ManageEngine

Firewall Analyzer

Non-intrusive & Real-time Monitoring of Corporate Users Internet Activity using Firewall Analyzer

Solution Brief

Non-intrusive & Real-time Monitoring of Corporate Users Internet Activity using Firewall Analyzer

Like unrestricted privileges to administrative users in a network (PUMA), uncontrolled web access in companies has its own set of problems. Irresponsible Internet usage tends to reduce employee productivity increases security risks, and the prime bandwidth necessary for business consumption becomes scarce.

The Social Enterprise

In this era of cloud computing and social media, access to Internet for business usage is the order of the day. Companies make use of social tools like Facebook, Twitter, LinkedIn to stay in touch with their customers, to quickly market their products, to stay informed about best practices, etc. But then, surveys by various agencies indicate that YouTube alone drains 10% of the business bandwidth usage, another 5% by Facebook. There is no dispute that Internet usage has to be streamlined and effectively monitored to ensure that it is responsibly used.

It is a fine balancing act. Take full advantage of the facilities of the Internet and at the same time, prevent over use and avoid security risk. So, what do we do now?

Non-intrusive & Real-time Monitoring

There is a fine line between being Big Brother and keeping employees from misusing corporate Internet access, and this is where an non-intrusive, real-time Internet user activity monitoring solution like ManageEngine Firewall Analyzer comes to your rescue. Firewall Analyzer is a log analytics and configuration management software for network security devices. It monitors corporate bandwidth usage in real-time, tracks web sites visited, provides protocol-wise & application-wise bandwidth consumption. It captures all network security events and notifies about the security situation. It audits the configuration and security of the perimeter device to assess the security of the device itself.

Customer Voice:

This is what one of our customer had to say about using Firewall Analyzer to monitor employee Internet usage and how they prevent large file downloads

Monitoring Corporate Users' Internet Activity using Firewall Analyzer

With Firewall Analyzer you can use any of three following use cases to monitor your employees Internet usage:

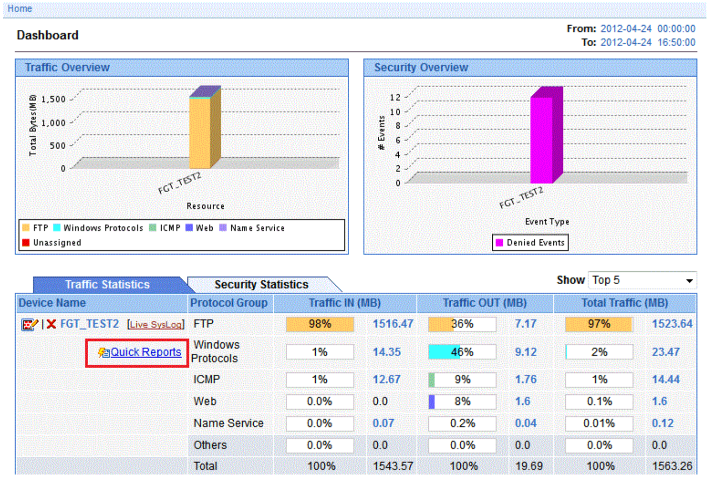
1. Quick Reports from Dashboard
2. Reports using Advanced Search
3. User-specific Custom Reports

Use Case 1: Quick Reports from Dashboard

Get a quick view of top Internet users in your network with a few clicks from the Dashboard

Step 1:

Click the Quick Reports link of the Firewall device in the **Traffic Statistics** tab

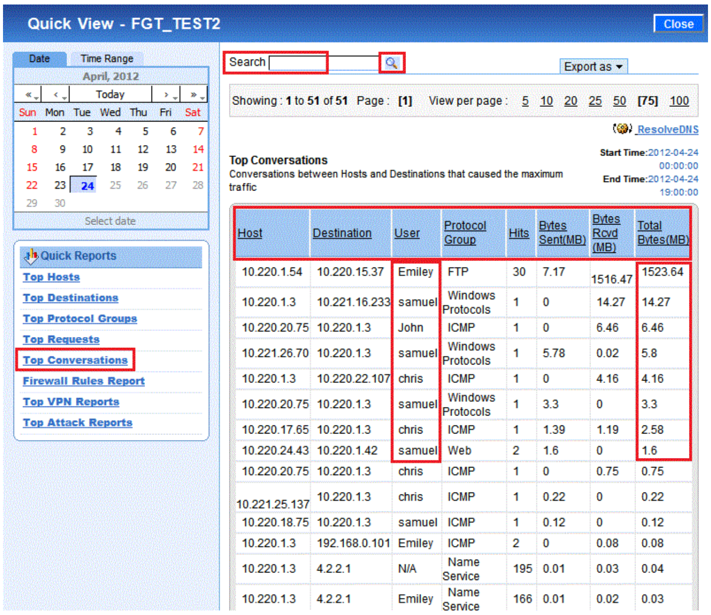


From: 2012-04-24 00:00:00
To: 2012-04-24 16:50:00

Device Name	Protocol Group	Traffic IN (MB)		Traffic OUT (MB)		Total Traffic (MB)	
FGT_TEST2 [Live SysLog]	FTP	98%	1516.47	36%	7.17	97%	1523.64
Quick Reports	Windows Protocols	1%	14.35	46%	9.12	2%	23.47
	ICMP	1%	12.67	9%	1.76	1%	14.44
	Web	0.0%	0.0	8%	1.6	0.1%	1.6
	Name Service	0.0%	0.07	0.2%	0.04	0.01%	0.12
	Others	0.0%	0.0	0.0%	0.0	0.0%	0.0
	Total	100%	1543.57	100%	19.69	100%	1563.26

Step 2:

Click the Top Conversation link in the left side. You will see a list of corporate users along with details on total bytes consumed, host/source, destination, protocol groups, hits, bytes sent, and bytes received.



