AdventNet

ManageEngine™

Firewall Analyzer 4

User Guide

www.fwanalyzer.com
support@fwanalyzer.com

Table Of Contents

Introduction

Firewall is an important perimeter defense tool which protects your network from attacks. Security tools like Firewalls, Proxy Servers, VPNs, and RADIUS servers generate a huge quantity of traffic logs, which can be mined to generate a wealth of security information reports.

What is Firewall Analyzer?

ManageEngine Firewall Analyzer is a browser-based firewall/VPN/proxy server reporting solution that uses a built-in syslog server to store, analyze, and report on these logs. Firewall Analyzer provides daily, weekly, monthly, and yearly reports on firewall traffic, security breaches, and more. This helps network administrators to proactively secure networks before security threats arise, avoid network abuses, manage bandwidth requirements, monitor web site visits, and ensure appropriate usage of networks by employees.

Firewall Analyzer analyzes your firewall and proxy server logs and answers questions like the following:

- Who are the top Web surfers in the company, and what web sites are they visiting?
- How many users inside the firewall are trying to access web sites with inappropriate content?
- How much network activity originates on each side of the firewall?
- Are we experiencing hack attempts? Where are they originating?
- Which servers receive the most hits?

This User Guide will help you install Firewall Analyzer on your machine, and get familiar with the Firewall Analyzer user interface. If you are unable to find the information you are looking for in this document, please let us know at support@fwanalyzer.com

About Firewall Analyzer

Firewall Analyzer automatically collects, correlates, and analyzes security device information from enterprise-wide heterogeneous firewalls, and proxy servers from Cisco, Fortinet, CheckPoint, WatchGuard, NetScreen, and more.

The following are some of the key features of this release:

Feature	Description
Multiple firewall vendor support	Support for most leading enterprise firewall appliances and servers
Automated syslog collection and processing	Automatically collects and parses logs, and updates the database at user-defined intervals
Syslog archiving	Allows for archiving of log files at user-defined intervals
Built-in database	Stores and processes syslog data in the embedded MySQL database
Dashboard	Provides a quick view of current activity across all devices from a single place
Automatic alerting	Automatically notifies and warns against specific events based on user-defined thresholds
Pre-defined device reports	Includes traffic analysis reports across all devices or specific to firewalls, proxy servers, and Radius servers
Historical trending	Allows you to analyze trends in bandwidth usage, protocol usage, etc. over varying time periods
Customizable report profiles	Allows you to build reports to meet your specific needs
Report scheduling	Automatically generates reports at specified time intervals and delivers them as PDF reports via email.
Multiple report formats	Generates and exports reports in HTML, PDF, and CSV formats.
Advanced user management	Allows you to create different users and set appropriate access privileges
Multi-platform support	Runs on Windows and Linux platforms

Release Notes

The new features, bug fixes and limitations in each of the release are mentioned below.

1. 4.0.0 - Build 4010
2. 4.0.0 - Build 4003
3. 4.0.0 - Build 4002
4. 4.0.0 - Build 4001
5. 4.0.0 - Build 4000 (GA)

4.0.0 - Build 4010

New Features and Enhancements

1. 20% to 30% improvement in performance.
2. Netscreen native log format support.
3. Zywall support.
4. FreeBSD support.
5. Microsoft ISA (firewall, web-proxy, packet filter) Server support.
6. Cisco ASA support.
7. IPSec VPN support for Cisco PIX - firewall reports capture duration of traffic and IPSec VPN client IP address.
8. NetASQ support.
9. Improved FWSM support - both UDP (with and with out connection id) and TCP connection logs support.
10. Checkpoint LEA support for versions R54 and above.
11. On demand DNS Resolution of IP addresses in reports.
12. Report view customization to configure the device specific reports to be shown in Device Tree and the Reports page.
13. Destination based Filter Criteria option provided in Include/Exclude filters for Add Report Profile.
14. Directory level recursive import of log files from remote hosts.
15. Importing of archived files in .zip format is supported.
16. Provision to Change Archive Location from the default location to the location of choice.
17. Drill-down for Traffic Statistics has been provided.
18. View reports of most type of archived firewall log files.
19. Enhanced Alert Criteria selection in Alert Profile creation.
20. Support for analysis of denied logs in WatchGuard firewall.

Bug Fixes

1. Issue regarding MySQL port 33336 being occupied by an earlier run of Firewall Analyzer has been fixed.
2. Out of memory issue while archiving huge log files have been fixed.

Limitation

1. Working hour and Non-Working hour traffic details for external hosts (hosts outside the intranet) will not be available in the Firewall Analyzer reports.
2. Viewing reports of archived log files of Microsoft ISA Server is not currently supported.

4.0.0 - Build 4003

Bug Fixes

1. Integrates the fix for MySQL Bug in Win 2003 SP1

4.0.0 - Build 4002

New Features and Enhancements

- The following reports have been added newly :
  - Attack Reports
  - Internet Reports
  - Inbound and Outbound Traffic reports
- Global "Search" in the product.
- Desktop Tray Icon for Windows.
- Automatic web-client connection, using the default browser, once the server has been started.
- URL reports for Cisco PIX.
- HTTP and FTP URL reports.
- Destination based report information included in most reports.
- Remote access VPN support in Cisco PIX.
- Import log support for Check Point.
- Exhaustive known protocol list support.
- Up Link Speed and Down Link Speed support to calculate % IN Traffic and % OUT traffic.
- Additional denied log messages support in Cisco PIX.
- Conversation reports added in drill down.
- Importing of archived files (.gz format) created by Firewall Analyzer.
- FTP Utility added in Support tab, to send the support information file.
- Ignore UnParsed Records while importing.

4.0.0 - Build 4001

This is a bug fix release.

Bug Fixes

- Cisco PIX EMBLEM log format support.
- Cisco PIX UNIX syslog format support.
- Netscreen quot problem.
- Wrong Hostname display in Top Inbound/Outbound Protocol drill down from Traffic Statistics table.
- Additional default protocol addition.
- Protocol identification issue which caused unknown protocol.

4.0.0 - Build 4000

GA release of Firewall Analyzer.

Features

The general features available in this release include,

- Support for most enterprise firewalls
- Support for VPN, proxy server, and RADIUS server logs

- Support for WELF, LEA, Syslog, and Native Log formats
- Built-in MySQL database to store log data
- Web-based user interface

The reporting features available in this release include,

- Pre-defined reports on bandwidth, protocol, users, etc.
- Instant reports on firewall activity
- Scheduling of reports
- Custom report profiles
- Historical trend reports
- Export and save reports to PDF
- Custom alert settings

Supported Firewalls

Firewall Analyzer is compatible with the following firewall devices.

Information on configuring some of the following firewalls is available in the Configuring Firewalls section

Company Name	Device/Version (versions up to)	WELF Certified	Other Log Format
ARKOON Network Security	ARKOON 2.20	✓	
Astaro	Astaro Security Linux v4	✓	
Aventail	Extranet Center v3.0	✓	
CheckPoint	log import from most versions and LEA support for R54 and above		✓
Cimcor	CimTrak Web Security Edition	✓	
Cisco Systems	Pix Secure Firewall v 6.x and 7.x, ASA		✓
CyberGuard	CyberGuard Firewall v4.1, 4.2, 4.3, 5.1	✓	
Fortinet	FortiGate family	✓	
FreeBSD	Most versions		✓
Global Technologies	Gnatbox (GB-1000) 3.3.0+	✓	
Ingate	Ingate firewall: 1200, 1400, 1800/1880	✓	
Inktomi	Traffic Server, C—Class and E—Class	✓	
Lucent	Security Management Server V. 6.0.471	✓	
Microsoft ISA	Microsoft ISA (firewall, web-proxy, packet filter) Server 2000 & 2004		✓
NetASQ	F10, F100 v3.x	✓	
Netopia	S9500 Security Appliance v1.6	✓	
NetScreen	Most versions	✓	
Network-1	CyberwallPLUS-WS CyberwallPLUS-SV	✓	
Recourse Technologies	ManHunt v1.2, 1.21	✓	
St. Bernard Software	iPrism 3.2 Sidewinder v5.x	✓	
SonicWALL	TELE, SOHO, PRO, GX v4.10, 5.x, 6.x	✓	
Sun Microsystems	SunScreen Firewall v3.1	✓	
WatchGuard	All Firebox Models v 5.x, 6,x, 7.x	✓	
Zywall	Most versions	✓	

Installation and Setup

System Requirements

This section lists the minimum system requirements for installing and working with Firewall Analyzer. Please refer our website for recommended system requirements.

- Hardware Requirements
- MySql Performance Improvement Parameters
- Supported Operating Systems
- Supported Web Browsers

Hardware Requirements

The minimum hardware requirements for Firewall Analyzer to start running are listed below.

Processor: 1GHz Intel™ Pentium 4 or equivalent

Memory*: 512MB of RAM

Disk Space*: 1GB for the product.

Firewall Analyzer is optimized for 1024x768 resolution and above.

***** The following table recommends the disk space and RAM size requirements of the system where Firewall Analyzer is installed. The disk space and RAM size requirements depends on the number of devices sending log information to Firewall Analyzer, the number of firewall log records received per second or the firewall log data received per day by Firewall Analyzer.

For analyzing firewall logs from more than 10 devices it is preferable to install Firewall Analyzer in a **dedicated machine with dual processor**:

Number of Devices	Log Records Per Second (Firewall Log Data Per Day)	RAM Size	Hard Disk Growth per Day if Archiving is enabled
1	250 (6 GB)	512 MB	4 GB/day
	>250	>= 1 GB	> 4 GB/day
2	250 (6 GB)	512 MB	4 GB/day
	>250	>= 2 GB	> 4 GB/day
5	100 (3 GB)	1 GB	1.5 GB/day
	>100	> 2 GB	> 4 GB/day
10	100 (3 GB)	2 GB	1.5 GB/day
	>100	>= 3 GB	> 4 GB/day
20	100 (3 GB)	>= 3 GB	1.5 GB/day
	>100	>= 3 GB	> 4 GB/day

Note: *The Log Records Per Second is the total log records received per second by Firewall Analyzer from all the configured devices.*

MySql Performance Improvement Parameters

For better performance, we recommend replacing the existing MySQL parameters mentioned in **startDB.bat/sh**, available under <FirewallAnalyzerHome>\bin directory, with the following MySQL parameters **changes** for the corresponding RAM Size.

RAM Size	MySQL Parameters
512 MB	Default configuration as given in startDB.bat/sh
1 GB	--innodb_buffer_pool_size=500M --key_buffer_size=150M --tmp_table_size=100M
2 GB	--innodb_buffer_pool_size=1200M --key_buffer_size=400M --tmp_table_size=100M
3 GB	--innodb_buffer_pool_size=1500M --key_buffer_size=600M --tmp_table_size=100M
4 GB	--innodb_buffer_pool_size=2048M --key_buffer_size=1024M --tmp_table_size=100M

Supported Operating Systems

Firewall Analyzer has been tested to run on the following operating systems and versions:

- Windows™ NT/2000/2003/XP
- RedHat Linux 8.0
- RedHat Linux 9.0

Supported Web Browsers

Firewall Analyzer has been tested to support the following browsers and versions:

- Internet Explorer 5.5 or later
- Netscape 7.0 or later
- Mozilla 1.5 or later
- Firefox 1.0 or later

Prerequisites

Before setting up Firewall Analyzer in your enterprise, ensure that the following are taken care of.

Ports to be Freed

Firewall Analyzer requires the following ports to be free:

Port Number	Usage
8500	This is the default web server port. You will access the Firewall Analyzer server from a web browser using this port number. You may change this port during installation.
514, 1514	These are the default listener ports on which Firewall Analyzer listens for incoming logs exported from devices. **You cannot change these default ports**, but you can add more ports on which Firewall Analyzer can listen for incoming logs.
33336	This is the port used to connect to the MySQL database in Firewall Analyzer

Look up Changing Default Ports for help on changing the default ports used by Firewall Analyzer

Recommended System Setup

Apart from the System Requirements, the following setup would ensure optimal performance from Firewall Analyzer:

- Run Firewall Analyzer on a separate, dedicated PC or server. The software is resource-intensive, and a busy processor may cause problems in collecting logs.
- Use the MySQL bundled with Firewall Analyzer that runs on port 33336. You need not start another separate instance of MySQL.

Changing Default Ports

Changing the default MySQL port:

1. Edit the **mysql-ds.xml** file present in the *<FirewallAnalyzer_Home>/server/default/deploy* directory.
2. Change the port number in the following line to the desired port number:
   ```
   <connection-url>jdbc:mysql://localhost:33336/firewall</connection-url>
   ```
3. Save the file and restart the server.

Changing the default web server port:

1. Edit the **sample-bindings.xml** file present in the *<FirewallAnalyzer_Home>/server/default/conf* directory.
2. Change the port number in the following line to the desired port number:
   ```
   <binding port="8500"/>
   ```
3. Save the file and restart the server.

Installing and Uninstalling

Firewall Analyzer is available for Windows and Linux platforms. For more information on supported versions and other specifications, look up System Requirements.

Installing Firewall Analyzer

Windows:

The Firewall Analyzer Windows download is available as an EXE file at http://manageengine.adventnet.com/products/firewall/download.html
Double-click the downloaded EXE file, and follow the instructions as they appear on screen.Once the installation is complete you will notice a tray icon, which provides you with the following options.

Option	Description
Firewall Server Status	This option provides you details like Server Name, Server IpAddress , Server Port, Server Status.
Start WebClient	This option will open up your default browser and connect you to the web login UI of Firewall Analyzer Server, provided the server has already been started.
Shutdown Server	This option will shutdown the Firewall Analyzer Server.

The tray icon option is only available for Windows !

Linux:

The Firewall Analyzer Linux download is available as a BIN file at http://manageengine.adventnet.com/products/firewall/download.html

1. Download the BIN file, and assign **execute** permission using the command: `chmod a+x` *<file_name>*`.bin`
   where *<file_name>* is the name of the downloaded BIN file.
2. Execute the following command: `./`*<file_name>*`.bin`

   During installation if you get an error message stating that the temp folder does not have enough space, try executing this command with the -is:tempdir <directory_name> option, where <directory_name> is the absolute path of an existing directory. ./<file_name>.bin -is:tempdir <directory_name>

3. Follow the instructions as they appear on the screen.

This will install Firewall Analyzer on the respective machine.

Uninstalling Firewall Analyzer

Windows:

1. Navigate to the Program folder in which Firewall Analyzer has been installed. By default, this is **Start > Programs > ManageEngine Firewall Analyzer 4**.
2. Select the option **Uninstall Firewall Analyzer**.
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.

Linux:

1. Navigate to the *<FirewallAnalyzerHome>/server/_uninst* directory.
2. Execute the command `./uninstaller.bin`
3. You will be asked to confirm your choice, after which Firewall Analyzer is uninstalled.

At the end of uninstallation you will be taken to the Uninstallation Feedback Form where you can provide reasons for your product uninstallation. This would help us improve this product.

Starting and Shutting Down

Once you have successfully installed Firewall Analyzer, start the Firewall Analyzer server by following the steps below.

