempts Reports - Web](#).

Web Categories

The widget report displays number of hits and amount of data transferred per category for the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per category while the tabular graph displays following information:

- Category: Displays name of the category as defined in the Device. If the category is not defined in the Device then this field will display 'Uncategorized' instead of category name
- Hits: Number of hits to the category.
- Bytes: Amount of data transferred through the category, in bytes.



Note: Click on a web category to view the [Filtered Web Risks & Usage Reports](#).

Virus Summary

The widget report displays, for the selected user, number of hits per application that is identified as virus by the Device.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per application, while the tabular graph displays following information:

- Protocol: Name of the application / combination of protocol and port number associated with the application.
- Module: Module associated with the application.
- Count: Number of application occurrence.

Unproductive Web Domains

The widget report displays, for the selected user, details on frequently accessed web domains falling under a web category that is classified as Unproductive in the Device.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per domain while the tabular graph displays following information:

- Domain: Domain name or IP Address of the domain.
- Category: Name of the web category, classified as Unproductive in the Device.
- Hits: Number of hits to the web domain.
- Bytes: Amount of data transferred through the web domain, in bytes.



Note: Click on a web domain to view the [Filtered Web Risks & Usage Reports](#).

Applications

The widget report displays top applications accessed by the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per application while the tabular report contains the following information:

- Application/Proto:Port: Displays name of the Application as defined in the Device. If the application is not defined in the Device, then this field will display the application identifier as a combination of the protocol and port number associated with the application.
- Risk: Level of risk associated with the application.
- Category: Application Category, as defined in the Device.
- Hits: Number of hits per application.
- Bytes: Amount of data transferred through the application, in bytes.



Note: Click an application to view the [Filtered User App Risks & Usage Reports](#).

Web Domains

This Widget displays the list of domains along with number of hits and the total data transferred per domain.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays number of hits per domain, while the tabular report contains following information:

- Domain: Displays name of the domain.
- Hits: Number of hits per domain.
- Bytes: Amount the of data transfer.



Note: Click the Domain hyperlink in the table or the pie chart to view the [Filtered Web Risks & Usage Reports](#).

Spam Senders

The widget report displays list of the Email Addresses of the selected user used for sending Spam Emails.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per Email ID used for sending spams while the tabular graph displays following information:

- Sender: Email ID used for sending spams.
- Mail Count: Number of spam emails sent.
- Percentage: Percent distribution among the Email IDs.



Note: Click on a Sender Email ID to view the [Filtered Spam Reports](#).

Spam Recipients

The widget report displays list of the Email Addresses of the selected user that received most number of Spam Emails.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per Email ID that received most number of Spam Emails, while the tabular graph displays following information:

- Recipient: Email ID of the selected user that received most number of Spam Emails.
- Mail Count: Number of spam emails received.
- Percentage: Percent distribution among the Email IDs.



Note: Click on a Recipient Email ID to view the [Filtered Spam Reports](#).

Advanced Threats

This widget report displays a comprehensive summary of advanced threats in your network.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays total number of attempts per threat while the tabular report contains following information:

- Attack: Name of the attack.
- Host Count: Number of hosts infected with the attack.

- Origins: Origin of the threat. Possible options:
 - Firewall
 - IPS
 - DNS
 - HTTP Proxy
 - Combination of any of the above
- Events: Total number of events per threat. The number is summation of Log only and Log & Drop events.



Note: Click on a threat hyperlink in the table or the graph to view the [Filtered ATP Reports](#).

Web Server Usage

This Report displays a list of frequently accessed web servers according to the utilization of bandwidth, along with the number of hits per web server.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The report is displayed using a graph as well as in a tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The bar graph displays the list of web servers along with the number of hits while the tabular report contains the following information:

- Web Server: Displays name of the web server.
- Bandwidth: Bandwidth used per web server.
- Requests: Number of requests per web server.



Note: Click on a web server hyperlink from the graph or the table to view [Filtered Web Server Usage Reports](#).

Files Uploaded via FTP

The widget report displays number of hits and amount of data transferred per file uploaded via FTP by the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays amount of data transferred per file, while the tabular graph displays following information:

- File: Name of the file.
- File Count: Number of files uploaded.
- Bytes: Amount of data transferred through the file.



Note: Click on a file name to view the [Filtered FTP Usage Reports](#).

Files Downloaded via FTP

The widget report displays number of hits and amount of data transferred per file downloaded via FTP by the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays amount of data transferred per file, while the tabular graph displays following information:

- File: Name of the file.
- File Count: Number of files downloaded.
- Bytes: Amount of data transferred through the file.



Note: Click on a file name to view the [Filtered FTP Usage Reports](#).

Severity Level

The Widget displays information regarding severity level wise attacks attempted on the network.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed both, as a pie chart as well as in tabular format.

By default, the report is displayed for the current date. Select the date from the calendar button provided on top of the page.