Showing : **1** to **51** of **51** Page : **[1]** View per page : 5 10 20 25 50 **[75]** 100

Top Conversations
Conversations between Hosts and Destinations that caused the maximum traffic

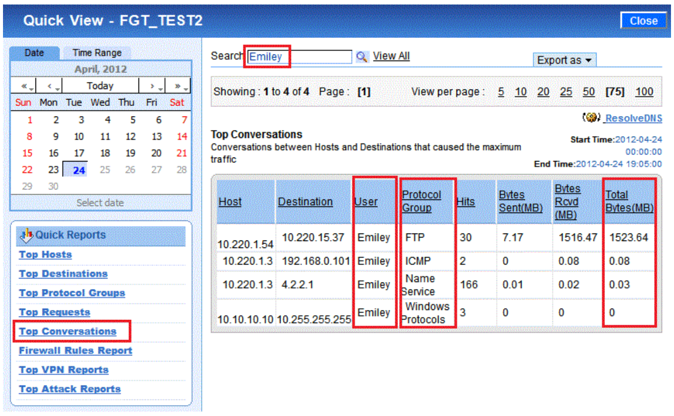
Start Time:2012-04-24 00:00:00
End Time:2012-04-24 19:00:00

Host	Destination	User	Protocol Group	Hits	Bytes Sent(MB)	Bytes Rcvd (MB)	Total Bytes(MB)
10.220.1.54	10.220.15.37	Emiley	FTP	30	7.17	1516.47	1523.64
10.220.1.3	10.221.16.233	samuel	Windows Protocols	1	0	14.27	14.27
10.220.20.75	10.220.1.3	John	ICMP	1	0	6.46	6.46
10.221.26.70	10.220.1.3	samuel	Windows Protocols	1	5.78	0.02	5.8
10.220.1.3	10.220.22.107	chris	ICMP	1	0	4.16	4.16
10.220.20.75	10.220.1.3	samuel	Windows Protocols	1	3.3	0	3.3
10.220.17.65	10.220.1.3	chris	ICMP	1	1.39	1.19	2.58
10.220.24.43	10.220.1.42	samuel	Web	2	1.6	0	1.6
10.220.20.75	10.220.1.3	chris	ICMP	1	0	0.75	0.75
10.221.25.137	10.220.1.3	chris	ICMP	1	0.22	0	0.22
10.220.18.75	10.220.1.3	samuel	ICMP	1	0.12	0	0.12
10.220.1.3	192.168.0.101	Emiley	ICMP	2	0	0.08	0.08
10.220.1.3	4.2.2.1	N/A	Name Service	195	0.01	0.03	0.04
10.220.1.3	4.2.2.1	Emiley	Name Service	166	0.01	0.02	0.03

Step 3:

To view Internet activity for a particular user, enter the user name in the Search field see at the top of the screen, and click the search icon. You will get the report filtered for the selected user.

Note: Click **Resolve DNS** to obtain the domain names for the host & destination IPs



Search Emiley

Showing : **1** to **4** of **4** Page : **[1]** View per page : 5 10 20 25 50 **[75]** 100

Top Conversations
Conversations between Hosts and Destinations that caused the maximum traffic

Start Time:2012-04-24 00:00:00
End Time:2012-04-24 19:05:00

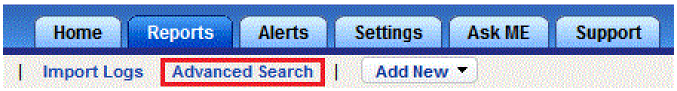
Host	Destination	User	Protocol Group	Hits	Bytes Sent(MB)	Bytes Rcvd (MB)	Total Bytes(MB)
10.220.1.54	10.220.15.37	Emiley	FTP	30	7.17	1516.47	1523.64
10.220.1.3	192.168.0.101	Emiley	ICMP	2	0	0.08	0.08
10.220.1.3	4.2.2.1	Emiley	Name Service	166	0.01	0.02	0.03
10.10.10.10	10.255.255.255	Emiley	Windows Protocols	3	0	0	0

Use Case 2: Advanced Search

Get the corporate users' internet activity reports faster. View of top Internet users in your network with advanced search and save it as a report

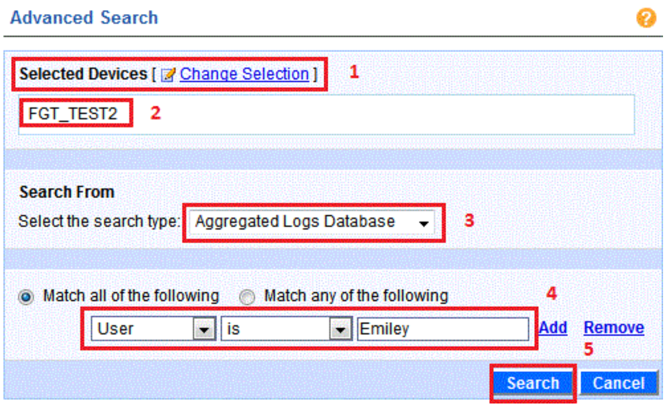
Step 1:

Click the **Advanced Search** link in the **Sub tab.** The **Advanced Search** screen opens up.