Starting Firewall Analyzer

Windows:

Click on **Start > Programs > ManageEngine Firewall Analyzer 4 > Firewall Analyzer** to start the server.
Alternatively, you can navigate to the *<FirewallAnalyzer_Home>\bin* folder and invoke the **run.bat** file.

Linux:

Navigate to the *<FirewallAnalyzer_Home>/bin* directory and execute the **run.sh** file.

As soon as this is done, a command prompt window opens showing startup information on several modules of Firewall Analyzer. Once all the modules have been successfully created, the following message is displayed:

```
Server started.
Please connect your client at http://localhost:8500
```

where `8500` is replaced by the port you have specified as the web server port during installation.

Shutting Down Firewall Analyzer

Follow the steps below to shut down the Firewall Analyzer server. Please note that once the server is successfully shut down, the MySQL database connection is automatically closed, and all the ports used by Firewall Analyzer are freed.

Windows:

1. Navigate to the Program folder in which Firewall Analyzer has been installed. By default, this is **Start > Programs > ManageEngine Firewall Analyzer 4**.
2. Select the option **Shut Down Firewall Analyzer**.
3. Alternatively, you can navigate to the *<FirewallAnalyzer_Home>\bin* folder and invoke the **shutdown.bat** file.
4. You will be asked to confirm your choice, after which the Firewall Analyzer server is shut down.

Linux:

1. Navigate to the *<FirewallAnalyzer_Home>/bin* directory.
2. Execute the **shutdown.sh** file.
3. You will be asked to confirm your choice, after which the Firewall Analyzer server is shut down.

Accessing the Web Client

Firewall Analyzer is essentially a firewall, VPN, and proxy server log analysis tool that collects, stores, and reports on logs from distributed firewalls, proxy servers, and Radius servers on the network.

Once the server has successfully started, follow the steps below to access Firewall Analyzer.

1. Open a supported web browser window
2. Type the URL address as ***http://<hostname>:8500*** (where *<hostname>* is the name of the machine on which Firewall Analyzer is running, and *8500* is the default web server port)
3. Log in to Firewall Analyzer using the default username/password combination of **admin/admin**.

Once you log in, you can start collecting firewall logs, generate reports, and more.

If you want to access the web client from the same machine on which Firewall Analyzer is installed, execute the startClient.bat/.sh file from the <FirewallAnalyzer_Home>/bin directory.

On a Windows machine, you can also access the web client from the Start menu by clicking on Start > Programs > ManageEngine Firewall Analyzer 4 > Firewall Analyzer Web Client

License Information

After you log in to Firewall Analyzer, click the **Upgrade License** link present in the top-right corner of the screen. The License window that opens, shows you the license information for the current Firewall Analyzer installation.

The License window displays the following information:

- Type of license applied - Trial or Registered
- Product version number
- Number of days remaining for the license to expire
- Maximum number of devices that you are allowed to manage

Upgrading your License

Before upgrading the current license, make sure you have the new license file from AdventNet saved on that system.

1. Browse for the new license file, and select it.
2. Click **Upgrade** to apply the new license file.

The new license is applied with immediate effect.

Contact support@fwanalyzer.com or sales@adventnet.com for any license-related queries.

Getting Started

Once Firewall Analyzer has been successfully set up and started in your network, the next thing you need to do is start sending logs to the Firewall Analyzer server.

As soon as you log in, you will see the Dashboard. If no devices are sending logs to Firewall Analyzer, you will see a welcome screen, with options to help you get started.

Each of those options is explained below:

Configure Your Firewall

If your firewall is capable of exporting logs to the displayed ports in Firewall Analyzer, then set the appropriate parameters in the firewall to do so. Click the **How do I do this?** link for specific instructions on setting up log exports on certain firewalls.

Add Syslog Server

If your firewall cannot export logs to the displayed ports in Firewall Analyzer, but can export logs to another port, click the **Add Syslog Server** link to add a virtual syslog server and start receiving exported logs on the newly configured port.

Import Log File

If your firewall cannot export logs, or you need to generate reports from a squid proxy server click the **Import Log File** link to import a log file from the local machine or a remote machine via FTP.

Simulate

If you do not want to receive log files from any device, but still generate reports, click the **Simulate** link to generate reports from sample firewall logs. You can later turn this off by clicking the **Stop Simulate** link from the **Settings** tab.

Using the Dashboard

The Dashboard is shown when the **Home** tab is clicked. It is the first page you see when you log in.

Once the server has started receiving records, the Dashboard dynamically changes to display the current statistics for each device whose log files are analyzed.

The **Traffic Overview** graph shows the protocol-wise distribution of traffic across all devices. At one glance, you can see the total traffic generated by each protocol group across each device. You can also drill down from the bars in the graph to see specific protocol usage in the Protocol Usage Report.

The **Event Overview** pie-chart shows the severity-wise distribution of events generated across all devices. Drill down from each pie to see the corresponding events generated. Click the **More...** link to view details of all events generated.

The Events table groups the number of events generated by each device, based on event severity. But the Event Overview pie-chart groups events from all devices based on event severity. Hence, the numbers may not match when you drill down.

The **Traffic Statistics** table, shows the Traffic Overview graph's data in more detail, with specific percentage values of incoming and outgoing traffic per protocol group across each device. You can click on the Traffic IN, Traffic OUT, and Total Traffic for each protocol group of the configured device to obtain the drill-downs of the traffic. If the ⚠ icon is displayed above the table, it indicates that intranets have not been configured. You need to configure intranets if you want to separate inbound and outbound firewall traffic.

The traffic values in the table let you drill down to see traffic details for the corresponding protocol group in the Protocol Usage Report.

The ? icon next to the Unassigned protocol group indicates traffic details for protocols that have not been assigned to any protocol group. Click the icon, and under the **View Identifiers** tab, you can see the traffic details for each of these unassigned protocols. The **Assign Group** tab provides you with options to either associate these unknown protocols to the predefined Protocol Groups (and Protocols) or create a new Protocol Group (and Protocol). You can do this by selecting from the listed identifier and assigning it to either the pre-defined Protocol Group (and Protocol) or create a + new protocol group (and new Protocol).

Multiple Selection enables you to assign multiple identifiers to a particular protocol group (and protocol). **Single selection** enables you to assign each of the individual identifier to a particular protocol group (and protocol).

Editing Device Details

Click the ✎ (for firewall) or ✎ (for squid) or ✎ (for radius) icon next to a device name to change the device's details. You can change the device's display name, up link speed and down link speed. The device name and the vendor type cannot be changed.

Up Link Speed and Down Link Speed determines the % IN Traffic and % OUT traffic.

Click the ✖ icon to delete the device from the database. You are asked to confirm your choice, after which the device is permanently deleted.

⚠	When a device is deleted, all existing data pertaining to that device is permanently deleted from the database. Later if logs are received from that device, the device is added as a new device, and reports are generated. To stop this from happening, you need to configure the device to stop sending logs to Firewall Analyzer.

Search

A **Global Search**, is available in all the pages of the product which enables you to search for the following :

Search for	Description
Hosts	Refers to the IP Address or DNS Names which were recorded in the firewall logs example: 192.168.0.1,web-server
Protocol Identifiers	Refers to the list of protocols and protocol identifiers that are available in the Protocol Groups page (Settings >> Protocol Groups) example: 6969/tcp, icmp, IPSec
User Names	Refers to the authenticated user name required by some firewalls. example: john, kate
Attack	Refers to the attack name. examples: UDP Snort, Ip spoof
Virus	Refers to the Virus name. examples: JS/Exception, W32/Mitglieder

- If the search string exists then the search result will be intelligently displayed based on the report category in which it occurred.
- By default, the search is carried out for the time period selected in the Global Calendar present in the left pane of the UI.
- You can also search within the search results.

Using The Sub Tab

The sub tab provides links to frequently accessed reports and tasks in Firewall Analyzer. It also shows the current server status using intuitive icons.

The following reports can be generated by clicking the corresponding links in the sub tab:

Link	Action
Live Reports	View live traffic reports for the past one day for each firewall, on a 5-minute average
My Report Profiles	View the list of custom report profiles created so far

The following tasks can be done by clicking the corresponding links in the sub tab:

Link	Action
Add Report Profile	Create a new custom report profile
Add Syslog Server	Add a virtual syslog server to receive logs from different ports
Add Protocol Group	Create a new protocol group to identify new protocols
Add Alert Profile	Create a new alert profile to trigger alerts and send notifications
Import Logs	Import a log file from your local machine or through FTP

The purpose of each icon in the sub-tab is described below:

Icon	Description
📂	Packet Count - the number of packets received from each device sending log files to the server.
💻	Listening Ports - the list of ports at which the server is listening for logs and devices that are sending logs to the syslog server at the particular port. If any of the ports is down, then you would receive a message in web UI "Syslog listener port <port number> is down"
●	No Unknown Packets Received - no unknown packets or unsupported log formats have been received by the server
❗	Unknown Packets Received - unknown packets have been sent to the server. Details such as, the source sending the records, receiving port, etc. are also displayed.

Using The Left Navigation Pane

The left navigation pane provides quick links to different tasks and reports in Firewall Analyzer. The components present in the left navigation pane depend on the tab that is currently selected.

The following is a list of all components found in the left navigation pane:

Component	Description
Global Calendar	Allows you to select the time period for all reports from one place. By default, the last day's data is shown.
Reports Across Devices	Includes links to generate reports across all devices from which logs have been collected
Firewall Reports	Includes links to generate reports for each firewall from which logs have been collected. Click on the 📊 icon against each firewall to generate reports for that firewall alone in a new window.
Squid Proxy Reports	Includes links to generate reports for each squid proxy server from which logs have been collected. Click on the 📊 icon against each squid proxy server to generate reports for that squid proxy server alone in a new window.
Radius Reports	Includes links to generate reports for each Radius server from which logs have been collected. Click on the 📊 icon against each Radius server to generate reports for that Radius server alone in a new window.
My Report Profiles	Includes links to generate custom reports created using the Add Report Profile link.
Bookmarks	Allows you to set a bookmark for the current page, and manage existing bookmarks

Most of the tasks in the left navigation pane can be done from the main tabs also, by clicking the corresponding links. The left navigation pane provides a quicker way to perform the same tasks.

Firewall Reports

Generating Reports

Firewall Analyzer offers a rich set of pre-defined reports that help in analyzing bandwidth usage and understanding network behavior. On a broad level, reports in Firewall Analyzer are classified into the following types:

Report	Description
Reports Across Devices	View bandwidth usage, protocol usage, etc. across all devices whose logs are analyzed
Firewall Reports	View traffic reports, protocol usage, event summary, etc. for each firewall
Squid Proxy Reports	View top talkers, site details, and squid usage summary for each squid proxy server
Radius Server Reports	View top users, request trends, and usage summary for each Radius server
My Report Profiles	Create custom report profiles to report on specific parameters
Trend Reports	View trends of bandwidth usage, protocol usage, and events generated

All the above reports can be accessed from the **Reports** tab. Except the **Live Report**, all other reports include links to several sections of the report which can be seen when the ⊞ icon, or the report bar itself is clicked. Click on each section to go to the corresponding section of the report directly, or click the **View Report** link to view the entire report with all the sections.

In each of the individual reports a **ResolveDNS** link has been provided at the top. Clicking this link enables DNS Resolution for all the IP Addresses of the unresolved hosts present in the current report. The status of DNS Resolution depends on the default DNS lookup time, within which Firewall Analyzer will try to resolve the IP Address. If DNS Resolution is in progress for any other Firewall Analyzer user, then the subsequent user will see the message "*Please wait, DNS Resolution in progress for another user*" when clicking ResolveDNS link. Once the DNS Resolution is complete for the first user, then the DNS Resolution for the subsequent user begins automatically.

Live Reports

The **Live Reports** provide a live visual representation of the traffic load across network links. Graphs are similar to that of MRTG, with the aim of providing a simple way to see exactly how much inbound and outbound traffic was generated for each device.

The graphs for each device shows the minimum, maximum, and average amount of incoming and outgoing traffic through that device, over several time periods. Traffic is broken down into the last day, last week, last month, and last year, with an average granularity of 5 minutes, 30 minutes, 2 hours, and 1 day respectively.

Click the **Live Reports** link in the sub tab or in the **Reports Across Devices** box in the left navigation pane, to see the live reports for all devices, for the last one day, over a 5-minute average.

Click the **Live Reports** link present inside the list of reports for a device, to see the live reports for that device alone, over all the time periods described above.

Drill down from each of the graphs in the live report to see the following details:

Graph	Description
Inbound/Outbound Traffic Conversations	The inbound/outbound conversations for all hosts across this firewall. This data is available only for the last day's traffic over a 5-minute average granularity.
Top Hosts	The top hosts contributing to inbound/outbound traffic across this firewall. Drill down from this graph to see the corresponding conversations for each host, during the selected time period.
Top Protocol Groups	The top protocol groups used in inbound/outbound traffic across this firewall. Drill down from this graph to see the corresponding conversations using each protocol group, during the selected time period.
Top Users	The top users contributing to inbound/outbound traffic across this firewall. Drill down from this graph to see the corresponding conversations for each user, during the selected time period.

Traffic Reports

The **Traffic Reports** section includes reports that show bandwidth usage based on the amount of traffic sent and received through the device.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocol Groups	The top protocol groups used by these hosts
Top Destinations	The top destination hosts or IP addresses accessed by these hosts
Traffic Distribution - Working Hours	The amount of traffic that was generated during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated after working hours - for example, between 8 p.m. to 10 a.m.
Rules Triggered	Firewall rules that were triggered by these hosts

The **Top Protocol Groups - Sent** and **Top Protocol Groups - Received** graphs show the top protocol groups sending and receiving data across the device respectively. The **Top Protocol Groups - Sent + Received** graph shows the top protocol groups grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the protocol group name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top protocols in this protocol group
Top Hosts	The top hosts generating traffic using protocols in this protocol group
Top Users	The top users generating traffic using protocols in this protocol group
Top Destinations	The top destinations accessed by protocols in this protocol group
Top Conversations	The overall top conversations through this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by protocols in this protocol group during working hours -for example : 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by protocols in this protocol group after working hours - for example : 8 p.m. to 10 a.m.

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users (Sent + Received)** graph shows the top users grouped by summing the number of bytes sent and received by each. The table below each graph shows the user name, number of hits, and the number of bytes sent or received or both as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocol Groups	The top Protocol Groups through which higher volume of data transferred.
Top Destinations	The top destinations accessed by user to transfer data
Top Hosts	The top hosts used by user, that transferred higher volume of data.
Rules Triggered	The Rules (policy violation, etc) that were triggered by the user whle transferring data..
Traffic Distribution - Working Hours	The amount of traffic that was generated by user during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by user after working hours - for example, between 8 p.m. to 10 a.m.

The **Events Generated** pie-chart shows the number of events generated, grouped by event severity. The table below the graph shows the event severity, number of events generated with that event severity, and the number of bytes of traffic generated.

