ManageEngine Firewall Analyzer

Quick Start Guide

July 29, 2022

Version 2.0

Table of Contents

Firewall Analyzer - Quick Start Guide

Get started with Firewall Analyzer in four easy steps.

- Download and Install
- Start and Configure
- Get Reports
- Get Alarms

Download and install

Download

- Download the Firewall Analyzer product from the download page.
- Check the system requirements to install the product.

Install the product

Click on the downloaded file for customized product installation. The wizard screens will guide you through the installation.

Quick view of the installation

- Agree to the terms and conditions of the license agreement.
  You may get it printed and keep it for your offline reference.
- Choose the language (English, Simplified Chinese, Traditional Chinese, Japanese, Spanish, German, Italian, French, and Korean).
  Ensure that the browser supports the selected language.
- Select the folder to install the product. Use the Browse option. The default installation location will be C:\ManageEngine\OpManager folder.
  If the new folder or the default folder does not exist, the installer will create and install the product.
- Enter the web server port. The default port number will be 8060.
  Ensure that the default port or the port you have selected is not occupied by some other application.
- Enter your details to get evaluation assistance.
- Select the back end database, PostgreSQL (bundled with the product) or MS SQL if you have an instance.
- At the end of the procedure, you can view the Readme file.

With this, the Firewall Analyzer product installation is complete.

Note: By default, the installer will install Firewall Analyzer as a Windows service.

Start and Configure

Start the server

- Ensure that the prerequisites are met.
- Run the product as a service.

Connect web client

Once the installer installs Firewall Analyzer as a service, it will launch the web client automatically. If it is not getting launched automatically, open a new browser window and in the address bar type the host name to connect to the Firewall Analyzer server.

- Open a supported web browser window.
- Type the URL address as https://<hostname>.
  The <hostname> is the name of the machine on which Firewall Analyzer is running. The default web server port is 8060, if you have configured some other port as web server, type https://<hostname>:<portnumber>.
- Log into Firewall Analyzer using the default username/password combination of admin/admin. ManageEngine suggests you to follow the security best practice and change the Admin username/password after the first login.

Configure firewalls to forward syslogs

Firewall Analyzer listens at the default ports for exported log files. In the help document The configuration instructions are available in the help document, for the different versions of various firewalls. Click the firewall name to see the corresponding configuration instructions.

Import security device logs

Firewall Analyzer can import the security device logs automatically at regular intervals.

- Use the Local Host option to import the log files from the local machine, from where you are accessing Firewall Analyzer over the web. The maximum log file size for import from local host is 1 GB.
- Use the Remote Host option to import the log files from remote machines. The maximum log file size for import from remote host is 2 GB.
- Click the Import button to start the file import operation

Import once or periodically from remote host

You can import the log file into Firewall Analyzer server, one time or periodically.

- If you have not entered the 'Time Interval' (Scheduling time in minutes) and selected the 'From' time, then the option allows you to import the log file once from the remote host.
- If you enter the 'Time Interval' (Scheduling time in minutes) and selected the 'From' time, then the option allows you to import the log file periodically from the remote host.
- If you have selected Remote Host to import the log file from the remote machines, for all Time Interval options manually type in the location of the file or folder containing the log files in the remote machine. Otherwise, click the 'Browse' button to get the location of the log file or folder.

Fetch rules/policies from firewalls for analysis and optimization

Firewall Analyzer fetches rules/policies from firewall using CLI, API, file. You can configure Firewall Analyzer to fetch rules using Device Rule or Credential Profile settings.

Get Reports

Once you configure the firewalls to send the syslogs and/or import the logs to Firewall Analyzer server, after 10 minutes, the reports start rolling out in the client.

View Firewall Reports

Firewall Analyzer offers a rich set of reports that help in analyzing network's security and bandwidth usage. The reports are displayed in the Reports tab of the UI. You can drill down the event counts shown in the reports to get the raw logs. You can filter the logs based on various log fields.

Description of reports

- Custom Reports - If you create custom reports, they are listed in this section.
- Firewall Reports - This covers a wide range of firewall reports such as traffic, protocols, security, VPN, and trend.
- Proxy Reports - This covers URL reports, websites visited, top talkers, and proxy usage.
- Rule Management - In this, Overview, Optimization, Cleanup, Reorder, Impact, administration, Comparison, and Expiry Notification reports are available.

- Compliance Reports - In this we have
    - Standards - This report covers major compliance regulations such as PCI-DSS, ISO-27001, NERC-CIP, NIST, SANS, SOX, HIPAA, GDPR, GLBA, and Basel-II
    - Change Management - Firewall configuration changes made and raw configuration are available in this report.
    - Security Audit - In this you will get a device-wise Security Audit and configuration Analysis report
- Search Report - You will get aggregated and raw log search in this report.

Create Custom Reports

The custom reports created are listed in the Custom Reports section. You can create new reports; edit or delete existing reports. You can schedule the unscheduled reports. Refer to the Create Custom Reports topic in the help document.

Search the Logs

Firewall Analyzer's log search functionality is easy and allows you to do a free-form search. When a user enters a search criterion in the search bar, Firewall Analyzer rapidly drills down into the raw logs and retrieves the results for your search query. You can save the results as report profiles.

Refer to the How to Search topic for explanation about search. You can conduct two types of searches: Basic Search and Advanced Search.

You can schedule report generation and distribute via email.

Get Alarms

Create Alarm Profiles

Firewall Analyzer can generate alarm for occurrence of specific security, anomalous, and bandwidth events. Refer to the Create Alarm Profiles topic in the help document.

You can notify the alarms via email and SMS. You can also execute scripts to run other applications.

With this you can start using Firewall Analyzer to manage your firewall security. Refer to the Help document for more information.

Configurations

Configure Email, SMS Settings

You have to configure a mail server to distribute reports and notify alarms. Also, you have to configure SMS settings to notify alarms.

- Ensure that you configure the 'Mail Server Settings' to send the Email alarm notification and distribute the scheduled reports generated
- Configure the SMS Settings, if required. You need to configure the SMS Setting, in order to receive alarm notifications on your mobile phone. You may need to connect a physical device with a SIM card from service provider to send SMS alarm notification.

Advanced Configurations

- Firewall Analyzer supports MS SQL as back end database. This is apart from the PostgreSQL database bundled with the product. If you have MS SQL already in your company, you can utilize the same with a simple migration procedure. Refer to the procedure in the help document
- Firewall Analyzer archives the log files periodically for internal, forensic and compliance audits. The archival interval and retention period are configurable. You can configure to encrypt and time-stamp the archive file to make it secure and tamper-proof.
- Firewall Analyzer retains the log data in the database for a limited period to process. After the period is over, Firewall Analyzer will purge the data from the database. You can set the database storage size.
- Configure 'Firewall Availability Alarm' under the Settings tab, so that you will receive an alarm, if the specific Firewalls does not send logs to the Firewall Analyzer server for a span of more than 15 minutes

Refer to the topics given below for more information about starting Firewall Analyzer:

- Frequently Asked Questions
- Troubleshooting Tips