Step 2:

In the **Advanced Search** screen, select a particular device for log search. Select **Aggregated Logs Database** in the *Select From* field. In the criteria, select **Match all of the following** option. Select **User, is, Emiley** in the criteria fields. Click **Search** button.



Selected Devices [Change Selection]

FGT_TEST2

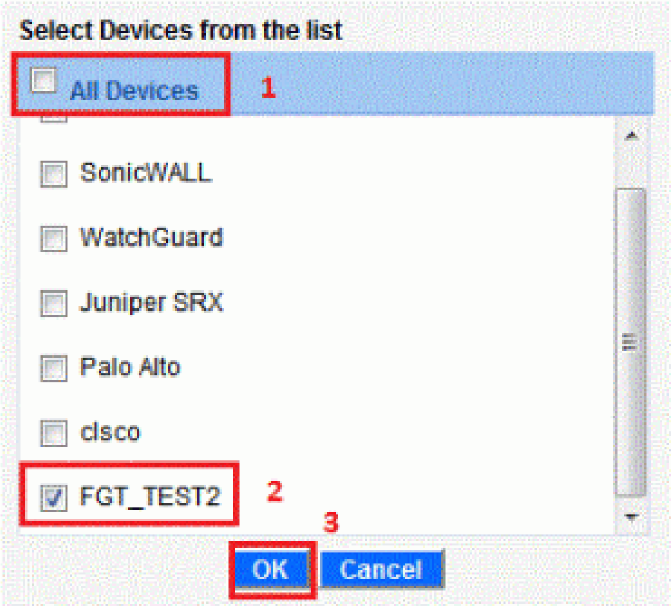
Search From

Select the search type: Aggregated Logs Database

● Match all of the following ○ Match any of the following

User | is | Emiley

Select devices from the device list.



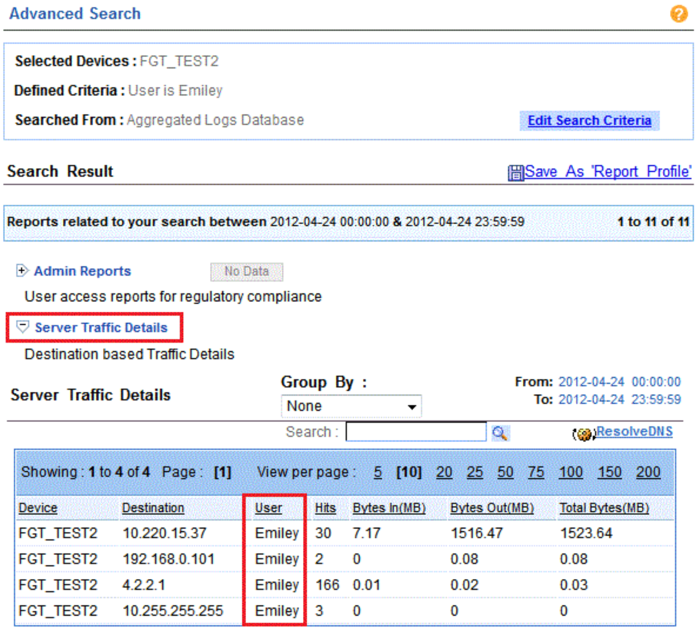
Select Devices from the list

- ☐ All Devices 1
- ☐ SonicWALL
- ☐ WatchGuard
- ☐ Juniper SRX
- ☐ Palo Alto
- ☐ cisco
- ☑ FGT_TEST2 2

3 OK Cancel

Step 3:

The search results will be displayed. Now, select the **Server Traffic Details** result. You will see the details of device, destination, hits, bytes sent, bytes received and total bytes consumed, for corporate user **Emiley**.



Advanced Search

Selected Devices : FGT_TEST2
Defined Criteria : User is Emiley
Searched From : Aggregated Logs Database

Edit Search Criteria

Search Result Save As 'Report Profile'

Reports related to your search between 2012-04-24 00:00:00 & 2012-04-24 23:59:59 **1 to 11 of 11**

Admin Reports No Data
User access reports for regulatory compliance

Server Traffic Details
Destination based Traffic Details

Server Traffic Details **Group By :** None **From:** 2012-04-24 00:00:00 **To:** 2012-04-24 23:59:59