Drill down from the pie-chart to see the following details:

Graph	Description
Top Hosts	The top hosts that generated events of this severity
Top Event Messages	The top event messages received with this severity along with the hosts which generated them
Event Distribution - Working Hours	The number of events generated during working hours - for example, between 10 a.m. to 8 p.m.
Event Distribution - Non-working Hours	The number of events generated after working hours - for example, between 8 p.m. to 10 a.m.

Protocol Usage Reports

The **Protocol Usage Reports** section includes reports that show bandwidth usage based on all the protocol groups generating traffic through the device.

Separate reports are available for Web, Mail, FTP, and Telnet protocol groups. Click on the respective reports to view bandwidth usage details.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocol Groups - Sent** and **Top Protocol Groups - Received** graphs show the top protocol groups sending and receiving data across the device respectively. The **Top Protocol Groups - Sent + Received** graph shows the top protocol groups grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the protocol group name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top protocols in this protocol group
Top Hosts	The top hosts generating traffic using protocols in this protocol group
Top Users	The top users generating traffic using protocols in this protocol group
Top Destinations	The top destinations accessed by protocols in this protocol group
Top Conversations	The top conversations using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by protocols in this protocol group during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by protocols in this protocol group after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Destinations	The top destination hosts or IP addresses accessed by these hosts
Top Users	The top users using this host in generating traffic
Traffic Distribution - Working Hours	The amount of traffic that was generated by the host during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by the host after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Destinations	The top destinations accessed by the user
Top Hosts	The top hosts used by user in generating traffic
Traffic Distribution - Working Hours	The amount of traffic that was generated by the user during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by the user after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the destination and the number of hits.

Web Usage Reports

The **Web Usage Reports** section includes reports on the top protocols under the Web protocol group, that have been used to generate traffic through that device.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the 📄 icon to export this report to PDF. Click on the csv icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

> 💡 Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top Web protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by using this protocol during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by using this protocol after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Web protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using Web protocols
Top Hosts	The top hosts used by this user to generate traffic using Web protocols
Traffic Distribution - Working Hours	The amount of traffic that was generated by this user, using Web protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this user, using Web protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each

graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Web protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using Web protocols
Top Conversations	The top conversations initiated by host using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by this host, using Web protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this host, using Web protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top URLs** table shows the top URL's or web sites that were accessed using protocols in the Web protocol group.

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the hosts triggering the rules.

Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

Mail Usage Reports

The **Mail Usage Reports** section includes reports on the top protocols under the Mail protocol group, that have been used to generate traffic through that device.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top Mail protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by using this protocol during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by using this protocol after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Mail protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using Mail protocols
Top Hosts	The top hosts used by this user to generate traffic using Mail protocols
Traffic Distribution - Working Hours	The amount of traffic that was generated by this user, using Mail protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this user, using Mail protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each

graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Mail protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using Mail protocols
Top Conversations	The top conversations initiated by host using protocols in this protocol group
Traffic Distribution – Working Hours	The amount of traffic that was generated by this host, using Mail protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this host, using Mail protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the destination and the number of hits.

📝	Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

FTP Usage Reports

The **FTP Usage Reports** section includes reports on the top protocols under the FTP protocol group, that have been used to generate traffic through that device.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the csv icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

> Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top FTP protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by using this protocol during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by using this protocol after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top FTP protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using FTP protocols
Top Hosts	The top hosts used by this user to generate traffic using FTP protocols
Traffic Distribution - Working Hours	The amount of traffic that was generated by this user, using FTP protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this user, using FTP protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each

graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top FTP protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using FTP protocols
Top Conversations	The top conversations initiated by host using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by this host, using FTP protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this host, using FTP protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the destination and the number of hits.

The **Top URLs** table shows the top URL's or web sites that were accessed using protocols in the FTP protocol group.

Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

Telnet Usage Reports

The **Telnet Usage Reports** section includes reports on the top protocols under the Telnet protocol group, that have been used to generate traffic through that device.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

> Click on the **Protocol Groups** link under the **Settings** tab to see what protocols fall under each protocol group, and how to edit them.

The **Top Protocols - Sent** and **Top Protocols - Received** graphs show the top Telnet protocols sending and receiving data across the device respectively. The **Top Protocols - Sent + Received** graph shows the top protocols grouped by summing the number of bytes sent and received by each protocol. The table below each graph shows the protocol name, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Hosts	The top hosts generating traffic using this protocol
Top Destinations	The top destinations accessed by using this protocol
Top Conversations	The top conversations using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by using this protocol during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by using this protocol after working hours -for example, between 8 p.m. to 10 a.m.

The **Top Users - Sent** and **Top Users - Received** graphs show the top users sending and receiving data across the device respectively. The **Top Users - Sent + Received** graph shows the top users grouped by summing the number of bytes sent and received by each protocol group. The table below each graph shows the user name, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Telnet protocols used by this user
Top Destinations	The top destination hosts or IP addresses accessed by this user using Telnet protocols
Top Hosts	The top hosts used by this user to generate traffic using Telnet protocols
Traffic Distribution - Working Hours	The amount of traffic that was generated by this user, using Telnet protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this user, using Telnet protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Hosts - Sent** and **Top Hosts - Received** graphs show the top hosts sending and receiving data across the device respectively. The **Top Hosts - Sent + Received** graph shows the top hosts grouped by summing the number of bytes sent and received by each host. The table below each graph shows the host name or IP address, the protocol used, number of hits, and the number of bytes sent or received as applicable.

Drill down from each of the above graphs to see the following graphs:

Graph	Description
Top Protocols	The top Telnet protocols used by this host
Top Destinations	The top destination hosts or IP addresses accessed by this host using Telnet protocols
Top Conversations	The top conversations initiated by hosts, using protocols in this protocol group
Traffic Distribution - Working Hours	The amount of traffic that was generated by this host, using Telnet protocols during working hours - for example, between 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated by this host, using Telnet protocols after working hours - for example, between 8 p.m. to 10 a.m.

The **Top Rules** table shows the top protocol groups triggering firewall rules, the rules that were triggered, and the destination and the number of hits.

📝	Look up Managing Protocol Groups for help on adding, editing, and deleting protocol groups and protocols.

Event Summary Reports

The **Event Summary Reports** section includes reports that show the summary of events generated by that device.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

The **Top Hosts** graph shows the top hosts generating events along with the respective event severities. The table below the graph shows the host name or IP address, the event severity, the number of events, and the number of bytes of traffic generated.

Drill down from this graph to see the following graphs:

Graph	Description
Top Event Messages	The top event messages generated and corresponding event ID
Event Distribution - Working Hours	The number of events generated during working hours - for example, between 10 a.m. to 8 p.m.
Event Distribution - Non-working Hours	The number of events generated after working hours - for example, between 8 p.m. to 10 a.m.

The **Event Summary** pie-chart shows the number of events generated, grouped by event severity. The table below the graph shows the event severity, number of events generated with that event severity, and the number of bytes of traffic generated.

Drill down from the pie-chart to see the following details:

Graph	Description
Top Hosts	The top hosts that generated events of this severity
Top Event Messages	The top event messages received with this severity along with the hosts which generated them
Event Distribution - Working Hours	The number of events generated during working hours - for example, between 10 a.m. to 8 p.m.
Event Distribution - Non-working Hours	The number of events generated after working hours - for example, between 8 p.m. to 10 a.m.

Event Messages will list all the event messages in the descending order of number of events along with the severity.

VPN Usage Report

The **VPN Usage Report** shows the bandwidth usage statistics across each VPN configured behind the firewall.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top VPN Users** graph shows the top VPN users across all VPNs behind this firewall. The table below the graph shows each user, along with the number of hits, and the total bytes of traffic generated by each user.

Drill down from the graph to see the following details for each user:

Graph	Description
Top VPN Protocol Groups	List of Protocol Groups through which this User transferred higher volume of data.
VPN Summary	The bandwidth used by this User across each VPN
Top VPN Hosts	List of VPN Hosts used by this User..
Top Destinations	List of Destinations Accessed by this User.
Top Clients	List of VPN Clients used by this User.
Top Conversations	List of conversations started by this User.
VPN Usage - Working Hours	VPN bandwidth used by this User during working hours - for example, between 10 a.m. to 8 p.m.
VPN Usage - Non-working Hours	VPN bandwidth used by this User after working hours - for example, between 8 p.m. to 10 a.m.

The **Top VPN Hosts** graph shows the top hosts using bandwidth across all VPNs configured behind this firewall. The table below the graph shows the host names or IP addresses along with the number of hits, and the total bytes of traffic generated by each host.

Drill down from the graph to see the following details for each host:

Graph	Description
Top VPN Protocol Groups	The top protocol groups used by this host. This graph drills down further to show the top users using these protocols.
VPN Summary	The bandwidth used by this host across each VPN
Top VPN Users	List of VPN users connecting through this host.
Top Destinations	The top Destinations Accessed by this host.
Top Clients	The top clients used by this host.
Top Conversations	The top conversations through this host.
VPN Usage - Working Hours	VPN bandwidth used by this host during working hours - for example, between 10 a.m. to 8 p.m.
VPN Usage - Non-working Hours	VPN bandwidth used by this host after working hours - for example, between 8 p.m. to 10 a.m.

The **Top VPN Clients** graph shows the top clients accessing the VPN. The table below the graph shows the host names or IP addresses along with the number of hits, and the total bytes of traffic transferred by each client.

Drill down from the graph to see the following details for each host:

Graph	Description
Top Protocol Groups	The top protocol groups Protocol Groups through which the client transferred higher volume of data.
Top VPN Users	The top VPN users connecting through the Client.
Top VPN Destinations	The top Destinations Accessed through Client.
Top Conversations	The top conversations connecting through Client.
VPN Summary	The list of VPNs used by Client
VPN Usage - Working Hours	VPN Usage during Working Hours by client - for example, between 10 a.m. to 8 p.m.
VPN Usage - Non-working Hours	VPN Usage during non Working Hours by client - for example, between 8 p.m. to 10 a.m.

The **Top VPN Protocol Groups** graph shows the top protocol groups used by VPNs behind this firewall. The table below the graph shows each protocol group, along with the number of hits, and the total bytes of traffic generated by each protocol group.

Drill down from the graph to see the following details for each protocol group:

Graph	Description
Top VPN Hosts	The top hosts behind the VPN using these protocol groups. This graph drills down further to show the top users using these protocols.
VPN Summary	The bandwidth used by this protocol group across each VPN
Top Destinations	List of Destinations Accessed through this protocol group.
Top Clients	List of Clients using this protocol group.
Top Conversations	List of VPN conversations through this protocol group.

The **VPN Summary** pie-chart shows the total bandwidth used by each VPN behind this firewall. The table below the pie-chart shows the VPN name, the gateway used, the number of hits, and the total bytes of traffic generated by each VPN.

Drill down from the pie-chart to see the following details for each VPN:

Graph	Description
Top Protocol Groups	The top protocol groups used by this VPN. This graph drills down further to show the top hosts using these protocols.
Top VPN Hosts	The top hosts or IP addresses using this VPN
Top Destinations	The top Destinations Accessed through Client.
Top Clients	The top clients using the VPN
Top Conversations	The top conversations through VPN.
VPN Usage - Working Hours	Bandwidth used by this VPN during working hours - for example, between 10 a.m. to 8 p.m
VPN Usage - Non-working Hours	Bandwidth used by this VPN after working hours - for example, between 8 p.m. to 10 a.m.

The **VPN Traffic Usage Trend** graph shows the hourly trend in VPN traffic across all VPNs configured behind this firewall. The table below the graph shows the the number of hits, and the total bytes of traffic generated every hour by all the VPNs.

Firewall Rules Report

The **Firewall Rules Report** shows the top firewall rules triggered on this firewall, grouped by different categories.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Rules - Protocol Group Based** graph shows the top protocol groups that have triggered firewall rules. The table below the graph shows the protocol group, the rule triggered, and the number of hits. Drill down from this graph to see the top hosts, the top protocols and the top conversations that triggered the firewall rule in that protocol group.

The **Top Rules - Host Based** graph shows the top hosts that have triggered firewall rules. The table below the graph shows the host, the rule triggered, the number of hits. . Drill down from this graph to see the top destinations accessed, the top protocols and the top conversations for each host that triggered the firewall rule .

The **Top Rules - Destination Based** graph shows the top destinations for which firewall rules have been triggered. The table below the graph shows the destination host name or IP address, the rule triggered, and the number of hits. Drill down from this graph to see the top hosts, the top protocols and the top conversations that triggered the firewall rule.

The **Top Rules** table shows the overall top firewall rules that have been triggered across this firewall. The table below the graph shows the rule triggered, and the number of hits. Drill down from this graph to see the top hosts, the top protocols and the top conversations that triggered the firewall rule.

Inbound Outbound Reports

The **Inbound Outbound Traffic Reports** section includes reports that show traffic details when inbound traffic (traffic coming into LAN) and outbound traffic (traffic going out of LAN) for the firewall, are separated. In order to separate inbound and outbound traffic, you need to first configure your intranets by clicking the **Intranet Settings** link from the **Settings** tab. When configured, the **Inbound Outbound Traffic Reports** shows you which hosts and what protocol groups have been contributing the most traffic on either side of the firewall.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Hosts - Inbound Firewall Traffic** graph shows the top hosts contributing to traffic inbound (traffic coming into LAN) to the firewall. The table below the graph shows the host name or IP address, along with the number of hits and the total bytes of traffic generated.

📝	If the host (IP / DNS Name of the machine which initiated the conversation) is INSIDE the LAN (Internal Host), then their RECEIVED will be counted as inbound and If the host (IP / DNS Name of the machine which initiated the conversation) is OUTSIDE the LAN (External Host) then their SENT will be counted as inbound.

The **Top Hosts - Outbound Firewall Traffic** graph shows the top hosts contributing to traffic outbound (traffic going out of LAN) to the firewall. The table below the graph shows the host name or IP address, along with the number of hits and the total bytes of traffic generated.

📝	If the host (IP / DNS Name of the machine which initiated the conversation) is INSIDE the LAN (Internal Host), then their SENT will be counted as outbound and If the host (IP / DNS Name of the machine which initiated the conversation) is OUTSIDE the LAN (External Host) then their RECEIVED will be counted as outbound.

The **Top Protocol Groups - Inbound Firewall Traffic** graph shows the top protocol groups contributing to traffic inbound to the firewall. The table below the graph shows the protocol group, along with the number of hits and the total bytes of traffic generated.

The **Top Protocol Groups - Outbound Firewall Traffic** graph shows the top protocol groups contributing to traffic outbound to the firewall. The table below the graph shows the protocol group, along with the number of hits and the total bytes of traffic generated.

Intranet Reports

The **Intranet Reports** section includes reports that show details of traffic transferred through the firewall by the internal hosts (hosts inside your LAN). In order to identify your internal hosts, you need to first configure your intranets by clicking the **Intranet Settings** link from the **Settings** tab.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Internal Hosts (Sent+Received)** graph shows the top internal hosts that are sending and receiving traffic through the firewall. You can expect only IP's **inside your LAN** here. The table below the graph shows the IP address, along with the number of hits, bytes received, bytes sent, and the total bytes (sent + received) of traffic generated.