The pie chart displays number of counts per severity level, while the tabular report contains following information:

- Severity Level: Severity level of the attack attempt. Predefined level are:
 - EMERGENCY - System is not usable.
 - ALERT - Action must be taken immediately.
 - CRITICAL - Critical condition.
 - ERROR - Error condition.
 - WARNING - Warning condition.
 - NOTICE - Normal but significant condition.
 - INFORMATION – Informational.
 - DEBUG - Debug - level messages.
- Attack: Name of the attack.
- Category: Name of the attack category, as defined in the Device. If the attack category is not defined in the Device then this field displays ‘Uncategorized’ which means the attack is uncategorized.
- Platform: Name of the attack platform, as defined in the Device.
- Target: Displays target type. Possible target types:
 - Client
 - Server
 - Client-Server
- Count: Number of counts of each severity level.

Web Viruses

The widget report displays number of hits per virus for the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per virus, while the tabular graph displays following information:

- Virus: Name of the virus as identified by the Device.
- Count: Number of virus occurrence.

User Data Transfer

The widget report displays total amount of data transfer and surfing time for the selected user.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Username**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays total amount of data transfer per user, while the tabular graph displays following information:

- User Name: Name of the user as defined in the Device.
- Data Transfer: Total amount of data transfer.
- Used Time: Total surfing time.



Note: Click user name hyperlink from the graph or the table to view the [Filtered User Data Transfer Reports](#).

Custom User Report by Source Host

The **Custom User Report by Source Host** dashboard provides a snapshot of traffic generated by the specified host.

To view the **Custom User Report by Source Host** dashboard:

- Go to **Monitor & Analyze > Reports > Custom > Custom User Report**.
- Select the criteria Source Host and specify it in the adjacent space provided.
- Click Go to view the customized dashboard.

The dashboard consists of the following reports in widget form:

- [Web Categories](#)
- [Files Uploaded via FTP](#)
- [Files Downloaded via FTP](#)
- [Blocked Web Categories](#)

Web Categories

The widget report displays number of hits and amount of data transferred per category for the selected host.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Source Host**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per category while the tabular graph displays following information:

- Category: Displays name of the category as defined in the Device. If the category is not defined in the Device, then this field will display 'uncategorized' instead of category name
- Hits: Number of hits to the category.
- Bytes: Amount of data transferred through the category, in bytes.



Note: Click on a web category to view the [Filtered Web Risks & Usage Reports](#).

Files Uploaded via FTP

The widget report displays number of hits and amount of data transferred per file uploaded via FTP by the selected host.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Source Host**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays amount of data transferred per file, while the tabular graph displays following information:

- File: Name of the file.
- File Count: Number of files uploaded.
- Bytes: Amount of data transferred through the file.



Note: Click on a file name to view the [Filtered FTP Usage Reports](#).

Files Downloaded via FTP

The widget report displays number of hits and amount of data transferred per file downloaded via FTP by the selected host.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Source Host**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays amount of data transferred per file, while the tabular graph displays following information:

- File: Name of the file.
- File Count: Number of files downloaded.
- Bytes: Amount of data transferred through the file.



Note: Click on a file name to view the [Filtered FTP Usage Reports](#).

Blocked Web Categories

The widget report displays the number of hits per blocked web category for the selected host.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Source Host**.

The Report is displayed as a graph as well as in a tabular format.

The bar graph displays number of hits per category while the tabular graph displays following information:

- Category: Displays name of the blocked web category as defined in the Device. If the category is not defined in the Device, then this field will display 'Uncategorized' instead of category name
- Hits: Number of hits to the category.



Note: Click on a category to view [Filtered Blocked Web Attempts Reports](#).

Custom User Report by Sender's Email Address

The **Custom User Report by Sender's Email Address** dashboard provides a snapshot of Email traffic generated by the specified Email Address.

To view the **Custom User Report by Sender's Email Address** dashboard:

- Go to **Monitor & Analyze > Reports > Custom > Custom User Report**.
- Select the criteria Sender's Email Address and specify it in the adjacent space provided.
- Click Go to view the customized dashboard.

The dashboard consists of the following reports in widget form:

- [Mail Recipients](#)
- [Mail Hosts](#)
- [Mail Destinations](#)
- [Mail Users](#)
- [Spam Recipients](#)
- [Mail Recipients](#)
- [Mail Hosts](#)
- [Mail Destinations](#)
- [Mail Users](#)
- [Spam Recipients](#)

Mail Recipients

The widget report displays the list of mail recipients along with number of hits and the amount of data transferred for the provided Sender's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the amount of data transferred per recipient, while the tabular report contains the following information:

- Recipient: Email Address of the recipient.
- Mail Count: Number of emails received.
- Bytes: Amount of data transferred.



Note: Click on a recipient to view [Report by Sender's Email Address and Recipient](#).

Report by Sender's Email Address and Recipient

The report displays amount of data transferred to the selected recipient(s) by the sender.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address > Recipient**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.

- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Host: IP Address of the host.
- Destination: IP Address of the destination.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Mail Hosts

The widget report displays list of mail sender hosts along with the number of hits and amount of data transferred per host.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the amount of data transferred per host, while the tabular report contains the following information:

- Source Host: IP Address of the host.
- Mail Count: Number of emails per host.
- Bytes: Amount of data transferred.



Note: Click on a host to view [Report by Sender's Email Address and Mail Host](#).

Report by Sender's Email Address and Mail Host

The report displays amount of data transferred from the selected host(s) by the sender.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address > Source Host**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Recipient: Email Address of the recipient.
- Destination: IP Address of the destination.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Mail Destinations

The widget report displays list of mail destinations along with the number of hits and amount of data transferred per destination, for the selected Sender's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the amount of data transferred per sender destination, while the tabular report contains the following information:

- Destination: IP Address or URL of the destination.
- Mail Count: Number of emails per destination..
- Mail Count: Number of emails per sender destination.
- Mail Count: Number of emails per destination..
- Bytes: Amount of data transferred.



Note: Click on a destination to view [Report by Sender's Email Address and Mail Destinations](#).

Report by Sender's Email Address and Mail Destinations

The report displays amount of data transferred to the selected destination(s) by the sender.

View the report from **> Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address > Destination**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user .
- Recipient: Email Address of the recipient.
- Host: IP Address of the host.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Mail Users

The widget report displays list of mail users along with the number of hits and amount of data transferred, for the provided Sender's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays amount data transferred per sender user, while tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined then it will display 'Unidentified', which means the traffic is generated by an unauthenticated user.
- Mail Count: Number of emails per user.
- Bytes: Amount of data transferred.



Note: Click on a user to view [Report by Sender's Email Address and Mail User](#).

Report by Sender's Email Address and Mail User

The report displays amount of data transferred by the selected user(s) and the sender.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address > User**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- Recipient: Email Address of the recipient.
- Host: IP Address of the host.
- Destination: IP Address of the destination.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Spam Recipients

The widget report displays the list of spam recipient(s) along with the number of hits per recipient, for the provided Sender's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per spam recipient, while tabular report contains following information:

- Recipient: Email Address of the spam recipient.
- Mail Count: Number of spam emails received.



Note: Click on a recipient to view [Report by Sender's Email Address and Recipient](#).

Report by Sender's Email Address and Recipient

The report displays amount of data transferred to the selected recipient(s) by the sender.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Sender's Email Address > Recipient**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Host: IP Address of the host.
- Destination: IP Address of the destination.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Custom User Report by Recipient's Email Address

The **Custom User Report by Recipient's Email Address** dashboard provides a snapshot of Email traffic generated by the specified Email Address.

To view the **Custom User Report by Recipient's Email Address** dashboard:

- Go to **Monitor & Analyze > Reports > Custom > Custom User Report**.
- Select the criteria Recipient's Email Address and specify it in the adjacent space provided.
- Click Go to view the customized dashboard.

The dashboard consists of the following reports in widget form:

- [Mails Senders](#)
- [Mail Hosts](#)
- [Mail Destinations](#)
- [Mail Users](#)
- [Spam Senders](#)

Mails Senders

The widget report displays the list of mail senders along with number of hits and the amount of data transferred for the provided Recipient's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the amount of data transferred per sender, while the tabular report contains the following information:

- Sender: Email Address of the sender.
- Mail Count: Number of emails sent.
- Bytes: Amount of data transferred.



Note: Click on a sender to view [Report by Recipient's Email Address and Sender](#).

Report by Recipient's Email Address and Spam Sender

The report displays amount of data transferred by the selected sender and recipient.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address > Sender**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Host: IP Address of the host.
- Destination: IP Address of the destination.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Mail Hosts

The widget report displays list of mail recipient hosts along with the number of hits and amount of data transferred per host, for the provided Recipient's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the amount of data transferred per source host, while the tabular report contains the following information:

- Source Host: IP Address of the source host.
- Mail Count: Number of emails per host.
- Bytes: Amount of data transferred.



Note: Click on a host to view [Report by Recipient's Email Address and Mail Host](#).

Report by Recipient's Email Address and Mail Host

The report displays amount of data transferred by the selected host and recipient.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address > Host**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Recipient: Email Address of the recipient.
- Destination: IP Address of the destination.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Mail Destinations

The widget report displays list of mail destinations along with the number of hits and amount of data transferred per destination, for the provided Recipient's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address**.

The report is displayed as a graph as well as in a tabular format.

The bar graph displays the amount of data transferred per recipient destination, while the tabular report contains the following information:

- Destination: IP Address or URL of the destination.
- Mail Count: Number of emails per destination.
- Bytes: Amount of data transferred.



Note: Click on a destination to view [Report by Recipient's Email Address and Recipient Destination](#).