Search : ResolveDNS

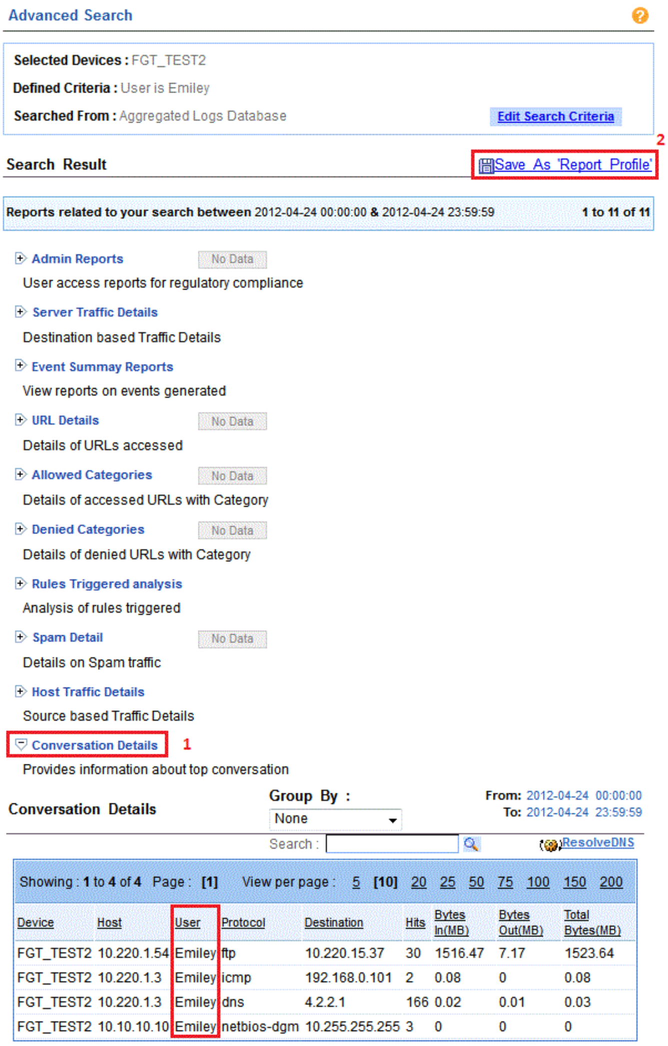
Showing : **1** to **4** of **4** Page : **[1]** View per page : 5 **[10]** 20 25 50 75 100 150 200

Device	Destination	User	Hits	Bytes In(MB)	Bytes Out(MB)	Total Bytes(MB)
FGT_TEST2	10.220.15.37	Emiley	30	7.17	1516.47	1523.64
FGT_TEST2	192.168.0.101	Emiley	2	0	0.08	0.08
FGT_TEST2	4.2.2.1	Emiley	166	0.01	0.02	0.03
FGT_TEST2	10.255.255.255	Emiley	3	0	0	0

Step 4:

Next, select the **Conversation Details** of the result. You will see the details of device, host, protocol, destination, hits, bytes sent, bytes received and total bytes consumed, for corporate user **Emiley**.

After this, if you want to save the search result as Report Profile, click the **Save As 'Report Profile'** link on the right top corner of the results page.



Advanced Search

Selected Devices : FGT_TEST2
Defined Criteria : User is Emiley
Searched From : Aggregated Logs Database

Edit Search Criteria

Search Result 2 Save As 'Report Profile'

Reports related to your search between 2012-04-24 00:00:00 & 2012-04-24 23:59:59 **1 to 11 of 11**

Admin Reports No Data
User access reports for regulatory compliance

Server Traffic Details
Destination based Traffic Details

Event Summay Reports
View reports on events generated

URL Details No Data
Details of URLs accessed

Allowed Categories No Data
Details of accessed URLs with Category

Denied Categories No Data
Details of denied URLs with Category

Rules Triggered analysis
Analysis of rules triggered

Spam Detail No Data
Details on Spam traffic

Host Traffic Details
Source based Traffic Details

Conversation Details 1
Provides information about top conversation

Conversation Details **Group By :** None **From:** 2012-04-24 00:00:00 **To:** 2012-04-24 23:59:59

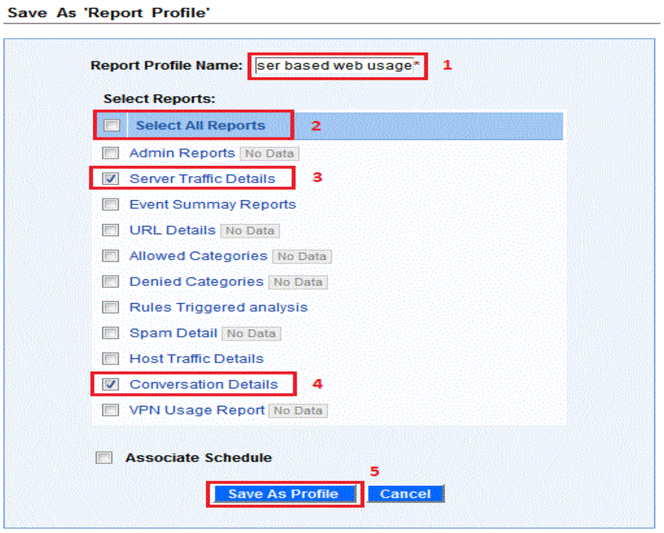
Search : ResolveDNS

Showing : **1** to **4** of **4** Page : **[1]** View per page : 5 **[10]** 20 25 50 75 100 150 200