The **Top Internal Protocol Groups (Sent+Received)** graph shows the top protocol groups used by internal host for sending and receiving traffic through the firewall. The table below the graph shows the protocol group, along with the number of hits, % hits, total bytes of traffic generated and what % of traffic each protocol group constitute to the total traffic.

The **Top Internal Servers** graph shows the top internal servers that served traffic. This is destination based report which list the internal servers which served more for external hosts. Transaction is not started/initiated by the servers listed here. Here you can expect all your server IPs which are behind your firewall, i.e. inside your LAN. The table below the graph shows the IP address of the internal server, along with the number of hits, the total bytes of traffic, and % of total traffic to the particular internal server.

The **Top Conversations** table lists details like host which initiated the conversation, its destination, the protocol used for the conversation along with the number of hits, the total bytes of traffic generated and % of total traffic for the particular conversation.

Internet Reports

The **Internet Reports** section includes reports that show details of traffic transferred through the firewall by the external hosts (hosts outside your LAN). In order to identify your external hosts, you need to first configure your intranets by clicking the **Intranet Settings** link from the **Settings** tab. When configured, all hosts outside your configured intranets will be considered as external hosts.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top External Hosts (Sent+Received)** graph shows the top external hosts that are sending and receiving traffic through the firewall. Here you can expect only IP's **outside your LAN**. The table below the graph shows the IP address, along with the number of hits, bytes received, bytes sent, and the total bytes (sent + received) of traffic generated.

The **Top External Protocol Groups (Sent+Received)** graph shows the top protocol groups used by external host for sending and receiving traffic through the firewall. The table below the graph shows the protocol group, along with the number of hits, % hits, total bytes of traffic generated and what % of traffic each protocol group constitute to the total traffic.

The **Top External Sites** graph shows the top external sites that were visited. This is destination based report which list the external servers or sites which served more for the internal hosts. Transaction is not started/initiated by the servers listed here. You can expect all external sites which are browsed more by your internal hosts. The table below the graph shows the host name or IP address, along with the number of hits, the total bytes of traffic to the site, and % of total traffic to the particular external site.

The **Top Conversations** table lists details like host which initiated the conversation, its destination, the protocol used for the conversation along with the number of hits, the total bytes of traffic generated and % of total traffic for the particular conversation.

Security Reports

The **Security Reports** section includes reports that help in monitoring and analyzing the security and effectiveness of the firewall, and assist in identifying, tracking, and investigating potential security risks.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Denied Hosts** report shows the top source IP addresses or host names that have been denied requests for the selected time period. The **Top Denied Destinations** report shows the top destination IP addresses or host names that have been denied responses for the selected time period.

Drill down from these graphs to see the following details:

Field	Description
Destination/ Host	The destination host name or IP address to which requests were denied/ The host name or IP address of the host whose requests were denied
Protocol	The protocol used by the denied request
Hits	The number of times the request was generated
Time	The timestamp of the last time when the request was received
Message	The message generated when the request was denied

The **Top Denied Protocols** report shows the top protocols that have been denied requests for the selected time period.

Drill down from this graph to see the following details:

Field	Description
Host	The host name or IP address of the host whose requests were denied
Destination	The destination host name or IP address that denied the request
Hits	The number of times the request was generated
Time	The timestamp of the last time when the request was received
Message	The message generated when the request was denied

The **Top Security Events** pie-graph shows the top events generated with severity as Emergency, Critical, Alert, Error, or Warning.

Drill down from this graph to see the following details:

Field	Description
Host	The host name or IP address of the host generating denied events
Severity	The event severity of the event generated
Hits	The number of times the event was generated
Time	The timestamp of the last time when the event was generated
Message	The event message generated

Virus Reports

The **Virus Reports** section includes reports that show details on viruses that have been identified by the firewall. These reports help in identifying the top viruses and worms that have affected the network, analyze the extent of damage, and also track the source of the attack.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the csv icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Virus Sending Hosts** report shows the top source IP addresses or host names from which viruses have been sent, along with the protocol used to send the virus. The **Top Virus Affected Hosts** report shows the top destination IP addresses or host names that have been affected by viruses, along with the protocol that was used to receive the virus.

Drill down from these graphs to see the following details:

Field	Description
Virus	The name of the virus that was sent or received
Destination/ Host	The destination host or IP address to which the virus was sent/ The host or IP address that sent the virus
Severity	The severity level of the virus, as defined by the firewall
File	The name of the virus file that was sent or received
Hits	The number of times the virus was sent to or received by the same host
Subtype	The subtype of the virus, as defined by the firewall
Time	The timestamp when the virus was sent or received
Message	The virus message generated by the firewall

The **Top Protocols Used By Viruses** report shows the top protocols used by each virus. The **Top Viruses By Priority** report shows the top severities with which viruses have been sent.
Drill down from these graphs to see the following details:

Field	Description
Host	The host or IP address that sent the virus
Destination	The destination host or IP address to which the virus was sent
Severity/ Protocol	The severity level of the virus, as defined by the firewall/ The protocol used to send the virus
File	The name of the virus file that was sent or received
Hits	The number of times the virus was sent to or received by the same host
Subtype	The subtype of the virus, as defined by the firewall
Time	The timestamp when the virus was sent or received
Message	The virus message generated by the firewall

The **Top Virus Files** report shows the top virus files that have been sent. The **Top Virus with Status** report shows the status of the Top Virus. Drill down from these graphs to see the following details:

Field	Description
Virus	The name of the virus that sent this file
Host	The host or IP address that sent the virus file
Destination	The destination host or IP address to which the virus file was sent
Protocol	The protocol used by the virus to send this virus file
Severity	The severity level of the virus, as defined by the firewall
Hits	The number of times the virus file was sent to the same host
Subtype	The subtype of the virus, as defined by the firewall
Time	The timestamp when the virus file was sent
Message	The virus message generated by the firewall

Attack Reports

The **Attack Reports** section includes reports that show details of attacks that have been identified by the firewall. These reports help in identifying the top attackers, the top targets for the attacks and other details like protocol used, the priority of the attack and the status of the attack.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the csv icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Attackers** report shows the top source IP addresses or host names from which attacks are originating, along with the protocol used for the attack and the number of hits. The **Top Targets** report shows the top destination IP addresses or host names that have been attacked, along with the protocol used for the attack and the number of hits.

Drill down from these graphs to see the following details:

Field	Description
Attack	The name or id (as defined by the firewall) of the attack that was sent or received
Destination/ Host	The destination host or IP address to which the attack was sent/ The host or IP address that sent the attack
Severity	The severity level of the attack, as defined by the firewall
Hits	The number of times the attack was sent to or received by the same host
Subtype	The subtype of the attack, as defined by the firewall
Time	The time stamp when the attack was sent or received
Status	The status of the attack that was sent or received
Message	The attack message generated by the firewall

The **Top Protocols Used By Attacks** report shows the top protocols used by each attack. The **Top Attacks By Priority** report shows the top attacks classified based on priority like Alert, Emergency etc.

Drill down from these graphs to see the following details:

Field	Description
Host	The host or IP address that sent the attack
Destination	The destination host or IP address to which the attack was sent
Severity/ Protocol	The severity level of the attack, as defined by the firewall/ The protocol used to send the attack
Hits	The number of times the attack was sent to or received by the same host
Subtype	The subtype of the attack, as defined by the firewall
Time	The time stamp when the attack was sent or received
Status	The status of the attack that was sent or received
Message	The attack message generated by the firewall

The **Top Attacks with Status** report shows the status of the Top Attacks (ID or names) based on the number of hits. Drill down from this graph to see the following details:

Field	Description
Attack	The name or id (as defined by the firewall) of the attack that was sent or received
Host	The host or IP address that sent the attack file
Destination	The destination host or IP address to which the attack file was sent
Protocol	The protocol used by the attack to send this attack file
Severity	The severity level of the attack, as defined by the firewall
Hits	The number of times the attack file was sent to the same host
Subtype	The subtype of the attack, as defined by the firewall
Time	The time stamp when the attack file was sent
Status	The status of the attack that was sent or received
Message	The attack message generated by the firewall

Squid Proxy Reports

Squid Proxy Server Reports

Squid is a widely used proxy cache for Linux and UNIX platforms. Squid is usually used together with a firewall to secure internal networks from the outside using a proxy cache.

The **Squid Proxy Reports** section in Firewall Analyzer includes reports that are based on squid proxy cache logs. This section can be accessed from the left navigation pane or the **Reports** tab.

In order to generate squid proxy reports, you need to configure Firewall Analyzer to import the squid proxy logs at specific intervals.

The following reports are generated based on squid proxy cache logs:

- Top Talkers Report
- Site Details Report
- Squid Usage Summary

Apart from these reports, **Live Reports** are available for squid proxy servers also. The Live Report for each squid proxy server shows the traffic load across the server, over different time periods.

Top Talkers

The **Top Talkers** section includes reports that show the top hosts and protocols generating traffic through the squid proxy server.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the icon to export this report to PDF. Click on the csv icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top LAN Hosts** and the **Top LAN Users** graphs show the respective top hosts and top users whose requests have been processed by the squid proxy cache itself. The table below the graph shows the host name, IP address, or user name of the source, along with the protocol used, the number of hits, and the total traffic in bytes.

The **Top WAN Hosts** and the **Top WAN Users** graphs show the respective top hosts and top users whose requests could not be processed by the squid proxy cache. The table below the graph shows the host name, IP address, or user name of the source, along with the protocol used, the number of hits, and the total traffic in bytes.

The **Top Users (LAN + WAN)** shows the top values when the **Top LAN Users** and **Top WAN Users** records are combined. The table shows the User, the host name or IP address of the source from which he is conducting the conversation, the type of user (LAN or WAN) , the number of hits and bandwidth usage.

Drill down from each of the above graphs to see the following details:

Report	Description
Top Sites	The top web sites accessed by this user or host
Top Pages	The top web pages or URL's accessed by this user or host
Top Denied Web Pages	The top web pages that were denied for this user or host
Cache Usage - Cache Code	The cache usage by this user or host, based on cache code
Squid Usage - HTTP Status Code	The squid usage by this user or host, based on HTTP status code
Squid Usage - Peer Status	The squid usage by this user or host, based on peer status
Top Users/Hosts	The top users or hosts accessing the squid proxy through this host/user
Traffic Distribution - Working Hours	The amount of traffic that was generated during working hours - 10 a.m. to 8 p.m.
Traffic Distribution - Non-working Hours	The amount of traffic that was generated after working hours - 8 p.m. to 10 a.m.

Website Details

The **Website Details** section includes reports that show the top domains, web sites, and web pages that were accessed using the squid proxy server.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Top Web Sites** report lists the top web sites that were accessed through this squid proxy server. This report classifies web sites based on the number of bytes that were transferred by a single user. Drill down from this graph to see the following details:

Report	Description
Top Users	The top users and the respective hosts accessing this web site
Top Web Pages	The top web pages accessed within this web site
Top Denied Web Pages	The top web pages in this web site that were denied
Cache Usage - Cache Code	The cache usage by web pages in this web site, based on cache code

The **Top Domains** report lists the top domains that were accessed through this squid proxy server. Drill down from this graph to see the following details:

Report	Description
Top Users	The top users and the respective hosts accessing this domain
Top Web Pages	The top web pages accessed within this domain
Top Denied Web Pages	The top web pages in this domain that were denied
Cache Usage - Cache Code	The cache usage by web sites in this domain, based on cache code

The **Top Web Pages** report lists the top web pages or URL's that were accessed through this squid proxy server, along with the number of hits and the total traffic sent to each web page, in bytes. This report classifies web pages based on the number of bytes that were transferred by a single user.

The **Top Denied Users** report lists the top users whose requests were denied by this squid proxy server. Drill down from this graph to see the top denied requests for each user.

The **Top Denied Requests** report shows the top requests that were denied by the squid proxy server.

Squid Usage Summary

The **Squid Usage Summary** section includes information about the cache usage and squid usage of the squid proxy server.

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. To show more than ten values, the report uses only tables. Click on the 📄 icon to export this report to PDF. Click on the csv icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Cache Usage - Cache Code** report shows the top cache result codes triggered. This report help you analyze the efficiency and performance of the squid proxy server. A high number of TCP_DENIED hits for example, could indicate that most users in the network are trying to access unauthorized resources, or are simply unaware of present network security policies. Drill down from this graph to see the following details:

Report	Description
Top Hosts	The top hosts and users that triggered this cache result code
Top Web Pages	The top web pages that triggered this cache result code

The **Squid Usage - Peer Status Code** report shows the top peer status codes triggered. This report shows you the number of requests that were generated directly from the origin, and how many were passed from another source. Drill down from this graph to see the following details:

Report	Description
Top Hosts	The top hosts and users that triggered this peer status code
Top Web Pages	The top web pages that triggered this peer status code

The **Squid Usage - HTTP Status Code** report shows the top HTTP status codes triggered, like 200, 404, etc...

The **Squid Usage - HTTP Operation** report captures the various operations like get, post, connect, etc..

All the above reports classify values based on the number of times each code was triggered.

Radius Server Reports

RADIUS servers are responsible for receiving user connection requests, authenticating a user, and then returning all of the configuration information necessary for the client to deliver the service to the user. Radius Server Usage Reports are a valuable source for helpdesk troubleshooting purposes, and analyzing end user or group-based network access patterns.

The **Radius Server Reports** section in Firewall Analyzer includes reports that are based on Radius server logs. This section can be accessed from the left navigation pane or the **Reports** tab.

In order to generate Radius server reports, you need to configure your Radius server to export logs to Firewall Analyzer

The **Show** bar lets you choose the level of detail in the reports. By default, the top five values are shown. Click on the icon to export this report to PDF. Click on the csv icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The following reports are generated based on Radius server logs:

Report	Description
Top Radius Users	This report identifies top talkers based on the the number of bytes of traffic transferred through the Radius server in each session
Users with Maximum Concurrency	This report shows the users with the longest session duration, as accounted by the Radius server.
Request Distribution Trend - Hourly	This graph shows the trend of the average number of requests received by the Radius server every hour
Usage Summary	This report shows the summary of requests processed, and total traffic transferred through the Radius server

Trend Reports

Trend Reports analyze traffic over several time periods and present graphs that make analysis and forecasting a lot easier. Firewall Analyzer includes trend reports based on traffic generated, protocols used, and events triggered. Trend reports compare the current trend with the historical trend on an hourly, daily, and weekly basis. Historical trends show data from the time the server was started.

Firewall Analyzer includes three types of trend reports that are described in the following sections:

- Protocol Trend Reports
- Traffic Trend Reports
- Event Trend Reports

Protocol Trend Reports

The **Protocol Trend Reports** section includes reports that show trends in the amount of traffic generated using different protocol groups. Protocol trends help in identifying peak usage times for each protocol group, understanding user trends, and enforcing better policies to allow traffic from each protocol group.

Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Hourly Trend Comparison** reports for Web, Mail, FTP, and Telnet protocol groups compare the traffic generated using these protocol groups over the past day, with the traffic generated since the time the server was started.