Report by Recipient's Email Address and Mail Destination

The report displays amount of data transferred by the selected destination(s) and the recipient.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address > Destination**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Sender: Email Address of the sender.
- Host: IP Address of the host.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Mail Users

The widget report displays list of mail recipient users along with the number of hits and amount of data transferred, for the provided Recipient's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays amount data transferred per recipient user, while tabular report contains following information:

- User: Username of the user as defined in the Device. If the User is not defined then it will display 'Unidentified', which means the traffic is generated by an unauthenticated user.
- Mail Count: Number of emails per user.
- Bytes: Amount of data transferred.



Note: Click on a user to view [Report by Recipient's Email Address and Mail User](#).

Report by Recipient's Email Address and Mail User

The report displays amount of data transferred by the selected user(s) and the recipient.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address > User**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Sender: Email Address of the sender.
- Subject : Subject line of the Email.

- User: Username of the sender as defined in the Device. If the User is not defined, then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Host: IP Address of the host.
- Destination: IP Address of the destination.
- Application/Proto:Port: Name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Spam Senders

The widget report displays the list of spam senders along with the number of hits per sender, for the provided Recipient's Email ID.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address**.

The report is displayed as a graph as well as in a tabular format.

Bar graph displays number of hits per spam sender, while tabular report contains following information:

- Sender: Email Address of the spam sender.
- Mail Count: Number of spam emails sent.



Note: Click on a sender to view [Report by Recipient's Email Address and Spam Sender](#).

Report by Recipient's Email Address and Spam Sender

The report displays amount of data transferred by the selected sender and recipient.

View the report from **Monitor & Analyze > Reports > Custom > Custom User Report > Recipient's Email Address > Sender**.

The bar graph displays amount of data transferred through each Email, while the tabular report contains the following information:

- Time: Date and Time in YYYY:MM:DD HH:MM:SS format.
- Subject : Subject line of the Email.
- User: Username of the sender as defined in the Device. If the User is not defined then it will display 'Unidentified' which means the traffic is generated by an unauthenticated user.
- Host: IP Address of the host.
- Destination: IP Address of the destination.
- Application/Proto:Port: Displays name of the application as defined in the Device. If the application is not defined, then this field will display the application identifier as a combination of protocol and port number.
- Size: Size of the Email.

Custom Web Server Report

Use the **Monitor & Analyze > Reports > Custom > Custom Web Server Report** to view Custom Web Server Report by performing a search in the Web Server Reports.

1. Go to **Monitor & Analyze > Reports > Custom > Custom Web Server Report**.
2. Select the 'Search Type' value. Possible values are:
 - Web Server Usage
 - Web Server Protection
3. Select the 'Search For' value: Possible values are:
 - User
 - Web Server
 - Domain
 - Source IP
 - Attack

- Attacker
- 4. Specify User Name / Web Server / Virus name values based on the selected 'Search For' value. If the value is not specified, then search result will be displayed for all the Users / Web Servers / Viruses.
- 5. Click Search.

Given below is the available Custom Web Server Report:

- [Web Server Usage Report](#)
- [Web Server Protection Report](#)

WAF Server Usage Report

This Report displays detailed usage of web servers hosted in your network.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Server Report**.
2. Select the 'Search Type' value: Web Server Usage.
3. Select the 'Search For' value: Possible values are:
 - User
 - Web Server
 - Domain
 - Source IP

The Tabular report contains the following information:

- Time: Time of web server usage activity, in YYYY-MM-DD HH:MM:SS format.
- Web Server: Name of the web server.
- User: Username of the user as defined in the Device.
- Source IP: IP Address from which access request to your web server was done.
- Local IP: Local IP Address.
- Virus: Name of the virus.
- URL: Name of the accessed URL.
- User Agent: Name of the browser and platform used to access the web server.
- HTTP Request: Displays first line of HTTP request.
- Domain: Dpmain request header data.
- Query String: Displays query string.
- HTTP Method: Name of HTTP request method.
- HTTP Status: HTTP status code returned to the client.

WAF Server Protection Report

This Report displays details of virus and attacks performed on the web servers hosted in your network.

1. To view the report, go to **Monitor & Analyze > Reports > Custom > Custom Web Server Report**.
2. Select the 'Search Type' value: Web Server Protection.
3. Select the 'Search For' value: Possible values are:
 - Web Server
 - Domain
 - Attack
 - Attacker

The Tabular report contains the following information:

- Time: Time of web server usage activity, in YYYY-MM-DD HH:MM:SS format.
- Web Server: Name of the web server.
- User: Username of the user as defined in the Device.
- Source IP: IP Address from which access request to your web server was done.
- Local IP: Local IP Address.
- Attack: Name of the attack.