Device	Host	User	Protocol	Destination	Hits	Bytes In(MB)	Bytes Out(MB)	Total Bytes(MB)
FGT_TEST2	10.220.1.54	Emiley	ftp	10.220.15.37	30	1516.47	7.17	1523.64
FGT_TEST2	10.220.1.3	Emiley	icmp	192.168.0.101	2	0.08	0	0.08
FGT_TEST2	10.220.1.3	Emiley	dns	4.2.2.1	166	0.02	0.01	0.03
FGT_TEST2	10.10.10.10	Emiley	netbios-dgm	10.255.255.255	3	0	0	0

Step 5:

The **Save As 'Report Profile'** page opens up. In that, enter the report profile name. Select the **Server Traffic Details** and Conversation Details reports using check boxes. Optionally, associate a schedule like any other custom report. You can also schedule automatic generation at a later point in time. Click **Save As Profile** button.



Save As 'Report Profile'

Report Profile Name: ser based web usage 1

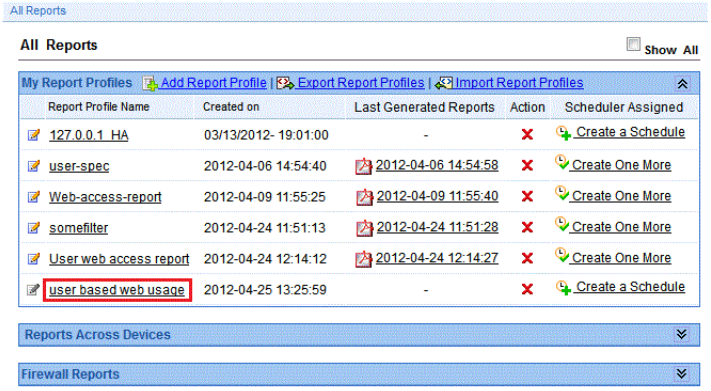
Select Reports:

- ☐ Select All Reports 2
- ☐ Admin Reports No Data
- ☑ Server Traffic Details 3
- ☐ Event Summay Reports
- ☐ URL Details No Data
- ☐ Allowed Categories No Data
- ☐ Denied Categories No Data
- ☐ Rules Triggered analysis
- ☐ Spam Detail No Data
- ☐ Host Traffic Details
- ☑ Conversation Details 4
- ☐ VPN Usage Report No Data

☐ **Associate Schedule**

5 Save As Profile Cancel

Now the report profile **user based web usage** gets saved under my reports. Click on the report profile and view the report (both Server Traffic and Conversation) for user **Emiley**.



All Reports

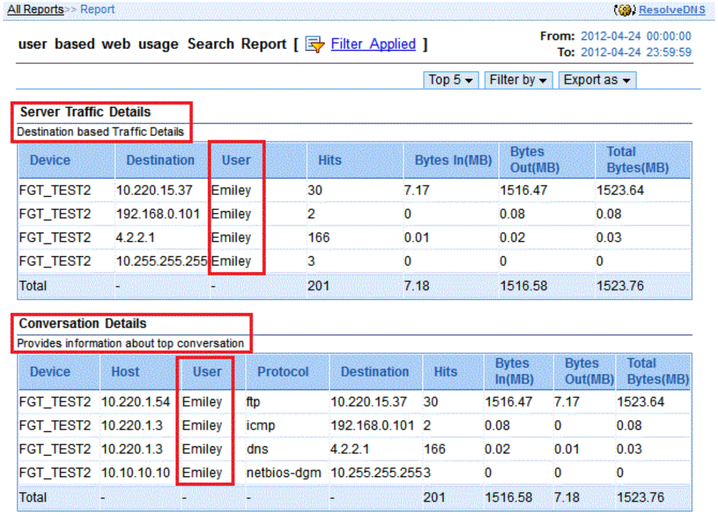
All Reports □ Show All

My Report Profiles | Add Report Profile | Export Report Profiles | Import Report Profiles

Report Profile Name	Created on	Last Generated Reports	Action	Scheduler Assigned
127.0.0.1_HA	03/13/2012- 19:01:00	-	✗	Create a Schedule
user-spec	2012-04-06 14:54:40	2012-04-06 14:54:58	✗	Create One More
Web-access-report	2012-04-09 11:55:25	2012-04-09 11:55:40	✗	Create One More
somefilter	2012-04-24 11:51:13	2012-04-24 11:51:28	✗	Create One More
User web access report	2012-04-24 12:14:12	2012-04-24 12:14:27	✗	Create One More
user based web usage	2012-04-25 13:25:59	-	✗	Create a Schedule

Reports Across Devices

Firewall Reports



All Reports>> Report | ResolveDNS

user based web usage Search Report [Filter Applied]