The **Working Hour** and **Non-working Hour Traffic Trend** reports show the amount of traffic generated using each protocol group during working and non-working hours respectively, since the time the server was started.

Traffic Trend Reports

The **Traffic Trend Reports** section includes reports that show trends in the amount of traffic generated across the firewall. Traffic trends help in understanding peak usage times, enforcing better security policies, and planning for effective bandwidth upgrades. In a large enterprise with several firewalls, traffic trends can also help the network administrator to distribute the traffic load between firewalls to reduce response times and thereby enable better quality of service.

Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Hourly Trend Comparison** report compares the amount of traffic generated across this firewall over the past day, with the amount of traffic generated across this firewall since the time the server was started.

The **Weekly Trend Comparison** report compares the amount of traffic generated across this firewall over the past week, with the amount of traffic generated across this firewall since the time the server was started.

The **Working Hour** and **Non-working Hour Traffic Trend** reports show the amount of IN and OUT traffic generated across this firewall during working and non-working hours respectively, since the time the server was started.

Event Trend Reports

The **Event Trend Reports** section includes reports that show trends in the number of events generated across the firewall. Event trends help in identifying malfunctioning hosts and malevolent systems, that eventually lead to enforcing better security policies, and increasing network perimeter security.

Click on the 📄 icon to export this report to PDF. Click on the CSV icon to export this report to CSV format (comma separated values).

Below each graph click the **Hide Details** link to hide the table. Click the **Show Details** link to see the table again.

The **Hourly Trend Comparison** report compares the number of events generated across this firewall over the past day, with the number of events generated across this firewall since the time the server was started.

The **Weekly Trend Comparison** report compares the number of events generated across this firewall over the past week, with the number of events generated across this firewall since the time the server was started.

The **Working Hour** and **Non-working Hour Event Trend** reports show the number of events generated across this firewall during working and non-working hours respectively, since the time the server was started.

Custom Reports

Creating Report Profiles

Custom reports in Firewall Analyzer are grouped into report profiles, and listed under the **My Reports** category. A report profile can contain a combination of pre-defined and custom reports. The **My Reports** section is present in the **Reports** tab and the left navigation pane.

The process of creating a report profile includes several other tasks such as including and excluding log filters, and setting custom criteria for specific reports.

Creating a Report Profile

Click the **Add Report Profile** link to create a new report profile. You can click this link from the sub tab, the left navigation pane, or the **My Reports** section in the **Reports** tab.

Step 1: Select Devices and Filters

1. For **Report Profile Name**, enter a unique name for the report profile.
2. Select the devices (firewalls, squid, radius ...) to report on. If you want to report on all the devices sending logs to a specific syslog port, then select the **Select All Devices** check box.
3. You can specify the filters on log data, in the section **Choose the Filters**. Follow the instructions available for Setting Log Filters to know more about operations on Include and Exclude filters.
4. Click **Next** to continue to the next step of the wizard. Click **Cancel** to exit the wizard.

Step 2: Select Report Type and Schedule

This step lets you specify which reports to include as part of this report profile, and set up schedules to generate this report profile automatically.

1. From the list of **Available Reports**, select the reports that you want to include in this report profile. All the pre-defined reports are listed, along with custom reports that you have previously set up.

   Look up Creating Custom Criteria Reports to know more about adding a new report to this list

2. In the **Schedule & Email Options** section, choose a **Schedule Type** to schedule this report to be automatically generated at specific time intervals. If the **Email the Report** option is checked, the scheduled report will be generated and emailed as PDF to the **Mail Id** that is provided. You can use comma "," separator for multiple mail ids.

   The **Schedule Description** box describes each scheduling option selected.

   ⚠ You need to configure the mail server settings in Firewall Analyzer before setting up an email notification. You can do this from the **Setup the Mail-Server Details** link.

3. Click **Preview** to see how this report will look like, once it is set up. Click **Save** to save this report profile under the **My Reports** section. Click **Cancel** to exit the wizard.

Setting Log Filters

Include filters specify those criteria which the log data must meet in order to be included in the report. *Exclude* filters specify those criteria which the log data must meet in order to be excluded from the report. Apart from selecting specific filters to apply on a report, you can also add, select, edit, and delete filters in this step. Include and Exclude filters let you filter log data and show only specific details in the custom report. Once you have set filters, you can include or exclude them while creating custom reports.

Adding a New Filter:

1. Click the ✚ Add icon to add a new filter
2. In the popup window that opens, enter a unique name for the filter
3. Select the type of filter you are creating, whether its a **Include Filter** or an **Exclude Filter.**
4. In the **Include the following Protocols** drop-down, choose the protocols to be filtered
5. In the **Include the following IP/Hostname** drop-down, specify the IP addresses of the hosts to be filtered
6. In the **Include the following Destinations** drop-down, specify the IP addresses of destination address to be filtered
7. In the **Include the following Events** drop-down, choose the event priorities to be filtered
8. In the **Include the following Users** drop-down, specify the users to be filtered
9. Click **Finish** to create the new filter. Click **Cancel** to exit the wizard without saving the new filter.

Selecting a Filter:

1. Click the ↖ Select icon to select from the list of already created filters.
2. You can select a specific filter or **All filters** and then click the **Select** button. Click **Cancel** to exit the wizard without selecting.

Editing a Filter:

1. Click the ✎ Edit icon to edit an existing filter
2. Editing a filter affects all existing report profiles to which this filter is applied. If you still want to edit the filter, accept the warning message and proceed editing.
3. The wizard for editing the filter is similar to that for adding a new filter. Follow the same steps and click **Finish** to save the edited filter. Click **Cancel** to exit the wizard without saving the edited filter.

Removing a Filter:

1. Click the ✖ Remove icon to remove or delete an existing filter
2. Choose whether you would like to **Remove filter from the list** or **Remove it completely**
3. **Remove filter from the list** option will only remove the filter from this listing, but would still be available for selection. **Remove it completely** option will remove this filter permanently and affects all existing report profiles to which this filter is applied. If you still want to remove this filter completely, accept the warning message. The filter is removed, and all report profiles to which this filter is applied, are permanently modified to reflect the changes.

Creating Custom Criteria Reports

Firewall Analyzer lets you define custom criteria and set up new reports. These reports are added to the Available Reports list, in Step 3 of the **Add Report Profile** wizard.

1. In Step 3 of the **Add Report Profile** wizard, click the ✚ icon to add a new report
2. In the popup window that opens, enter a unique name for the report
3. In the *Report based on* selection, choose Protocol, URL, or Event depending on the report criteria you will specify.
4. In the *Graph Settings* tab, choose the following:
    1. The type of graph to be displayed, in the Graph Types drop-down list
    2. The attributes to be used for the X and Y axes of the graph, along with the labels to be displayed
    3. The attribute based on which all data will be grouped together, in the Grouping Criteria option
    4. The attribute based on which data will be sorted, in the Order By option
5. In the *Table Settings* tab, choose the values to be shown in the table of the report

Once you have selected all the required options, click **Apply** to include this new report in the Available Reports list. Select the checkbox next to this report to include it in a report profile.

You can click the ✖ icon at any time to delete a custom report from the Available Reports list.

Notifications

Creating an Alert Profile

An alert is triggered whenever an event matching a specific criteria is generated. An alert profile lets you define such specific criteria, and also notify you by email, when the corresponding alert is triggered.

Creating a New Alert Profile

Click the **Add New Alert Profile** link to create a new alert profile. You can find this link on the sub tab or in the **Alerts** box in the left navigation pane when the **Alerts** tab is selected.

Step 1:

1. Enter a unique name for the alert profile.
2. Choose the firewalls for which the alert needs to be triggered. Check the checkbox next to a firewall to select it. If you want to apply the alert profile to a group of firewalls sending logs to a specific syslog port, check the corresponding syslog server.
3. Define the criteria for which the alert needs to be triggered. You can set criteria based on the Severity, Protocol, Date, Received (in Bytes), Sent (in Bytes), Source, Destination, URL, Status, File Name, Rule, VPN, Virus, Attack, Protocol Identifies, Message, Duration (in seconds), or Record Type. Use the **Add Criteria** and **Remove Criteria** to specify more or fewer criteria for the alert.

Step 2:

1. Choose the **Alert Priority**. Alert priority can be High, Medium, or Low. This is a value that you set for the alert, for your reference.
2. Enter the threshold criteria, which is the number events that need to be generated within a time interval, in order to trigger the alert.
3. Choose the firewalls for which the threshold needs to be applied. If you choose **Each Firewall**, the alert will be triggered when each firewall crosses the threshold set in the threshold criteria above. If you choose **All Firewalls**, the alert will be triggered when all the firewalls, selected in Step 1, cumulatively cross the threshold.
4. Tick the checkbox next to **Notify by Email** to receive an email every time an alert matching this alert profile is triggered. Fill in the recipient email address in the **To** box. Emails can be sent to more than one email address by separating the email addresses using a comma (,).

⚠	You need to configure the mail server settings in Firewall Analyzer before setting up an email notification.

5. Finally click **Save Alert Profile** to save and activate this alert profile. Click **Back** to go back to Step 1. Click **Cancel** to return to the previous page.

Viewing Alerts

After setting up an Alert Profile, select the **Alerts** tab to see the list of alerts triggered. By default, the Alerts tab lists all the alerts triggered so far. The list shows the timestamp of the alert, the host which triggered it, the alert priority, and the status of the alert.

Viewing Alerts for an Alert Profile

The Alerts box on the left navigation pane lists all the alert profiles created so far. Click on each alert profile to view the corresponding list of alerts triggered.

The ✉ icon against an alert profile indicates that an email notification has been setup. The ⚡ icon indicates that the alert profile is currently enabled and active. To disable the alert profile, click on this icon. The alert profile is now disabled, and the ⚡ icon is shown. When an alert profile is disabled, alerts will not be triggered for that alert profile. To start triggering alerts again, click on the icon to enable the alert profile.

The **Alerts** tab lets you view alerts for various alert profiles set up. To manage alert profiles, click the **Alert Profiles** link in the **Settings** tab.

System Settings

Configuring System Settings

The **Settings** tab lets you configure several system settings for the server running Firewall Analyzer, as well as other settings.

The **Simulate** option sends sample firewall logs to Firewall Analyzer so that you can view reports without having to send actual firewall logs. At any time, click the **Stop Simulate** link to stop sending sample data.

The following is the the list of configuration options available under the System Settings section:

Setting	Description
Syslog Server Settings	Click this link to configure syslog servers to receive logs at different ports
Checkpoint Firewall Settings	Click this link to configure settings specific to CheckPoint firewalls
Alert Profiles	Click this link to view the alert profiles set up so far
Import Log Files	Click this link to import log files from the local machine or by FTP
Device Details	Click this link to view details of logs received from each device
Archived Files	Click this link to configure archiving intervals, or load an archived file into the database
Schedule Listing	Click this link to view the list of reports scheduled
Working Hour	Click this link to configure Working and Non-Working hour firewall event log collection pattern of the organization.
Customize Report	To customize the device specific reports to be shown in Device Tree and the Reports page.

The following is the the list of configuration options available under the Administration Settings section:

Setting	Description
Protocol Groups	Click this link to manage protocol groups
Intranet Settings	Click this link to configure intranets to identify internal and external traffic
User Management	Click this link to add, edit, or delete users in Firewall Analyzer
Mail Server Settings	Click this link to configure the mail server
Database Console	Click this link to access the database and execute queries
Server Diagnostics	Click this link to view system-related information for Firewall Analyzer

Simulating Firewall Logs

The **Simulate** option lets you test Firewall Analyzer with sample data before setting it up on your network. The sample data is taken from the **firewall_records.xml** file present in the *<FirewallAnalyzer_Home>/server/default/conf* directory on the server.

⚠	The **Simulate** option lets you view reports for firewalls only, and not squid proxy servers or Radius servers.

When you click the **Simulate** link from the welcome screen or the **Settings** tab, the syslog server in Firewall Analyzer starts receiving the sample data as logs. The server then analyzes this data and generates reports assuming this data to be actual firewall logs. As a result, you can view all the pre-defined firewall reports, create custom report profiles, and set up notifications just like you would when actual data is received.

At any time, click the **Stop Simulate** link from the **Settings** tab to stop sending the sample data to the server. However, data already sent to the server will be present until the database is reinitialized.

Managing Syslog Servers

The **Syslog Server Settings** page lets you manage the various virtual syslog servers set up to receive exported logs at different ports.

The default listener ports for the syslog server in Firewall Analyzer are **514** and **1514**. If your firewalls are exporting log files to either of these ports, you do not have to set up any virtual syslog servers.

The **Syslog Servers** table shows the various virtual syslog servers set up so far, along with their IP address, listener port, and status. You can delete a virtual syslog server by clicking the ✖ icon. Once a virtual syslog server is deleted, the corresponding listener port is also freed. You can also stop the syslog collection by clicking the ■ icon and restart the syslog collection by clicking on the ↻ icon.

Adding a New Syslog Server

The **Add Syslog Server** box lets you add a new virtual syslog server and begin listening on a new port for exported log files.

Enter a unique **SysLog Server Name** for the new virtual syslog server, and the listener port. The **Host Name/IP Address** field is currently not editable, and takes the IP address of the machine on which the Firewall Analyzer server is running.

Click **Add Syslog Server** to add this virtual syslog server, and begin listening for log files at the specified port.

Managing LEA Servers

The **CheckPoint Firewall Settings** link lets you manage the LEA servers that have been configured to connect to Check Point firewalls and access the log files.

The list of LEA servers configured, along with the respective LEA listener port and authentication details, is displayed.

Adding an LEA Server

Enter the host name of the LEA server and the port on which it has to connect to the Check Point firewall. The syslog server IP address is the same as that on which Firewall Analyzer is running. If you are using an unauthenticated connection, select the **Use Un-authenticated Login** checkbox.

Click **Add to LEA Server Lists** to add the LEA server.

💡	The Configuring Check Point Firewalls section includes detailed instructions on configuring Check Point firewalls for reporting in Firewall Analyzer

Managing Alert Profiles

The **Alert Profiles** link lets you manage all the alert profiles set up so far.

The **Add New Alert Profile** link lets you create a new alert profile.

The Alert Profiles table lists all the alert profiles, along with the priority, and the number of times each alert has been triggered. Click an alert profile to see the corresponding list of alerts triggered. The ⚡ toggle icon lets you enable or disable an alert profile and correspondingly start or stop triggering alerts for the same.

The ✖ icon lets you delete an alert profile. Once deleted, the alerts associated with this profile are also deleted from the database. The ✉ icon indicates that an email notification has been set up for this alert profile. The corresponding email address is also displayed next to this icon.

Importing Log Files

The **Import Log Files** link lets you import a log file from the local machine or remotely, through FTP. The **Imported Log Files** page shows you the list of log files imported, along with details such as the host from which it was imported, and the status of the import. Importing of archived files (.gz format) created by Firewall Analyzer and zipped log files (.zip format) are also supported.

> Use this option to import log files from squid proxy servers.

