- Introduction
- Installation
  - ✓ firewall analyzer step by step installation
- Startup
  - ✓ Syslog and SNMP setup on firewall side
  - ✓ firewall analyzer startup
- Configuration
  - ✓ Syslog server add and check
  - ✓ Configure SNMP on Analyzer side
  - ✓ Configure Intranet
  - ✓ Configure reporting plan
  - ✓ Configure DNS
  - ✓ View firewall status and schedules
- Report Browsing
  - ✓ Types of Reports
  - ✓ Time Range of reports
  - ✓ Work hours allocation
  - ✓ Protocol category for reports
- Appendix
  - ✓ Configure user authentication for Internet access
  - ✓ Retrieve the saved logs from database

Introduction

Firewall DFL series are mature products offering a variety of functionality to satisfy customer's demands. For security administrators and IT managers, network monitoring and analyzing are keys to lead network usage more efficiently. To fulfill this kind of needs, DFL series provides thorough status and logging report system; this system, however, has its constraints due to the memory size. Those limitations may cause inconvenience to security administrators or IT managers occasionally. To avoid this predicament and expand abilities of network monitoring and analyzing, we introduce ManageEngine® Firewall Analyzer to complement our DFL series.

ManageEngine® Firewall Analyzer is a web based, agent-less, firewall log analysis and reporting software. The software application monitors, collects, analyzes, and archives logs from network perimeter security devices and generate reports. Two prominent features of the application are network monitoring and security reports.

ManageEngine® Firewall Analyzer consists of four parts – syslog server, log parsing engine, Web GUI and MySQL database. Syslog server collects logs from firewall and passes them to log parsing engine for further data processing. MySQL database sorts data, producing various reports and archiving logs. To provide users an easy and friendly way to view reports and configure system, Web GUI is developed to achieve this goal. ManageEngine® Firewall Analyzer joins all components together to help security administrators and IT managers to arrive at decisions on bandwidth management, network security, monitor web site visits, audit traffic, and ensure appropriate usage of networks by employees.

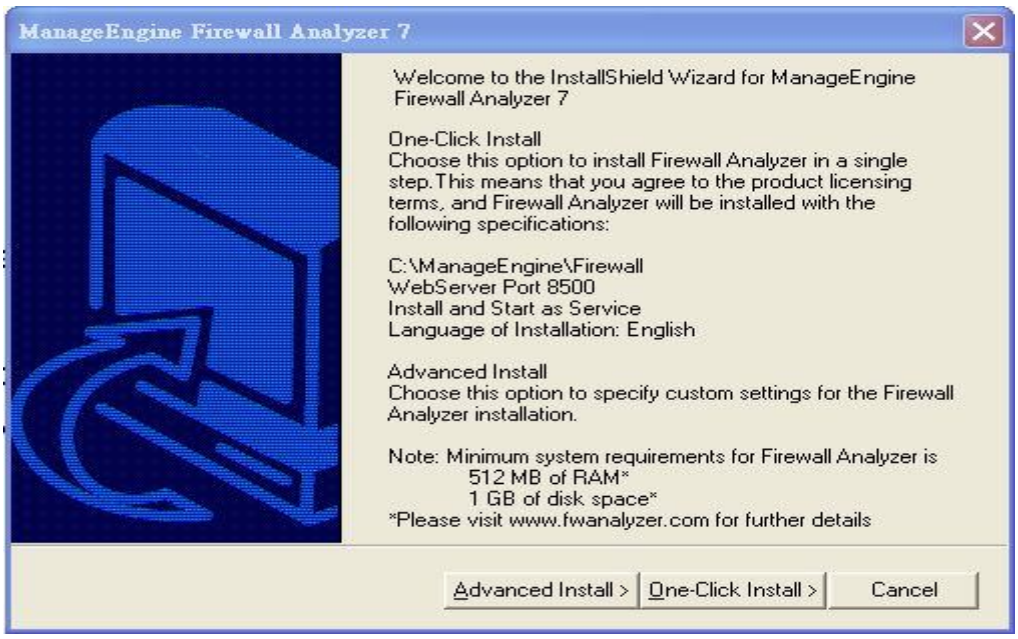
By combining powerful DFL logging system with smart ManageEngine® Firewall Analyzer analysis, we can deliver a complete network reporting and analyzing solution to content all network administrator and IT managers.