From: 2012-04-24 00:00:00
To: 2012-04-24 23:59:59

Top 5 | Filter by | Export as

Server Traffic Details

Destination based Traffic Details

Device	Destination	User	Hits	Bytes In(MB)	Bytes Out(MB)	Total Bytes(MB)
FGT_TEST2	10.220.15.37	Emiley	30	7.17	1516.47	1523.64
FGT_TEST2	192.168.0.101	Emiley	2	0	0.08	0.08
FGT_TEST2	4.2.2.1	Emiley	166	0.01	0.02	0.03
FGT_TEST2	10.255.255.255	Emiley	3	0	0	0
Total	-	-	201	7.18	1516.58	1523.76

Conversation Details

Provides information about top conversation

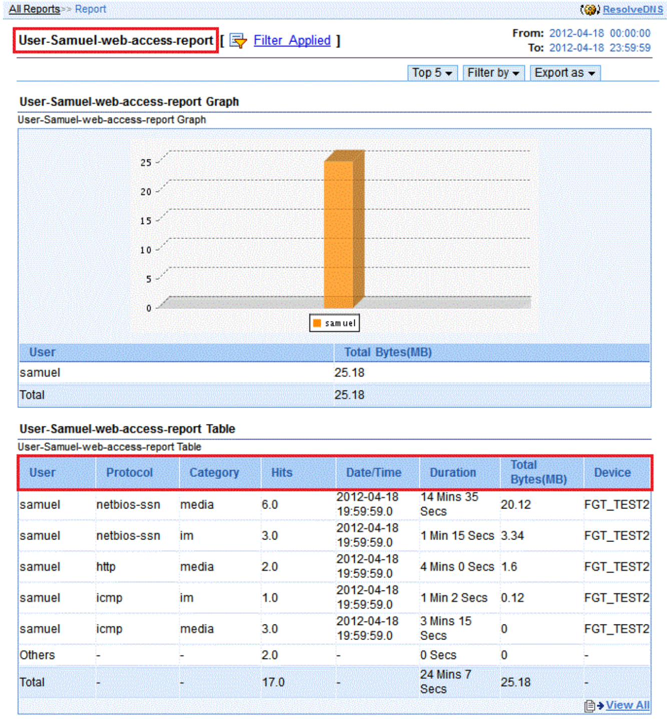
Device	Host	User	Protocol	Destination	Hits	Bytes In(MB)	Bytes Out(MB)	Total Bytes(MB)
FGT_TEST2	10.220.1.54	Emiley	ftp	10.220.15.37	30	1516.47	7.17	1523.64
FGT_TEST2	10.220.1.3	Emiley	icmp	192.168.0.101	2	0.08	0	0.08
FGT_TEST2	10.220.1.3	Emiley	dns	4.2.2.1	166	0.02	0.01	0.03
FGT_TEST2	10.10.10.10	Emiley	netbios-dgm	10.255.255.255	3	0	0	0
Total	-	-	-	-	201	1516.58	7.18	1523.76

Use Case 3: Custom Report

With Firewall Analyzer you can create a custom report to get the web sites (URLs) visited by network users. The custom report generated will be available under 'My Reports'.

This report displays the details of the web sites accessed by an enterprise user like, URLs, URL Categories, Number of visits (Hits), Date & Time of visit, Duration of visit, Total bytes consumed, Resource, Source, Destination, Protocol, Bytes sent and Bytes received. The details can be chosen as per requirement.

The screen shot of web access report for user 'samuel' is displayed below:



All Reports>> Report | ResolveDNS

User-Samuel-web-access-report [Filter Applied]

From: 2012-04-18 00:00:00
To: 2012-04-18 23:59:59

Top 5 | Filter by | Export as

User-Samuel-web-access-report Graph

User-Samuel-web-access-report Graph

User	Total Bytes(MB)
samuel	25.18
Total	25.18

User-Samuel-web-access-report Table

User-Samuel-web-access-report Table

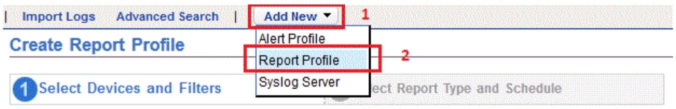
User	Protocol	Category	Hits	Date/Time	Duration	Total Bytes(MB)	Device
samuel	netbios-ssn	media	6.0	2012-04-18 19:59:59.0	14 Mins 35 Secs	20.12	FGT_TEST2
samuel	netbios-ssn	im	3.0	2012-04-18 19:59:59.0	1 Min 15 Secs	3.34	FGT_TEST2
samuel	http	media	2.0	2012-04-18 19:59:59.0	4 Mins 0 Secs	1.6	FGT_TEST2
samuel	icmp	im	1.0	2012-04-18 19:59:59.0	1 Min 2 Secs	0.12	FGT_TEST2
samuel	icmp	media	3.0	2012-04-18 19:59:59.0	3 Mins 15 Secs	0	FGT_TEST2
Others	-	-	2.0	-	0 Secs	0	-
Total	-	-	17.0	-	24 Mins 7 Secs	25.18	-

View All

The procedure to create a report profile is given below.