- Virus / Attack Info: Name of the virus or information about the intrusion attack.
- URL: Name of the accessed URL.
- User Agent: Name of the browser and platform used to access the web server.
- HTTP Request: Displays first line of HTTP request.
- HTTP Host: HTTP Host request header data.
- Query String: Displays query string.
- HTTP Method: Name of HTTP request method.
- HTTP Status: HTTP status code returned to the client.

Settings

Settings section provides a number of configuration options to customize and use Reports.

This section describes management of application groups, custom views, report notifications and database.



Note: This page only displayed when Show Configuration is selected.

This section includes the following topics:

- [Custom View](#) – Create and manage customized view of reports.
- [Report Scheduling](#) – Send reports in HTML format to configured Email address(s).
- [Data Management](#) – Manage disk space and data required to generate reports.
- [Manual Purge](#) – Allows removing logs manually.
- [Bookmark Management](#) – Create and manage report and report group bookmarks.
- [ConnectWise](#) – Integrate Reports with ConnectWise PSA.
- [Custom Logo](#) – Configure a custom logo for reports.

Custom View

Custom view of reports allows grouping of the most pertinent reports that requires the special attention for managing the device. Reports from different report groups can also be grouped in a single view. In a view, maximum 8 reports can be grouped.

Custom view provides a single page view of all the grouped reports.

Use **Monitor & Analyze > Reports > Settings > Custom View** to create and manage custom views.

Custom View Name

Name of custom view.

Custom View Description

Description of the custom view.

Add Button

Click to add a new custom view.

Delete Button

Click to delete custom view(s).

Use this page to:

- [Add Custom View](#)
- [Edit Custom View](#)
- Delete Custom View(s).

Add Custom View

Create a new Custom View.



Note: Added Custom Views will be displayed under Custom Views sub-menu of navigation pane.

1. Go to **Monitor & Analyze > Reports > Settings > Custom View**.
2. Click **Add** to create a new Custom View.
3. Specify Custom View Name. Custom view name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
4. Specify description of the Custom View, if required.
5. Expand Report Groups and select the reports to be added in custom view. Maximum 8 reports can be added per custom view.
6. Click **Save** to add selected reports in the Custom View.

Custom View: (Special Characters "|", " ", "\" are not allowed)

Custom View Description : (Special Character "\" is not allowed)

Report Groups (You can select upto 8 reports.)

- ▶ User App Risks & Usage
- ▶ Blocked User Apps
- ▶ Web Risks & Usage
- ▶ Blocked Web Attempts
- ▶ Search Engine
- ▶ Web Server Usage
- ▶ Web Server Protection
- ▶ User Data Transfer Report
- ▶ FTP Usage
- ▶ FTP Protection
- ▶ Intrusion Attacks
- ▶ Advanced Threat Protection
- ▶ VPN
- ▶ SSL VPN
- ▶ Clientless Access
- ▶ Wireless
- ▶ Security Heartbeat
- ▶ Email Usage
- ▶ Email Protection
- ▶ Events

Figure 302: Add Custom View

Report Scheduling

Sophos Firewall can send various reports except ConnectWise reports to specified Email address(es) as per the configured frequency. The scheduled reports will be sent in PDF format.



Note: The PDF attachment contains details of report schedules and displays reports in in-line graph format.

Use the **Monitor & Analyze > Reports > Settings > Report Scheduling** page to create and manage report schedules.

Screen Components

Add Button

Click to add a new report schedule.

Update Report Schedule

Click existing report schedule to update it.

Delete Button

Click to delete a report schedule.

Send Test Mail

Click to send a test Email on configured Email address.

Report Scheduling**Name**

Name of the report schedule.

Report Group/Bookmark

Category of reports.

Email Frequency

Report Schedule frequency- daily or weekly.

To Email Address

Comma separated email addresses of the recipients.

Last Sent Time

Last time when the report schedule was sent, in YYYY-MM-DD HH:MM:SS format.

Security Audit Report**Name**

Name of the report schedule.

Organization Name

Name of the organization.

Email Frequency

Report schedule frequency.

To Email Address

Comma separated email addresses of the recipients.

Last Sent Time

Last time when the report schedule was sent.

Generate Now

Click **Generate Now** to generate the report in PDF format, which will be sent as an attachment to the configured Email address. The button is available for Cyberoam Models CR100iNG and above.

Connectwise Schedule**Name**

Name of the report schedule.

Report

Name of the report to be sent.

Frequency

Report schedule frequency with time of the day.

Number of Record(s)

Number of records to be sent in report schedule.

Last Sent Time

Last time when the report schedule was sent.

Add Report Schedule

Create a new Report Schedule for one or more reports, Security Audit Report or ConnectWise reports.