Installation

Firewall analyzer step by step installation

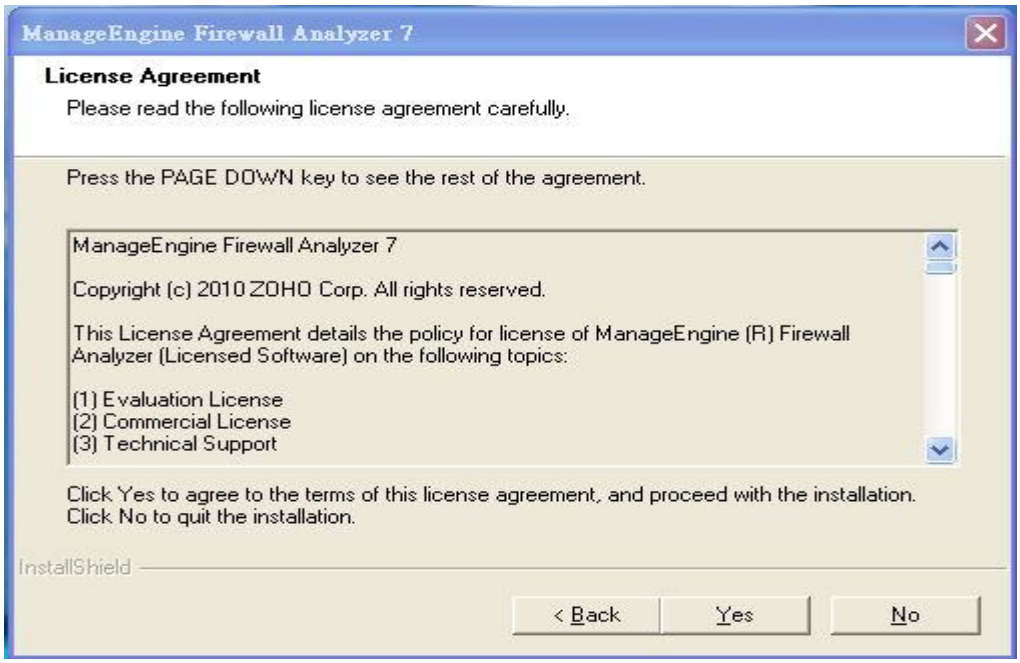
Step 1: Double click ManageEngine_FirewallAnalyzer_7