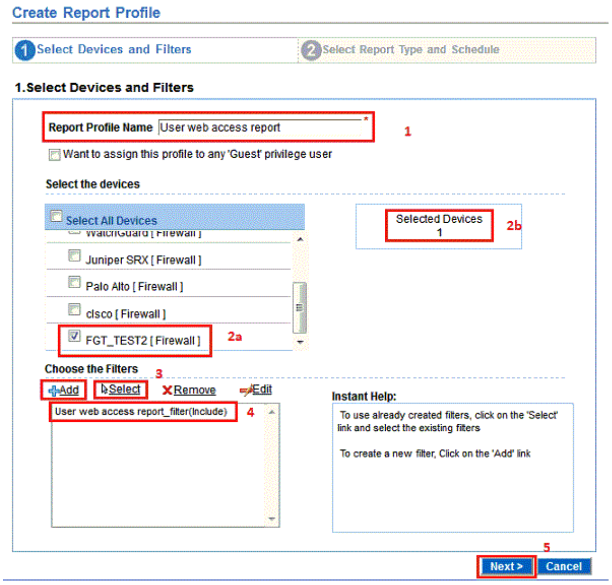
Step 1:

Create custom report using Add New > Report Profile menu.



Step 2:

Select the required device(s). Add a new filter for the report profile of select an existing filter.



Create Report Profile

1 Select Devices and Filters | 2 Select Report Type and Schedule

1.Select Devices and Filters

Report Profile Name: User web access report * — 1

□ Want to assign this profile to any 'Guest' privilege user

Select the devices

□ Select All Devices
- WatchGuard [Firewall]
- □ Juniper SRX [Firewall]
- □ Palo Alto [Firewall]
- □ cisco [Firewall]
- ☑ FGT_TEST2 [Firewall] — 2a

Selected Devices 1 — 2b

Choose the Filters 3

Add | Select | ✗Remove | Edit

User web access report_filter(Include) — 4

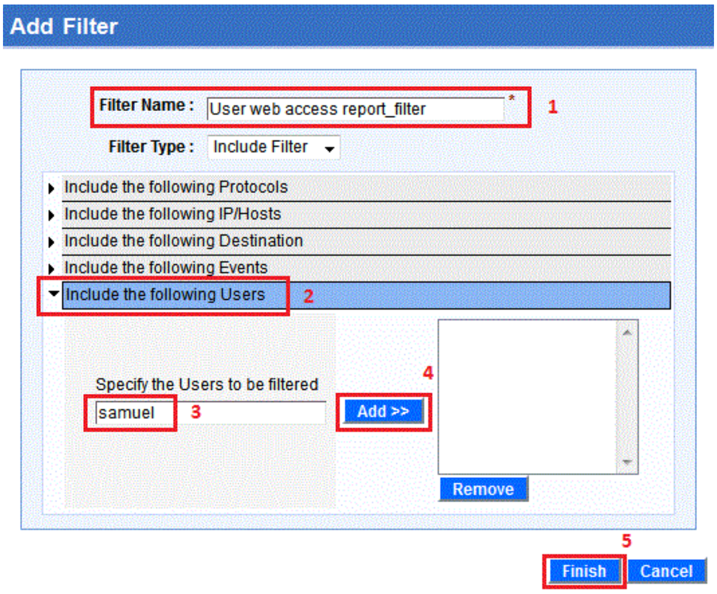
Instant Help:

To use already created filters, click on the 'Select' link and select the existing filters

To create a new filter, Click on the 'Add' link

5 Next > | Cancel

Add a new report filter. Include or exclude the Protocols, IP/Hosts, Destination, Events, and User in the filter. The 'include' and 'exclude' filter criteria combination offers basic level correlation. Select 'Include the following User'. Specify the user to be filter as 'samuel' in the text box and add it.


Add Filter

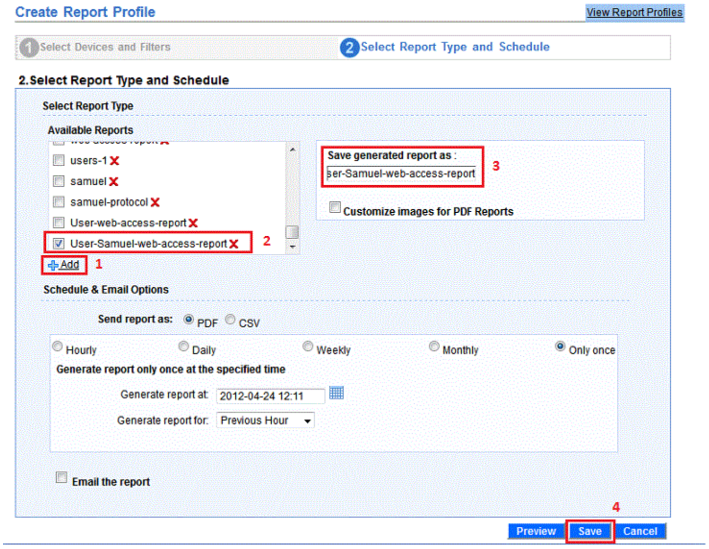
Filter Name : User web access report_filter *
Filter Type : Include Filter

- Include the following Protocols
- Include the following IP/Hosts
- Include the following Destination
- Include the following Events
- Include the following Users

Specify the Users to be filtered: samuel

Step 3:

Select the graphical and table report types. If required schedule the periodic generation of report