Click the ✖ icon to delete an imported log file from the database.

Importing a Log File

1. Click the **Import Log File** link to import a new log file.
2. Choose **Local Host** if the log file is present in the local machine from which you are accessing the Firewall Analyzer server.
   Click **Browse** to locate the log file.

   > HTTP protocol is used to retrieve log records from the local machine.

3. The option **Ignore UnParsed/Junk Record(s)** enables the Firewall Analyzer to skip those records in the imported log file, that are in unsupported format and continue with parsing the subsequent supported records in the file. If not selected, the Firewall Analyzer will not parse the entire log file even if one record contains unsupported log format. Then click **Import** to import the log file into the database.
4. Choose **Remote Host** if you need to import the particular log file or the entire directory containing the log files from a remote location on the network.
   1. Enter the remote host's hostname or IP address, and the FTP user name and password.
   2. Enter the time interval after which Firewall Analyzer should retrieve new log files.
   3. Enter the location on the remote machine where the log file or the entire directory containing the log files is present. You can click the **List Remote Files** link to locate the file on the remote computer.
5. Finally click **Import** to import the log file into the database.

The supported formats for imported log files is shown below the **Location** box. We also support importing of archived files (.gz format) created by our Firewall Analyzer.
If you are importing an unsupported log file, a warning message is shown. You can still import the file, but records will show up when the 📊 icon is clicked on the sub tab.

> If you have selected the **Ignore UnParsed/Junk Record(s)** while importing the logs, then records **will not** be show up when the 📊 icon is clicked on the sub tab.

The time taken to import a log file depends on its file size. Once the file has been imported successfully, the device from which it was imported is listed in the appropriate category, and the reports are generated automatically.

The **Imported Log Files** table shows the list of all log files imported so far. The 🖥 icon is displayed if logs have been imported from the local machine. The 🖥 icon is displayed if logs have been imported from a remote machine. Click this icon to see the remote host details, and file details for the log file imported. Click the ⚡ toggle icon to enable or disable collecting logs from this device after the specified time interval. Click the ✖ icon to delete all log files imported from this device.

Archiving Log Files

Firewall Analyzer archives the logs received from each device, and zips them in regular intervals. The **Archived Files** page files that have been archived for each device, along with options to load the file into the database, and delete the file.

Loading Archived Files

The **Archived Files** page lists the files that have been zipped for each device, along with the archived time, file size, and archiving status.

To load an archived file into the database, click the **Load into DB** link against the device for which you need to see archived data. Once the file is fully loaded into the database, you can search for data in the archives, and view specific information.

Click the ✖ icon against an archived file to delete it. Once deleted, the archived data cannot be retrieved.

Viewing Data from Archived Files

Once the archive is fully loaded into the database, click the **Report** link to search for specific data in the archive. In the popup window that opens, enter the criteria for the data, such as the firewall, user name, protocol, etc. You can enter a maximum of three criteria.

Choose the time interval for which you want to see the data that meets all the criteria. Click **Generate Report** to view the records that match the criteria that you have specified.

Changing Archive Settings

Click the **Archive Settings** link to change the archiving intervals or to disable archiving. In the popup window that opens, uncheck the **Enable Archiving** checkbox to disable file archiving.

The archiving options available are described below:

Attribute	Default Value	Description
File Creation Interval	12 hours	The time interval after which a log file is created for each device from which logs are collected.
Zip Creation Interval	24 hours	The time interval after which log files created for each device, are zipped to save disk space.

By default the Archive Location for the firewall logs in Firewall Analyzer is <FirewallAnalyzerHome>\server\default\archive, you can change this location by enabling the **Change Archive Location** and providing the location of your choice.

Click **Zip Now** to create a zipped file with the currently available log files. Click **Save** to save the archiving options, if you have changed them. Click **Close** to close the Archive Settings box.

Viewing Device Details

The **Device Details** link shows you the various devices from which logs are collected in Firewall Analyzer.

The **Supported Logs Received** table shows all the devices from which logs supported by Firewall Analyzer, are received, along with the timestamp of the last received log file, the syslog port, and the current status of log collection.

The W icon indicates that this firewall is exporting logs in the WELF format. The icon indicates that the device is a Squid proxy server. Click on the icon next to a device to change the device name or the link speed values.

Click the ✕ icon to delete the device from the database. All logs collected from that device will also be deleted.

The **Unsupported Log Record Details** table shows all the devices from which logs that are not supported by Firewall Analyzer are received.

Click the **View Record** link to view the first few lines from the unsupported log record. Click the **Tell Us** link to open a popup window, through which you can send a mail to the Firewall Analyzer Technical Support team telling us about the unsupported log format. Type the relevant details, and click **Send Mail** to send the message. The Technical Support team will get back to you with more details about the unsupported log format, and how we can help you.

The **Schedules Executed** table shows the schedules that have run so far, along with the user that executed the schedule, the report profile the schedule was associated with, and the status of execution of the schedule.

Scheduling Reports

Once you have created a custom report profile, you can set up schedules to run the report automatically at specified time intervals. You can also configure Firewall Analyzer to automatically email the report once it runs.

> Scheduled reports are generated and emailed only as PDF files. If you are viewing PDF reports on a Windows machine, make sure you have Adobe Acrobat Reader installed.

Click the **Schedule Listing** link under the **Settings** tab takes you the All Schedules page to view the list of reports that have been scheduled so far. The list shows all the schedules that have been set up so far, along with the report profile they are associated with, the type of schedule, and options to delete the schedule.

Click the ✖ icon to delete a schedule. The report profile associated with this schedule will no longer be generated automatically at the specified time interval.

The ⏱ icon against a schedule is a toggle icon used to enable or disable a schedule. When the ⏱ icon is displayed, the schedule is enabled, and reports will be generated automatically for that schedule. Click the ⏱ icon to disable the schedule. The ⏱ icon is displayed indicating that the schedule is currently disabled. Reports will not be generated automatically for this schedule.

Creating a New Schedule

Click the ➕ icon or the **New Schedule** link to add a new schedule. In the Add New Schedule page that comes up, enter the following details:

Attribute	Description
Task Name	Enter a unique name to identify this schedule
Profile Name	Choose the report profile to which this schedule has to be applied. All the report profiles that have been created are listed.
Mail Id	The first time a schedule is associated with a report profile, you need to enter the e-mail address to which the report has to be sent. Enter multiple e-mail addresses separated by a comma(,).
Hourly*	If you want to schedule this report to run every hour, enter the date and time after which this report has to run every one hour
Daily*	If you want to schedule this report to run every day, enter the date and time after which this report has to run every one day
Weekly*	If you want to schedule this report to run every week, enter the date and time after which this report has to run every one week
Monthly*	If you want to schedule this report to run every month, enter the date and time after which this report has to run every one month
Once only*	If you want to run this report only once, enter the date and time when the report has to be generated

**Choose from any one of these options*

Once you have chosen all the required values click **Save Task** to save and activate the new schedule. Click **Cancel** to return to the All Schedulespage.

Working Hour Configuration

Here you can configure the Working and Non-Working hour patterns of your enterprise. This will help you to distinguish between the working and non-working hour firewall log trends. By default, 10 - 20 Hours are considered as Working Hours and the remaining hours are considered as Non working Hours.

Two options are provided for configuring the working hour patterns.

- **General**

  Here you can mention the **Start Time** and **End Time** for your official working hours, and all hours outside the given range is considered as non-working hours.

- **Advanced**

  This option provides more customized working hours classification.For example, you may mention intermittent working hours like 8-12, 15-18, 19, 20, 21 Hours. Which means your non-working hour are 12-15 Hours and 21-8 Hours.

Working hour and Non-Working hour traffic details for external hosts (hosts outside the LAN) will not be available in the Firewall Analyzer reports.

Report View Customization

Here you can customize the device specific reports to be shown in Device Tree and the Reports page.

For each of the selected device, you are provided with the option of selecting from the default **Available Reports** the most required list of reports and move it to the **Selected Reports**. And only these selected reports would be listed in the Device Tree and the Reports page for this device.

The report view customization for the selected device can be applied on the selected device alone by clicking **Apply for Selected Device**. And, if you would like the report view customization for the selected device to applied for all other devices too then click **Apply for All Device.**

Admin Settings

Setting up the Mail Server

You need to configure the mail server on EventLog Analyzer in order to receive email alert notifications and scheduled reports.

Click the **Mail Server Settings** link to edit the mail server settings. Enter the following details:

Field	Description
Outgoing Server Name	Enter the name of the SMTP server on your network which is used for outgoing emails.
Port	Enter the port used by the SMTP server. Usually this is 25.
Requires Authentication	If your SMTP server requires you to authenticate yourself before sending an email, check this option. Otherwise leave it unchecked. * The below two fields are active only when this checkbox is checked.
User Name*	Enter the user name used to authenticate email sending from this machine.
Password*	Enter the corresponding password for the typed user name.

After all the details have been filled in, click **Save Changes** to save the mail server settings.

💡	If the mail server is not configured, you will see an error message when you are setting up an email alert notification or scheduling a report to be emailed automatically. Click the **Configure Mail Server now** link inside the error message to configure the above settings from the opened popup window.

Managing Protocol Groups

A protocol group is a set of related protocols typically used for a common purpose. The **Protocol Groups** link lets you define protocols as well as protocol groups, so that you can identify traffic that is unique to your enterprise. Most of the common enterprise protocols are already included in Firewall Analyzer under appropriate groups.

Some of the important protocol groups include the following:

Protocol Group	Protocols Included	Description
Web	HTTP, HTTPS, Gopher	Includes protocols used to access IP traffic (the Internet)
Mail	POP, SMTP, IMAP	Includes protocols used to send or receive e-mail traffic
FTP	FTP, TFTP, FTPS	Includes protocols used to transfer files through FTP
Telnet	telnet	Includes protocols used to access telnet services

Click the **Protocol Groups** link to view the list of protocol groups and the corresponding protocols. The **View by Group** box lets you view the list, one protocol group at a time.

The **Others** protocol group contains all the protocols that are not assigned to any group.

	Some firewalls interpret protocols at Layer 4(Application Layer), which means that a combination of port and protocol is identified as an application, and written into the log file. For example, *tcp* protocol on port *80* is identified as *http* traffic. Hence *http* is shown in the Protocols column. Other firewalls interpret protocols at Layer 3 only, which means only the port and protocol values are written into the log file. Hence, in the same example, *tcp/80* is shown in the Protocols column.

Operations on Protocols

Click the ✕ icon next to a protocol to delete it from the protocol group. Once a protocol is deleted, all the database records related to that protocol will be deleted. Click the ↱ icon to move a protocol from the current protocol group to another.

Click the **Add Protocol** link or the ✚ icon next to it to add a new protocol, and assign it to a protocol group. Remember to enter the protocol value exactly as it appears in the log file. If you want to add it to a new protocol group, select the **New Group** option, and enter the name of the new protocol group.

	When you see the ? icon next to the *Unassigned* protocol group on the Dashboard, you need to add the protocols and assign them to protocol groups in this way.

Operations on Protocol Groups

Click the **Add Protocol Group** link or ✚ icon next to it to add a new protocol group. In the popup window that opens, enter a unique group name, and a short description. From the list of protocols currently not assigned to any protocol group, choose the protocols to be included in this protocol group. Please note that a protocol can belong to only one protocol group at a time.

Select the protocol group from the list and click the **Edit Protocol Group** or the ✎ icon to edit the properties of that protocol group. In the popup window that opens, you can edit the protocol group's description, add currently ungrouped protocols, or remove existing protocols from this protocol group.

To delete a protocol group, select the protocol group from the list and click the **Delete Protocol Group** link or the ✕ icon next to it. The protocol group is deleted, and all associated protocols are put in the **Others** protocol group.

Adding Different Users

Click the **User Management** link to create and manage the different users who are allowed to access the Firewall Analyzer server.

The different types of users and their respective privileges are described in the table below:

User	Description
Administrator	This user can do all operations including configuring syslog servers, setting up file archiving, adding additional users, and more
Operator	This user can do all operations **except** adding more users, and managing existing users
Guest	This user can only generate reports, view device details, and view alerts triggered so far

By default, an Administrator user with username as **admin** and password as **admin**, and a Guest user with username **guest** and password **guest** are already created.

Adding a New User

Click the **Add New User** link to add another user to access Firewall Analyzer. Enter the new user's username, password, access level, and default e-mail address.

Click **Add User** to add this user to the list of users accessing Firewall Analyzer.

Editing User Details

If you have logged in as an Administrator user, the User Management page lists all the users created so far. Click the user's username to view the respective user details. You can change the password, access level, and the default e-mail address for this user.

If you have logged in as an Operator or Guest user, click on the **Account Settings** link to change your password and default e-mail address.

Once you are done, click **Save User Details** to save the new changes.

Viewing Login Details

If you have logged in as an Administrator user, click the **View** link against a user to view the corresponding login details. The **Login Details** page shows the remote host IP address from which the user logged on, the timestamp of the login, and the duration of the session.

Accessing the Database

Firewall Analyzer lets advanced users access the in-built database and run standard queries.

Click the **Database Console** link to open the Database Console page. In the prompt window displayed, enter the query to be executed.

Remember the following when executing a query:

- Table names and table columns are case-sensitive.
- For SELECT queries, set the row limit between 1 and 500. Default row limit is 10.

⚠	Keep in mind that you are accessing the database directly at your own risk. Any update or delete operations will result in loss of data.

Setting up Intranets

Firewall Analyzer includes the option to specify networks, or a range of IP addresses to identify machines behind a firewall. This setup is identified as the Intranet. By adding the machines or IP addresses that are located on the LAN, you can identify and distinguish between traffic that is generated internally within the LAN, and traffic that is coming from, or destined outside the LAN.

Click the **Intranet Settings** link to define intranets. The Intranet Settings page comes up.

- To designate an entire IP network as an Intranet, select **IP Network** from the list, and enter the network IP address and the corresponding Net Mask value.
- To include a single host in the Intranet, select **IP Address** from the list, and enter the IP address of the host.
- To designate a range of IP address as the Intranet, select **IP Range** from the list, and enter the starting IP address and the ending IP address.

> *For Example* : If you have three private **IP Network** (say) 10.8.0.0, 10.9.0.0, and 10.10.0.0, each with Net Mask: 255.255.0.0, then instead of adding them separately, we would recommend you to give the entire private IP network : 10.0.0.0 with Net Mask 255.0.0.0, as this would improve the performance of Firewall Analyzer. The same is recommended for **IP Range** too, where you can mention Start IP: 10.0.0.0, End IP: 10.255.255.255 .And this is applicable to Class B & Class C networks too!

You can specify multiple intranets by clicking the **Add** button. Once you are done, click **Save Settings** to activate the new settings.

Viewing Server Diagnostics

Click the **Server Diagnostics** link to see server-specific device information. This information will be useful while troubleshooting the server or reporting a problem.