Step 2: Select Advanced Install

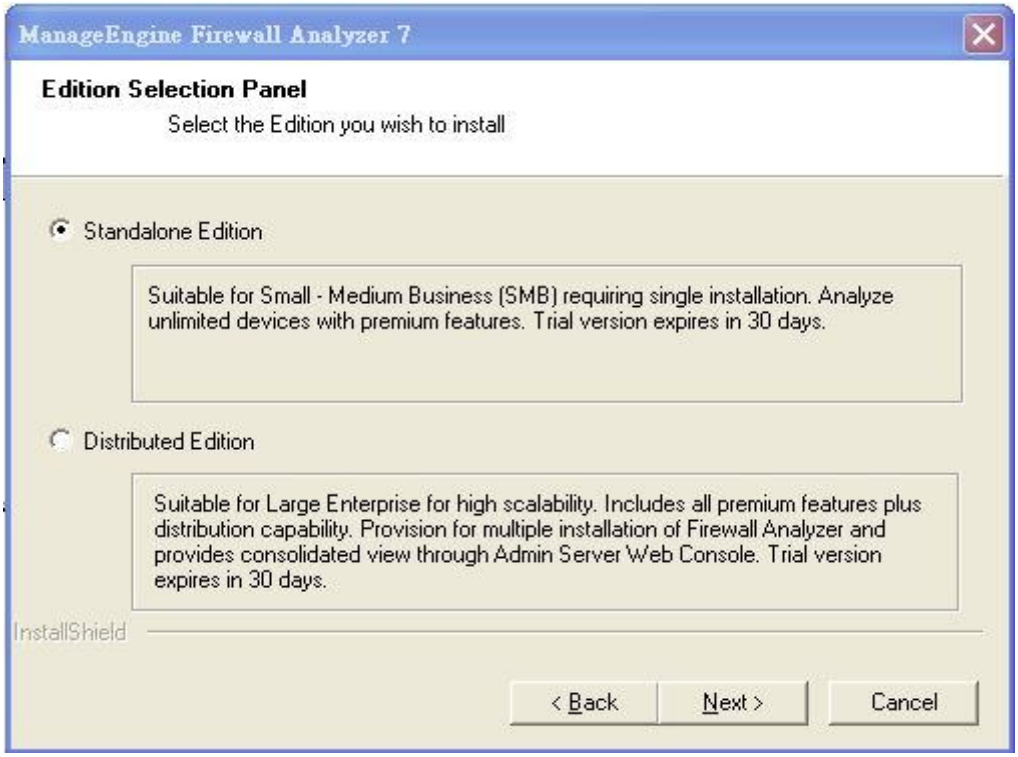


Notice: ManageFirewall Analyzer requires at least 512 MB of RAM and 1GB of disk space.

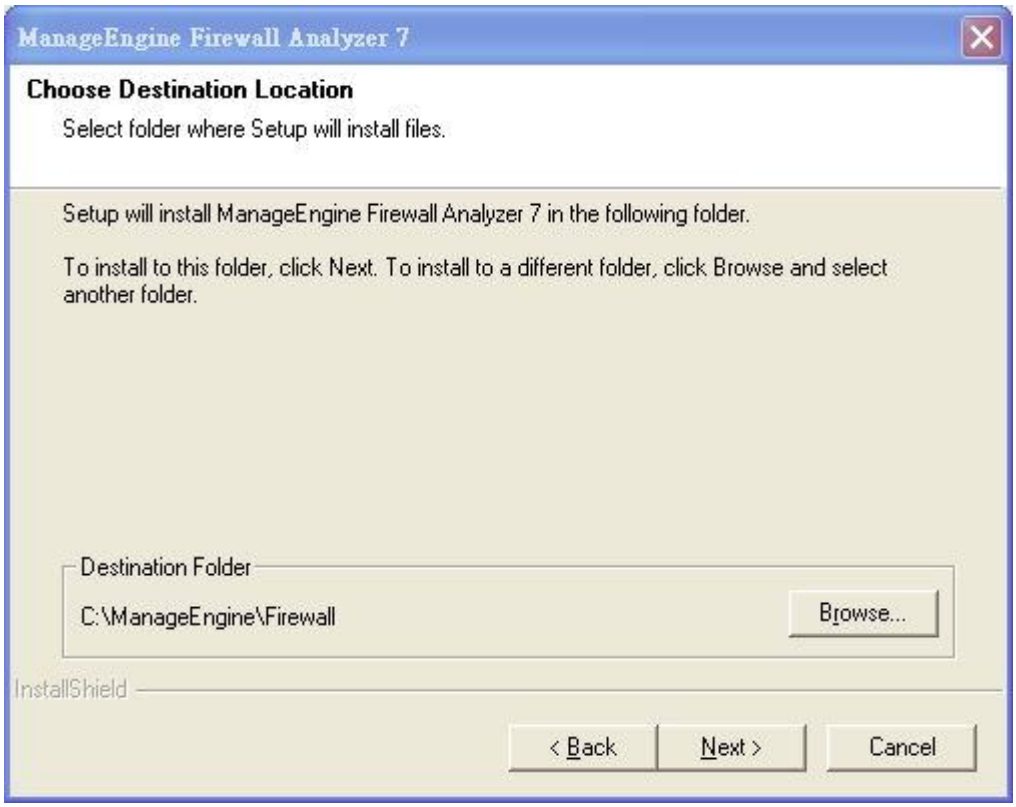
Step 3: Click “Yes” to agree to the terms of this license agreement



Step 4: Selecting “Standalone Edition”