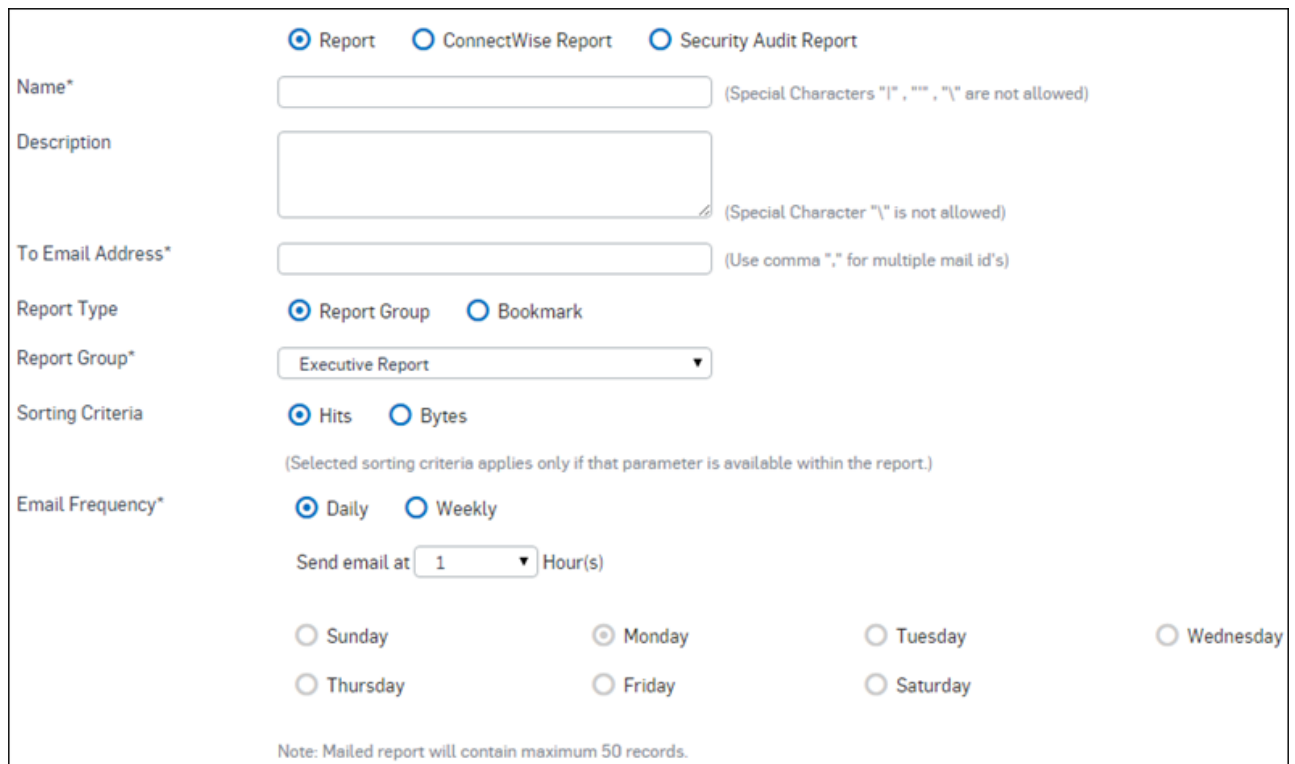
1. Go to **Monitor & Analyze > Reports > Settings > Report Scheduling**.
2. Click **Add** to create a new report schedule.



Note:

- ConnectWise Report schedule can only be sent when ConnectWise option is enabled from **Reports > Settings > ConnectWise**. If ConnectWise option is disabled, report schedule option for ConnectWise will remain greyed.
 - Report schedule for ConnectWise reports can not be deleted after disabling ConnectWise.
3. Select reports to be sent.
 - Report:
 - Specify report schedule name. Name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
 - Specify description of the report schedule, if required.
 - Specify Email address of the recipient in ‘To Email Address’ field. Use comma, with no space in between, to specify multiple Email IDs.
 - Select report type. Possible types of reports are Report Group and Bookmark.
 - Select sorting criteria from the Sorting Criteria field. Possible options are Hits and Bytes.
 - Select report category from the Report Group or Bookmark drop down list. Reports from selected category will be sent to the recipients.
 - Set Email frequency and time. Reports can be mailed daily or weekly. For daily notification select time of the day to send the report. For weekly notification, select day of the week and time of the day to send the report.
 - Security Audit Report:
 - Specify report schedule name. Name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
 - Specify name of the Organization.
 - Specify Email address of the recipient in ‘To Email Address’ field. Use comma, with no space in between, to specify multiple Email IDs.
 - Set Email frequency and time. Reports can be mailed daily or weekly. For daily notification select time of the day to send the report. For weekly notification, select day of the week and time of the day to send the report.
 - ConnectWise:
 - Specify report schedule name. Name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
 - Specify description of the report schedule, if required.
 - Select reports to be sent. Available reports are Top Sites, Filtered Sites, Bandwidth Usage and Top Attacks.
 - Specify number of records to be sent in the report schedule. You can send maximum of 50 records in a report schedule.

Reports can be sent daily. Select time of the day to send the report.