The various information boxes on this page are described in the table below:

Box	Description
License Information	This box shows details about the license that is currently applied.
System Information	This box shows device information for the Firewall Analyzer server
Installation Information	This box shows details about the Firewall Analyzer installation on the server machine
JVM Memory Information	This box shows statistics on the amount of memory used by the JVM

Changing Account Settings

Click the **Account Settings** link under the **Settings** tab to change the default password and e-mail address set for this account. You cannot change the account's user name or access level.

Once you have made the required changes, click **Save User Details** to save the changes. Click **Cancel** to return to the default **Settings** tab.

📝	This option is visible only for users with **Guest** or **Operator** access level

Using Ask ME

The **Ask ME** tab offers a quick way to see just the reports that you need, without having to create a new report profile, or drilling down through the pre-defined reports.

Ask ME enables managers and other non-technical staff to answer simple but critical questions about bandwidth usage and network security.

The Ask ME tab shows a series of questions. In Step 1, select the area of interest - bandwidth usage, firewall rules, etc. If you are not sure, leave it to the default **All Questions** option.

In Step 2, select the appropriate question for which you need an answer. Then click the **Get the Answer** button.

The report corresponding to the question selected is now generated and displayed.

If you want more questions to come up in the Ask ME tab, click the **Tell us here** link. In the popup window that opens, enter the question and describe it shortly. Once you are done, click **Send**.

The Firewall Analyzer Technical Support team will analyze your question, and if found valid, will include it in upcoming releases of Firewall Analyzer.

Contacting Technical Support

The **Support** tab gives you a wide range of options to contact the Technical Support team in case you run into any problems.

Link	Description
Request Technical Support	Click this link to submit a form from the Firewall Analyzer website, with a detailed description of the problem that you encountered
Create Support Information File [SIP]	Click this link to create a ZIP file containing all the server logs that the Technical Support team will need, to analyze your problem. You can then send this ZIP file to support@fwanalyzer.com or upload the ZIP file to our ftp server by clicking on Upload to **FTP Server**, in the pop-up window provide your E-Mail id and browse for the zipped SIP file and then press Upload.
Troubleshooting Tips	Click this link to see the common problems typically encountered by users, and ways to solve them
User Forums	Click this link to go to the Firewall Analyzer user forum. Here you can discuss with other Firewall Analyzer users and understand how Firewall Analyzer is being used across different environments
Need a Feature	Click this link to submit a feature request from the Firewall Analyzer website
Toll-free Number	Call the toll-free number +1 888 720 9500 to talk to the Firewall Analyzer Technical Support team directly

The Support tab also displays the latest discussions in the Firewall Analyzer user forum.

At any time, you can click the **Feedback** link in the top pane, to send any issues or comments to the Firewall Analyzer Technical Support team. You can also send an email to support@fwanalyzer.com to let us know about your problem

Tips and Tricks

Frequently Asked Questions

For the latest list of Frequently Asked Questions on Firewall Analyzer, visit the FAQ on the website or the public user forums.

General Product Information [Show/Hide All]

1. Is a trial version of Firewall Analyzer available for evaluation?

   Yes, a 30-day free trial version can be downloaded from the website at http://www.fwanalyzer.com/

2. Does the trial version have any restrictions?

   The trial version is a fully functional version of Firewall Analyzer. When the trial period expires, you cannot restart the server.

3. Do I have to reinstall Firewall Analyzer when moving to the fully paid version?

   No, you do not have to reinstall or shut down the server. You just need to enter the new license file in the Upgrade License box.

4. What other devices can Firewall Analyzer report on?

   Apart from reporting on most enterprise firewalls, Firewall Analyzer can also analyze logs and generate specific reports on Squid Proxy servers, and Radius servers.

5. I don't have a firewall, a proxy server, or a Radius server. Can I still use this product?

   You can still use Firewall Analyzer to simulate firewall logs and see how reports will look like when real-time data is used. Click the **Simulate** link in the **Settings** tab to begin sending sample log files to Firewall Analyzer.

6. How many users can access the application simultaneously?

   This depends only on the capacity of the server on which Firewall Analyzer is installed. The Firewall Analyzer license does not limit the number of users accessing the application at any time.

7. Firewall Analyzer runs in a web browser. Does that mean I can access it from anywhere?

   Yes. As long as the web browser can access the server on which Firewall Analyzer is running, you can work with Firewall Analyzer from any location.

8. How secure is the data that is sent to the web browser over the Internet?

   Data sent from Firewall Analyzer is normally not encrypted and hence is readable if intercepted.

9. How do I buy Firewall Analyzer?

   You can buy Firewall Analyzer directly from the AdventNet Online Store, or from a reseller near your location. Please see the website at http://www.fwanalyzer.com/ for more information on purchasing options.

10. Is there a limit on the number of users or web sites that I can monitor?

    There is no license restriction on the number of users or web sites that you can monitor. However, you may face performance issues when using lower end machines to run Firewall Analyzer.

Installation [Show/Hide All]

1. What are the recommended system requirements for Firewall Analyzer?

   It is recommended that you install Firewall Analyzer on a machine with the following configuration:
   * Processor - Pentium 4 - 1.5GHz
   * Disk Space - 100MB * RAM - 512MB
   * Operating System - Windows 2000/XP, Linux 8.0/9.0
   * Web Browser - Internet Explorer 6.0, or Mozilla Firefox 1.0

   Look up System Requirements to see the minimum configuration required to install and run Firewall Analyzer.

2. Does the installation of Firewall Analyzer make any changes to the firewall server configuration?

   The installation of Firewall Analyzer does not make any changes to the firewall server configuration.

3. Can I install Firewall Analyzer as a root user?

   Firewall Analyzer can be started as a root user, but all file permissions will be changed, and later you cannot start the server as another user.

4. When I try to access the web client, another web server comes up. How is this possible?

   The web server port you have selected during installation is possibly being used by another application. Configure that application to use another port, or change the Firewall Analyzer web server port.

5. Is a database backup necessary, or does Firewall Analyzer take care of this?

   The archiving feature in Firewall Analyzer automatically stores all logs received in zipped flat files. You can configure archiving settings to suit the needs of your enterprise. Apart from that, if you need to backup the database, which contains processed data from firewall logs, you can run the database backup utility, BackupDB.bat/.sh present in the <FirewallAnalyzer_Home>/troubleshooting directory.

Configuration [Show/Hide All]

1. How do I see session information of all users registered to log in to Firewall Analyzer?

   The session information for each user can be accessed from the User Management page. Click the View link under Login Details against each user to view the active session information and session history for that user. Look up User Management for more information on users in Firewall Analyzer

2. How do I configure my firewalls to produce WELF log files?

   Firewalls usually need to be configured specifically to generate log files in WELF. The Configuring Firewalls section includes configuration instructions for some of the firewalls supported by Firewall Analyzer.

3. My firewall cannot export logs. How do I configure Firewall Analyzer to report on my firewall?

   You can set up Firewall Analyzer to import the logs from the firewall at periodic intervals

4. Does Firewall Analyzer store raw logs?

   Raw logs are archived periodically, and stored as zipped flat files. You can load these archived log files into Firewall Analyzer at any time and generate reports based on them.

Reporting [Show/Hide All]

1. Why am I seeing empty graphs?

   Graphs are empty if no data is available. If you have started the server for the first time, wait for at least one minute for graphs to be populated.

2. What are the types of report formats that I can generate?

   Reports can be generated in HTML, CSV, and PDF formats. All reports are generally viewed as HTML in the web browser, and then exported to CSV or PDF format. However, reports that are scheduled to run automatically, or be emailed automatically, are generated only as PDF files.

3. Are IP addresses automatically resolved?

   IP addresses are automatically resolved by connecting to the network DNS server.

4. Why are some traffic values shown as 0.0MB or 0.00%?

   Since Firewall Analyzer processes log files as and when they are received, traffic values of 0.0MB or 0.0% may be displayed initially when the amount of traffic is less than 10KB. In such a case, wait until more data is received to populate the report tables.

5. Why do I see zero results for kilobytes transferred in the reports for Check Point firewall?

   This could be happening because bandwidth information is not being captured in the log file. Ensure that your Check Point firewall has been configured to generate both regular and accounting log files. While regular log files contain information regarding firewall activity, the accounting log file contains the bandwidth and session information. Please refer the Configuring Check Point Firewalls section for help on creating the accounting log file.

6. What are the different formats in which reports can be exported?

   Reports can be exported as PDF or CSV files. However, reports are emailed only as PDF files.

7. Why do the intranet reports show zero results?

   Verify if intranets have been configured correctly. If you have specified IP addresses that are not actually behind the firewall, you will get zero values in the reports.

8. Why don't trend reports take time values or top-n values into account?

   Trend reports show historical data for the corresponding traffic statistics shown in the report. Hence time changes from the Global Calendar, or top-n value changes from the **Show** bar on the report, do not affect these reports.

Troubleshooting Tips

For the latest Troubleshooting Tips on Firewall Analyzer, visit the Troubleshooting Tips on the website or the public user forums.

General

1. Where do I find the log files to send to Firewall Analyzer Support?

   The log files are located in the *<FirewallAnalyzer_Home>/server/default/log* directory. Typically when you run into a problem, you will be asked to send the **serverout.txt** file from this directory to Firewall Analyzer Support.

2. Internet Explorer says "Error opening this document. File cannot be found" when I try to open an exported PDF report.

   Internet Explorer throws this error when you try to open an exported PDF report in the web browser itself. This is a known issue, and we are working on resolving it. For now, save the report to your local machine, and open it using the regular PDF software that you use (Adobe Acrobat Reader or xpdf)

3. I am having a Cisco PIX, but I only see Traffic IN and not Traffic OUT?

   - You need to configure your Intranets in order to separate inbound and outbound traffic. The Inbound Outbound Traffic report will show the traffic details about inbound traffic (traffic coming into LAN) and outbound traffic (traffic going out of LAN) of the firewall.When configured, the Inbound Outbound Traffic Reports shows you which hosts and what protocol groups have been contributing the most traffic on either side of the firewall. Please follow the instructions available for Setting Up Intranets.
   - Typical firewall logs are in the following format: *16.1.1.1 www.yahoo.com 10 bytes 1MB* (i.e. Source-IP Destination-IP Bytes-Sent Bytes-Received). But Cisco PIX does not provide a split-up of bytes-sent and bytes-received, but just provides a cumulative BYTES info. In most of the cases/protocols, RECEIVED will be more than SENT with respect to the source who originated the transaction. So we assume BYTES in Cisco PIX as RECEIVED. And in the case of FTP, Cisco PIX provides another log to identify the direction of the traffic. In that case, based on FTP put/get, we will determine whether the traffic is SENT or RECEIVED.

Installation

1. Firewall Analyzer displays "`Enter a proper AdventNet license file`" during installation.

   This message could be shown in two cases:

   Case 1: Your system date is set to a future or past date. In this case, uninstall Firewall Analyzer, reset the system date to the current date and time, and re-install Firewall Analyzer.
   Case 2: You may have provided an incorrect or corrupted license file. Verify that you have applied the license file obtained from AdventNet, Inc.

   If neither is the reason, or you are still getting this error, contact licensing@adventnet.com

2. When I try to access the web client, another web server comes up. How is this possible?

   The web server port you have selected during installation is possibly being used by another application. Configure that application to use another port, or change the Firewall Analyzer web server port.

Startup and Shut Down

1. MySQL-related errors on Windows machines.

   Probable cause: An instance of MySQL is already running on this machine

   Solution: Shut down all instances of MySQL and then start the Firewall Analyzer server.

   Probable cause: Port 33336 is not free

   Solution: Kill the other application running on port 33336. If you cannot free this port, then change the MySQL port used in Firewall Analyzer.

2. Firewall Analyzer displays "`Port 8500 needed by Firewall Analyzer is being used by another application. Please free the port and restart Firewall Analyzer`" when trying to start the server.

   Probable cause: The default web server port used by Firewall Analyzer is not free.

   Solution: Kill the other application running on port 8500. If you cannot free this port, then change the web server port used in Firewall Analyzer.

Reporting

1. Why am I seeing empty graphs?

   Probable cause: Graphs are empty either because there is no traffic is passing through the firewall or if firewall traffic is not sufficient enough to populate the reports table of Firewall Analyzer.

   Solution: If you are starting Firewall Analyzer for the first time or if you are shutting down and restarting Firewall Analyzer, it will wait for the reports table to be populated with 5000 log records for the first time. From the next time onwards, Firewall Analyzer will populate reports table once in 7 minutes or once it receives the next 5000 records, whichever is earlier. You can check for the number of records received in " Packet Count " icon shown in top right corner in client UI. This will list out the details like the number of logs received and also the last received log time. It is better to run the server continuously and check whether 5000 records are collected. Do not stop and restart the server in-between!

   Moreover, for viewing the already collected log records in the reports, kindly do the following:

   1. Login into Firewall Analyzer client UI. You will be seeing the Dashboard page.
   2. Replace the URL shown in your browser with the following URL. *http://localhost:8500/fw/genreport.do*
   3. Wait for sometime. Once the reports are generated an empty page will be shown.
   4. Now remove *genreport.do* from the URL and just type *http://localhost:8500/fw* alone.
   5. Now you will be able to see the report data.

2. I can't see the Live Reports for my SonicWALL firewall

   You cannot see Live Reports for SonicWALL firewalls because the time duration attribute is not supported in the SonicWALL log files.

3. Why are some traffic values shown as 0.0MB or 0.0%?

   Since Firewall Analyzer processes log files as and when they are received, traffic values of 0.0MB or 0.0% may be displayed initially when the amount of traffic is less than 10KB. In such a case, wait until more data is received to populate the report tables.

4. Why do I see zero results for kilobytes transferred in the reports for Check Point firewall?

   This could be happening because bandwidth information is not being captured in the log file. Ensure that your Check Point firewall has been configured to generate both regular and accounting log files. While regular log files contain information regarding firewall activity, the accounting log file contains the bandwidth and session information.

5. Why do the Intranet Reports show zero results?

   Verify if intranets have been configured correctly. If you have specified IP addresses that are not actually behind the firewall, you will get zero values in the reports.

6. Why doesn't Trend Reports take time values or top-n values into account?

   Trend reports show historical data for the corresponding traffic statistics shown in the report. Hence time changes from the Global Calendar, or top-n value changes from the **Show** bar on the report, do not affect these reports.

7. My firewall is sending WELF logs, but the reports do not show any URL information?

   Firewall Analyzer checks for the entry "**arg=your URL**" in the firewall logs to populate and show URL in report data. If this entry is not present in the firewall logs then the reports wouldn't be showing any URL information.

Configuring Firewalls

Firewall Analyzer listens at the default ports for exported log files. The following is a list of firewalls and versions for which configuration instructions are included. Click the firewall name to see the corresponding configuration instructions.

Firewall Name	Version Numbers
Check Point	log import from most versions and LEA support for R54 and above
Cisco Systems	PIX Secure Firewall v6.x PIX Secure Firewall v7.x *(Cisco Firewall Service Module (FWSM) is supported)*
FortiNet	FortiGate Family
SonicWALL	TELE, SOHO, PRO, GX v4.10, 5.x, 6.x

Configuring Check Point Firewalls

Firewall Analyzer supports log import froms most versions and LEA support for R54 and above.