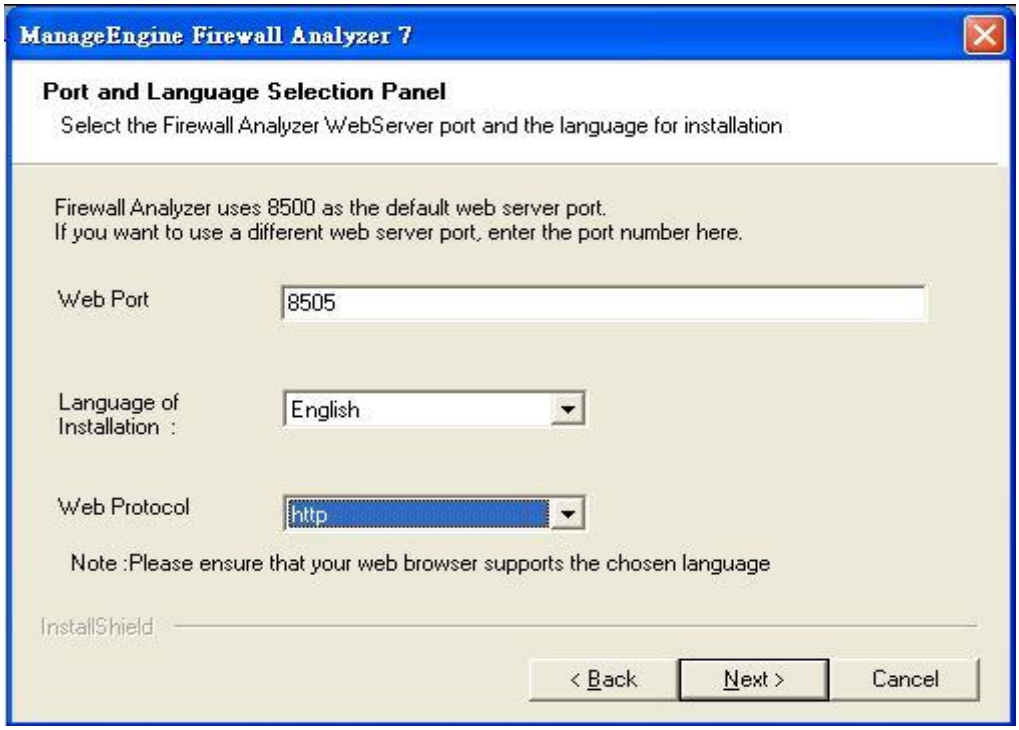


Step 5: Choose Destination Location

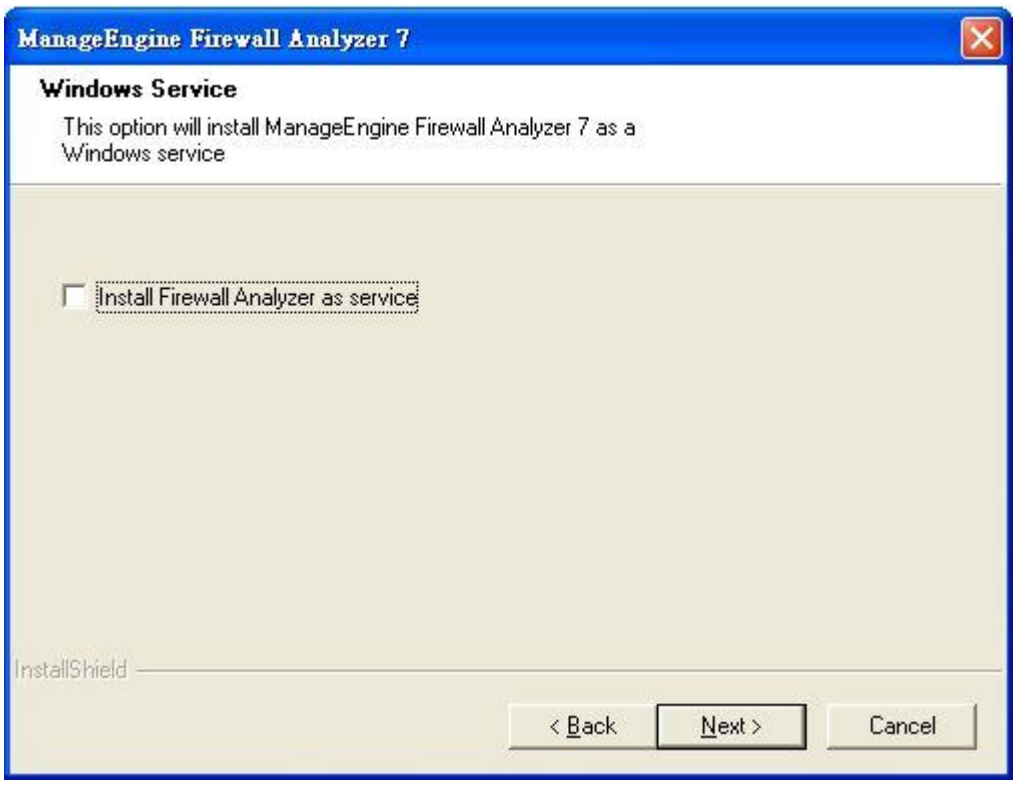


Step 6: Select port and favor language

Please change default Web Port 8500 to unused ports e.g. 8505 to avoid