Create Report Profile

1 Select Devices and Filters — 2 Select Report Type and Schedule

2.Select Report Type and Schedule

Select Report Type

Available Reports

- □ users-1
- □ samuel
- □ samuel-protocol
- □ User-web-access-report
- ☑ User-Samuel-web-access-report

Save generated report as : ser-Samuel-web-access-report

□ Customize images for PDF Reports

Schedule & Email Options

Send report as: ● PDF ○ CSV

○ Hourly ○ Daily ○ Weekly ○ Monthly ● Only once

Generate report only once at the specified time

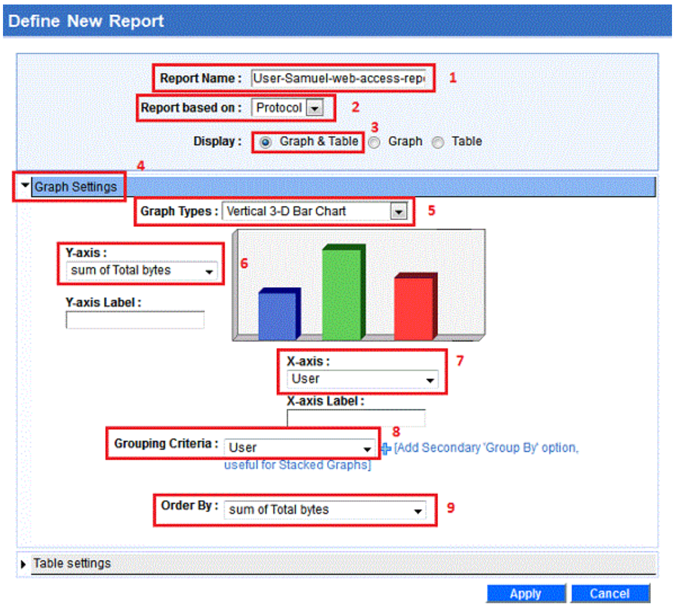
Generate report at: 2012-04-24 12:11

Generate report for: Previous Hour

□ Email the report

Step 4:

Configure the graphical setting of the report


Define New Report

Report Name : User-Samuel-web-access-rep
Report based on : Protocol
Display : ● Graph & Table ○ Graph ○ Table

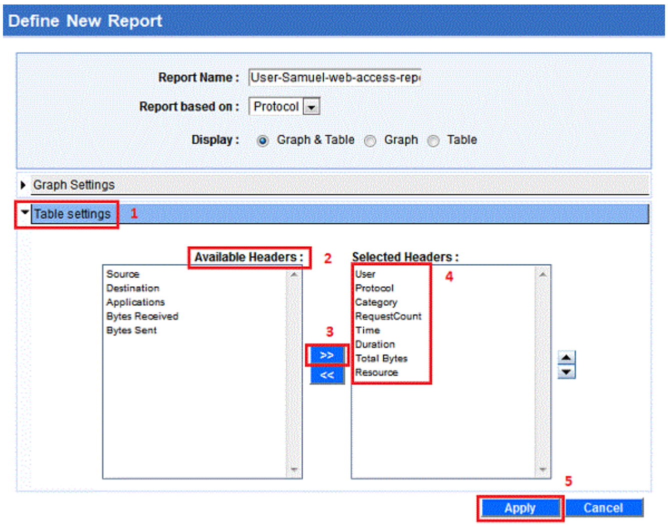
Graph Settings

Graph Types : Vertical 3-D Bar Chart
Y-axis : sum of Total bytes
Y-axis Label :
X-axis : User
X-axis Label :
Grouping Criteria : User [Add Secondary 'Group By' option, useful for Stacked Graphs]
Order By : sum of Total bytes

Table settings

Step 5:

Configure the table setting of the report


Define New Report

Report Name : User-Samuel-web-access-rep
Report based on : Protocol
Display : ● Graph & Table ○ Graph ○ Table

Graph Settings

Table settings

Available Headers : Source, Destination, Applications, Bytes Received, Bytes Sent

Selected Headers : User, Protocol, Category, RequestCount, Time, Duration, Total Bytes, Resource

With this, web sites access report for each user can be generated. As you can see the filters and report settings are so flexible that versatile reports can be created to monitor the employee web usage.

About ManageEngine Firewall Analyzer

ManageEngine Firewall Analyzer is an automated firewall log analysis tool for security event management that collects, analyses, and reports on enterprise-wide firewalls, proxy servers, VPNs, IDS/IPS, and other network perimeter devices. More than 3000 customers worldwide are using Firewall Analyzer as their Security Event Management solution to detect network anomalies, monitor firewall configuration changes (firewall change management), fine-tune firewall rules, measure bandwidth usage, manage user/employee internet access, audit traffic, and improve incident response.

https://forums.fwanalyzer.com www.facebook.com/LogAnalyzer https://twitter.com/LogGuru

About ManageEngine

ManageEngine is the leading provider of cost-effective enterprise IT management software and the only one making the 90-10 promise - to provide 90 percent of the capabilities offered by the Big 4 at just 10 percent of the price. More than 50,000 organizations in 200 countries, from different verticals, industries and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of Zoho Corp.

ManageEngine is a trademark of ZOHO Corporation. All other brand names and product names are trademarks or registered trademarks of their respective companies.