Determining the Check Point Version Number

To determine the version number of the Check Point that you are running, use the following command:

```
$FWDIR/bin/fw ver
```

where *$FWDIR* is the directory where Check Point is installed.

Pre-Requisites

You need to do the following in Smart Dashboard of Check Point Firewall.

Changes in Smart Dashboard :

1. Open the "Smart Dashboard" where all the rules will be displayed. Set the "Track" value as "Account" instead of "log". This can be done by right clicking on "Track" value for each rule and select "Account". When this is set to "Account" the CheckPoint firewall will log the information regarding bytes.
2. After setting the "Track" value as "Account"for all the rules, please re-apply all the policies.

There are two ways of obtaining logs from Checkpoint firewall:

- Configuring LEA (Log Extraction API) Connection
  (or)
- Import of Check Point Log Files

Configuring LEA Connection

The following instructions will help you set up an authenticated or unauthenticated connection between Firewall Analyzer and the Check Point Management Server. For additional information please refer the Check Point documentation or contact Check Point technical support.

For managing the LEA servers the configurations that needs to be done for the different check point firewalls are explained below:

- Setting up an Unauthenticated LEA Connection
- Setting up an Authenticated LEA Connection for 4.*x*
- Setting up an Authenticated LEA Connection for NG
- The LEA Configuration File

Setting up an Unauthenticated LEA Connection

Follow the steps below to configure an unauthenticated connection from the Check Point firewall:

1. In the *FWDIR\conf* directory on the computer where the Check Point Management Server is installed, edit the `fwopsec.conf` file to include the following line:
   ```
   lea_server port 18184
   lea_server auth_port 0
   ```

2. Restart the firewall service
   [4.1] `fwstop ; fwstart`
   [NG] `cpstop ; cpstart`
3. Add a rule to the policy to allow the port defined above `port 18184` (assuming default LEA connection port) from the Firewall Analyzer machine to the Check Point Management Server
4. Install the policy

Adding to LEA Server Lists on Firewall Analyzer

Once this unauthenticated LEA connection has been set up, follow the instructions for Adding an LEA Server to the Firewall Analyzer.

Setting up an Authenticated LEA Connection to v4.x

Follow the steps below to configure an authenticated connection from the Check Point v4.*x* firewall:

1. In the *FWDIR\conf* directory on the computer where the Check Point Management Server is installed, edit the `fwopsec.conf` file and define the port to be used for authenticated LEA connections:
```
lea_server port 0
lea_server auth_port 18184
lea_server auth_type auth_opsec
```
2. Restart the firewall service
```
fwstop ; fwstart
```
3. Set a password (eg. abc123) for the LEA Server on Firewall Analyzer (eg. 10.1.1.2)
```
fw putkey -opsec -p abc123 10.1.1.2
```
4. Add a rule to the policy to allow the port defined above from the Firewall Analyzer machine to the Check Point Management Server
5. Install the policy

Changes to LEA Server on Firewall Analyzer

Once this has been set up, edit the LEA configuration file for this Check Point firewall:

1. Define the IP address(eg. 10.1.1.1), port(eg. 18184), and authentication type for authenticated LEA connections:
```
lea_server ip 10.1.1.1
lea_server port 18184
lea_server auth_type auth_opsec
```
2. Set the password to connect to the Check Point Management Server. This is the same password that has been set on the Check Point Management Server
```
opsec_putkey -p abc123 10.1.1.1
```

Setting up an Authenticated LEA Connection to NG

The following steps will help you configure an **sslca** authenticated connection to the Check Point NG Management Server:

1. In the *FWDIR\conf* directory on the computer where the Check Point Management Server is installed, edit the `fwopsec.conf` file and define the port to be used for authenticated LEA connections:
```
lea_server port 0
lea_server auth_port 18184
lea_server auth_type sslca
```
2. Restart the firewall service
```
cpstop ; cpstart
```

3. Create a new Opsec Application Object with the following details:
    1. Name (eg. myclient)
    2. Vendor: user defined
    3. Server Entities: none
    4. Client Entities: LEA
4. Initialize Secure Internal Communication (SIC) for this Opsec Application Object and enter the activation key (e.g. def456). Note down this activation key, as you will need it later.
5. Write down the DN of this Opsec Application Object. This is the Client Distinguished Name, which you need later on.
6. Open the object of the Check Point Management Server and write down the DN of that object. This is the Server Distinguished Name, .
7. Add a rule to the policy to allow the port defined above, as well as port 18210/tcp (FW1_ica_pull) in order to allow pulling of PKCS#12 certificate from the Firewall Analyzer to the Check Point Management Server. The port 18210/tcp can be shut down after the communication between Firewall Analyzer and the Check Point Management Server has been established successfully.
8. Install the policy

Changes to LEA Server on Firewall Analyzer

Once this has been set up, edit the LEA configuration file for this Check Point firewall:

1. Define the IP address(eg. 10.1.1.1), port(eg. 18184), authentication type, and SIC names for authenticated LEA connections:
   (The SIC names are the Client DN and Server DN that were noted down earlier)
   ```
   lea_server ip 10.1.1.1
   lea_server port 18184
   lea_server auth_type sslca
   opsec_sslca_file opsec.p12
   opsec_sic_name "CN=myleaclient,O=cpmodule..gysidy"
   lea_server opsec_entity_sic_name "cn=cp_mgmt,o=cpmodule..gysidy"
   ```
2. Get the **opsec_pull_cert** tool either from **opsec-tools.tar.gz** from the project home page, or directly from the OPSEC SDK. This tool is needed to establish the Secure Internal Communication (SIC) between Firewall Analyzer and the Check Point Management Server.
3. Get the client certificate from the Check Point Management Server (e.g. 10.1.1.1). The activation key has to be the same as specified before in the firewall policy. After that copy the resulting PKCS#12 file (default: opsec.p12) to the *<FirewallAnalyzer_Home>/server/default/leaconf* directory.
   ```
   opsec_pull_cert -h 10.1.1.1 -n myleaclient -p def456
   ```

The LEA Configuration File

The LEA configuration files are present in the *<FirewallAnalyzer_Home>/server/default/leaconf* directory. By default, only the **leaclient.conf** file is present here. If you are adding a single Check Point firewall, use this file to configure LEA client parameters.

If you are configuring more than one Check Point firewall, create a separate .conf file with the **same name** as the host name entered when the LEA Server was added in Firewall Analyzer.

The parameters to be set in the LEA client configuration file are described in the table below:

Parameter	Description
lea_server ip <IP address>	The IP address to which the LEA Server on Firewall Analyzer should connect to.
lea_server port <port number>	The port to which the LEA Server on Firewall Analyzer should connect to, for an unauthenticated connection.

Parameter	Description
lea_server auth_port <port number>	The port to which the LEA Server on Firewall Analyzer should connect to, for an authenticated connection.
lea_server auth_type <authentication mechanism>	The authentication mechanism to be used. The default value is sslca. Supported values in this field are: sslca, sslca_clear, sslca_comp, sslca_rc4, sslca_rc4_comp, asym_sslca, asym_sslca_comp, asym_sslca_rc4, asym_sslca_rc4_comp, ssl, ssl_opsec, ssl_clear, ssl_clear_opsec, fwn1 and auth_opsec.
opsec_sslca_file <p12-file>	The location of the PKCS#12 certificate, in the case of authenticated connections.
opsec_sic_name <SIC name of LEA-client>	The SIC name of the LEA client (the LEA Server on Firewall Analyzer), in the case of authenticated connections.
lea_server opsec_entity_sic_name <SIC name of LEA-server>	The SIC name of the Check Point Management Server.

Importing Check Point Log Files

Before proceeding with the importing of Check Point logs, you need to do the following changes in the Smart View Tracker of the Check Point Firewall to obtain the complete log information:

Changes in Smart View Tracker :

1. Open the "Smart View Tracker" and click on "View" --> "Query Properties".
2. Please select the following attributes if they where not selected previously:
   - Elapsed
   - Bytes
   - Client InBound Bytes
   - Client OutBound Bytes
   - Server InBound Bytes
   - Server OutBound Bytes
   - Status
   - URL

For Non-LEA connections, there are two ways to create plain text check point log file and export the log file, which then can be imported in Firewall Analyzer. For LEA connections you can skip the below mentioned methods and follow the LEA configuration instructions.

Method 1 :

In the command prompt of Check Point Firewall Server machine execute the following command

```
fw logexport -d ; -i fw.log -o exportresult.log -n
```

where, *-d* refers to *delimiter*, *-i* refers to *input log file*, *-o* refers to *output ASCII file*, and *-n* implies *don't perform DNS resolution of the IP addresses in the Log File (this option significantly improves processing speed)*.

For detailed information please refer the Check Point documentation or contact Check Point technical support.

The above command creates an ascii file named *exportresult.log*. Copy or transfer this file to Firewall Analyzer machine. Then in Firewall Analyzer you can Import this log file.

Method 2 :

1. In the Check Point Smart Tracker UI (UI where you are seeing all logs in Check Point Management Station), select All Records option in the left tree.
2. Click "File" --> "Export".
3. Give a proper file name, like exportresult.log. Copy or transfer this file to Firewall Analyzer machine. Then in Firewall Analyzer you can Import this log file.

Configuring Cisco PIX Firewalls

Firewall Analyzer supports Cisco PIX versions 6.*x* and 7.*x* . To find out the version of your PIX firewall, Telnet to the PIX firewall and enter the `show version` command.

Cisco PIX does not create log files, but instead directs a log stream to the syslog server, which writes the log information into a file. Make sure the syslog server on Firewall Analyzer can access the PIX firewall on the configured syslog port. For this, you may have to make a rule specific to this situation.

Configuring Versions Earlier than Version 4.2(2)

1. Telnet to the PIX firewall and enter the `enable` mode
2. Type the following in the command prompt:
   ```
   syslog facility 20.7
   ```
   where facility 20 is the function that you want to perform, and 7 is the log detail level or debug level of messages to be sent to the syslog server.
3. Then type the following:
   ```
   syslog host <machine_IP>
   ```
   where <IP address> is the IP address of the syslog server.

Configuring Versions Higher than Version 4.2(2)

1. Telnet to the PIX firewall and enter the `enable` mode

Type the following:
`configure terminal`
`logging on`
`logging facility 20`
`logging timestamp`
`logging trap informational`
`logging host <interface_name> <machine_IP> [17/<syslog_port>]`
where,
`<interface_name>`
	is the interface on the PIX firewall whose logs need to be analyzed

`<machine_IP>`	is the IP address of the syslog server on Firewall Analyzer
`17/<syslog_port>`	indicates that logs will be sent using the UDP protocol, to the configured syslog port on the syslog server. If left blank, logs will be sent to the default 514 port.

Example: `logging host inside 11.23.4.56 17/1514`

To verify your configuration, enter the `show logging` command after the last command above. This will list the current logging configuration on the PIX firewall.

Configuring Cisco PIX from the Web Interface

Log in to the Cisco PIX web interface, and follow the steps below to configure the PIX firewall:

1. *Enabling Logging*
    1. Select **Configure > Settings > Logging > Logging Setup**
    2. Select the **Enable logging setup** and **Enable logging failover** checkboxes
    3. Click **Apply**.
       Changes are applied to the assigned PIX firewall configuration files when they are generated. The configuration files are then downloaded to PIX firewalls at deployment.
2. *Configuring Syslog Server*
    1. *Select **Configure > Settings > Logging > Syslog***
    2. *Check **Include Timestamp**.*
    3. *Click **Add** to add a row.*
    4. *In the **Add Syslog Server** page that appears, enter the following:*
        1. ***Interface Name** - the firewall interface through which FirewallAnalyzer can be reached, the interface can be either inside or outside.*
        2. ***IP Address** - the IP address of the syslog server to which logs have to be sent*
        3. *Under **Protocol**, select the **UDP** radio button*
        4. *The default UDP port is 514. If you have configured a different syslog listener port on your syslog server, enter the same port here.*
    5. *Click **Apply***
3. *Configuring Logging Level*
    1. Select **Configure > Settings > Logging > Other**
    2. Under **Console Level List** select **Informational** so that all report data is available
    3. Click **Apply**

For more information, refer the Cisco PIX documentation.

Configuring Fortinet Firewalls

Firewall Analyzer supports the following versions of FortiGate:

- FortiOS v2.5 and 2.8
- Fortinet - 50,100, 200, 300, 400, 800
- Fortigate - 1000, 5000 series

> Firmware v2.26 or later is required

To determine the version number of the Fortigate that you are running, use the command: *get system status*

Configuring the FortiGate Firewall

Follow the steps below to configure the FortiGate firewall:

1. Log in to the FortiGate web interface
2. Select **Log & Report > Log Setting** or **Log & Report > Log Config > Log Setting** (depending on the version of FortiGate)
3. If you want to export logs in WELF format:
    1. Select the **Log in WebTrends Enhanced Log Format** or the **WebTrends** checkbox (depending on the version of FortiGate)
    2. Enter the IP address of the syslog server
    3. Choose the logging level as **Information** or select the **Log All Events** checkbox (depending on the version of FortiGate)
4. If you want to export logs in the syslog format (or export logs to a different configured port):
    1. Select the **Log to Remote Host** option or **Syslog** checkbox (depending on the version of FortiGate)
    2. Enter the IP address and port of the syslog server
    3. Select the logging level as **Information** or select the **Log All Events** checkbox (depending on the version of FortiGate)
    4. Select the facility as **local7**
5. Click **Apply**

Configuring RuleSets for Logging Traffic

Follow the steps below to configure rulesets for logging all traffic from or to the FortiGate firewall:

1. Select **Firewall > Policy**
2. Choose a rule for which you want to log traffic and click **Edit**. You can configure any traffic to be logged separately if it is acted upon by a specific rule.
3. Select the **Log Traffic** checkbox
4. Click **OK** and then click **Apply**

Repeat the above steps for all rules for which you want to log traffic.

For more information, refer the Fortinet documentation.

Configuring SonicWALL Internet Security Appliances

Firewall Analyzer supports the following versions of SonicWALL:

- SonicWALL Internet Security Appliance versions 4.1 and 5.x
- SonicWALL PRO-VX
- SonicWALL PRO
- SonicWALL XPRS2 or XPRS
- SonicWALL DMZ
- SonicWALL SOHO2 or SOHO
- SonicWALL TELE2 or TELE

The logging preferences in SonicWALL version 6.0.0.0 differ from those of earlier versions. There are now two logging formats: WELF format and standard format. In the standard format, the source and destination fields contain port number and link (i.e., WAN, LAN, DMZ) information. This information is not included in the WELF format.

Configuring SonicWALL To Direct Log Streams

1. Log in to the SonicWALL appliance
2. Click **Log** on the left side of the browser window
3. Select the **Log Settings** tab
4. Type the IP address of the Firewall Analyzer server in the **Syslog Server** text box
5. Click **Update** at the bottom of the browser window
6. Restart the SonicWALL appliance for the changes to take effect.

For more information, refer the SonicWALL documentation.

The **time duration** attribute is not supported on SonicWALL device. Hence you cannot see Live Reports for SonicWALL devices.