☒ Report ☐ ConnectWise Report ☐ Security Audit Report

Name* (Special Characters "!", " ", "\" are not allowed)

Description (Special Character "\" is not allowed)

To Email Address* (Use comma "," for multiple mail id's)

Report Type ☒ Report Group ☐ Bookmark

Report Group*

Sorting Criteria ☒ Hits ☐ Bytes
 (Selected sorting criteria applies only if that parameter is available within the report.)

Email Frequency* ☒ Daily ☐ Weekly

Send email at Hour(s)

☐ Sunday ☒ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☐ Friday ☐ Saturday

Note: Mailed report will contain maximum 50 records.

Figure 303: Add Report Schedule

4. Click **Save** to save changes.

Send Test Mail

Send a test Email to verify the Email Server configuration and report notification configuration.

1. Go to **Monitor & Analyze > Reports > Settings > Report Scheduling**.
2. Click **Send Test Mail** and specify the Email Address of the recipient.
3. Click **Send** to send a test mail to the specified Email Address.

Data Management

This section describes how to configure Log Retention Period.

Retention of data and log archives use enormous amount of disk space. To control and optimize the disk space usage, configure the data retention period of detailed and summarized table. Depending on the compliance requirement, configure the log retention period.

Use **Monitor & Analyze > Reports > Settings > Data Management** to configure retention period of various data tables. You can configure retention period for various log types.



Note: Based on configured retention period, log data will be deleted on day-by-day basis.

User App Risks & Usage Logs:

User App Risks & Usage logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

Blocked User Apps Logs:

Blocked User Apps logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

Web Risk & Usage Logs:

Web Risk & Usage logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

Blocked Web Attempts Logs:

Blocked Web Attempts logs can be retained for time interval starting from 1 month to 3 months.

Default - 3 months.

Web Server Usage & Protection Logs:

Web Server Usage & Protection logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

User Data Transfer Report Logs:

User Data Transfer Report logs can be retained for time interval starting from 1 month to 1 year.

Default - 3 months.

FTP Usage Logs:

FTP Usage logs can be retained for time interval starting from 1 month to 3 months.

Default - 3 months.

Intrusion Attacks Logs:

Intrusion Attacks logs can be retained for time interval starting from 1 month to 3 months.

Default - 3 months.

Advanced Threat Protection Logs:

Advanced Threat Protection logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

VPN, SSL VPN & Clientless Access Logs:

VPN, SSL VPN & Clientless Access logs can be retained for time interval starting from 1 month to 1 year.

Default - 1 month.

RED Logs:

RED logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

Wireless Logs:

Wireless logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

Security Heartbeat Logs:

Security Heartbeat logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

Email Usage Logs:

Email Usage logs can be retained for time interval starting from 1 month to 3 months.

Default - 3 months.

Email Protection Logs:

Email Protection logs can be retained for time interval starting from 1 month to 3 months.

Default - 3 months.

Web, FTP & Email Virus Logs:

Web, FTP & Email Virus logs can be retained for time interval starting from 1 month to 3 months.

Default - 3 months.

Events Logs:

Events logs can be retained for time interval starting from 1 month to 1 year.

Default - 1 month.

User Threat Quotient (UTQ) Logs:

User Threat Quotient (UTQ) logs can be retained for time interval starting from 1 month to 1 year.

Default - 6 months.

Log Retention

Displays type of logs to be retained.

Report Period

Displays retention period for summary reports.

Export Customization

Enable Selection of reports and number of records per report (MS Excel) to enable selection of reports and number of records per report while exporting reports in MS-Excel format.

Apply Button

Click to apply changes. Changes in the retention period will be applied at 12:00 O' clock in the night.

Log Retention Report Period

Retain User App Risks & Usage Logs for last	6 Month ▼
Retain Blocked User Apps Logs for last	6 Month ▼
Retain Web Risk & Usage Logs for last	6 Month ▼
Retain Blocked Web Attempts Logs for last	3 Month ▼
Retain Web Server Usage & Protection Logs for last	6 Month ▼
Retain User Data Transfer Report Logs for last	3 Month ▼
Retain FTP Usage Logs for last	3 Month ▼
Retain Intrusion Attacks Logs for last	3 Month ▼
Retain Advanced Threat Protection Logs for last	6 Month ▼
Retain VPN, SSLVPN & Clientless Access Logs for last	1 Month ▼
Retain RED Logs for last	6 Month ▼
Retain Wireless Logs for last	6 Month ▼
Retain Security Heartbeat Logs for last	6 Month ▼
Retain Email Usage Logs for last	3 Month ▼
Retain Email Protection Logs for last	3 Month ▼
Retain Web, FTP & Email Virus Logs for last	3 Month ▼
Retain Events Logs for last	1 Month ▼
Retain User Threat Quotient (UTQ) Logs for last	6 Month ▼

Export Customization

Selection of reports and number of records per report (MS Excel)

Enable ▼

Figure 304: Data Management

Manual Purge

Retention of data and log archives use enormous amount of disk space. You can configure the log retention period from Data Management page. Based on the configured retention period data will be automatically deleted on day-by-day basis.

Use **Monitor & Analyze > Reports > Settings > Manual Purge** page to delete logs manually.

Report Module

Select Reports to be purged.

Available Options:

- All Reports
- User App Risks & Usage
- Blocked User Apps
- Web Risks & Usage
- Blocked Web Attempts
- Web Server Usage & Protection
- User Data Transfer Report
- FTP Usage
- Intrusion Attacks
- Advanced Threat Protection
- VPN, SSL VPN & Clientless Access
- RED
- Wireless
- Security Heartbeat
- Email Usage
- Email Protection
- Web, FTP & Email Virus
- Events
- User Threat Quotient (UTQ)

Criteria

Select Custom Duration to purge selected reports for specified period or Purge All to purge all the reports.

From

Select month and year, from which the reports have to be purged.

Up To

Select month and year, up to which the reports have to be purged.

Purge Button

Click to purge the reports manually.

Report Module	<div>All Reports ▼</div>	
Criteria	<input checked="" type="radio"/> Custom Duration <input type="radio"/> Purge All	
From	<div>Oct ▼</div>	<div>2015 ▼</div>
Up To	<div>Oct ▼</div>	<div>2015 ▼</div>

Figure 305: Manual Purge

Bookmark Management

Bookmark management allows the user to create bookmark of any report at any level of report drill-down. It provides administrator with great level of network visibility based on any criterion.

For example, the administrator can monitor web usage of a particular user by creating bookmark of user based web usage report.

Every bookmark should be a part of a defined bookmark group; if the bookmark group is not created then bookmarks will be members of the Default group.

Every bookmark can be sent to specified Email Address(s) in the form of report notification. Use **Monitor & Analyze > Reports > Settings > Bookmark Management** to create bookmark groups.

Bookmark Groups

Name of the bookmark group.

Add Button

Click to add a new bookmark group.

Delete Icon

Click to delete a bookmark group.

Use this page to:

- [Add Bookmark Group](#)
- Delete Bookmark Group

Add Bookmark Group

Create a new Bookmark Group.

1. Go to **Reports > Settings > Bookmark Management**.
2. Click **Add Bookmark Group** to create a new Bookmark Group.
3. Specify Bookmark Group Name, name can be any combination of alphanumeric characters and special characters “_”, “@” and “.”.
4. Click **Save**.

The newly created bookmark group will be displayed under **Reports > Bookmarks** as well as under **Reports > Settings > Bookmark Management**.

Add Bookmark

Bookmark a report.

1. Access any report and Click **Bookmark** to create a new Bookmark for the report.
2. Specify Bookmark Name. Note that special characters like "|", "'", "\" are not allowed
3. Provide a description, if required.
4. Choose the Bookmrk Group under which the report is to be bookmarked. Note that every bookmark has to have a bookmark group.
5. Click **Save** to bookmark the report under the specified bookmark group.

Integration with ConnectWise

This page allows the administrator to integrate ConnectWise PSA with Reports. The integration allows use of Reports database to generate ConnectWise reports.

1. Go to **Monitor & Analyze > Reports > Settings > ConnectWise**.
2. Enable ConnectWise option to send Device report data to ConnectWise server.
3. Specify Company ID configured in ConnectWise server to identify your company.
4. Specify URL for ConnectWise server. Report data from Device will be sent to specified URL.
5. Specify Integrator's credentials (Username and Password) created in ConnectWise to send report data from the Device to ConnectWise server.
6. Specify Device name. By default, the Device displays Device key in Device name field.
7. Specify Manage ID configured in ConnectWise to link management solution with your company.
8. Specify name of Management Solution configured in ConnectWise to link management solution with your company.
9. Click **Apply** to apply ConnectWise settings.

Given below is the list of reports which can be sent to ConnectWise along with respective ConnectWise report name.

- Top Sites
- Filtered Sites

- Bandwidth Usage
- Top Attacks



Note: If there is no report notification configured for ConnectWise, the Device will create report notification for all four reports automatically as soon as ConnectWise configuration is applied. But if there exists a report notification for ConnectWise, the administrator will need to create rest of the report notifications manually.

☒ Enable ConnectWise

Company ID*

URL*

Integrator Login*

Integrator Password*

Appliance Key*

Manage ID*

Management Solution*

Figure 306: ConnectWise

Custom Logo

This page allows the administrator to configure a custom logo for HTML reports. The administrator can choose to use a custom logo for all the reports which are to be exported in HTML format.

To configure custom logo for the reports, go to **Monitor & Analyze > Reports > Settings > Custom Logo**.

Logo Settings

Available Options:

- Default - Sophos' Logo
- Custom - Select to upload an image file to be used as logo

Upload File

Browse image file to be used as report logo. The image file size should not exceed 50kb.

Apply

Click to save changes.