port conflictions. If you don't change the web port, you may encounter initialization problems during Firewall Analyzer starts up.

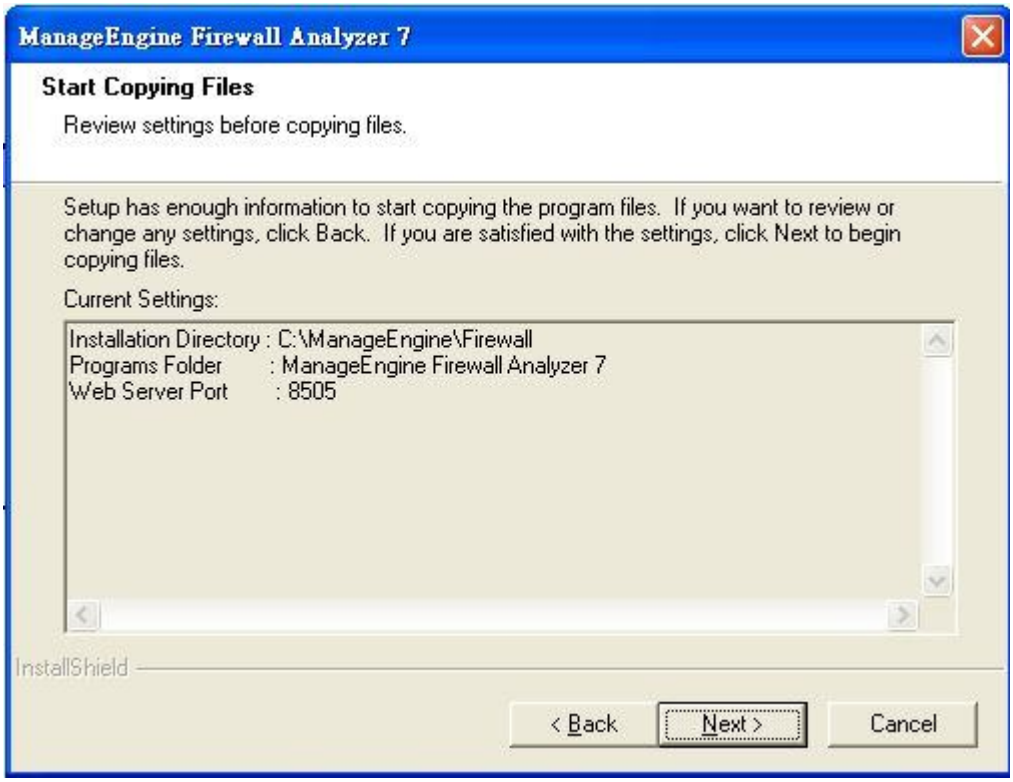


Step 7: Unselect "Install Firewall Analyzer as service"

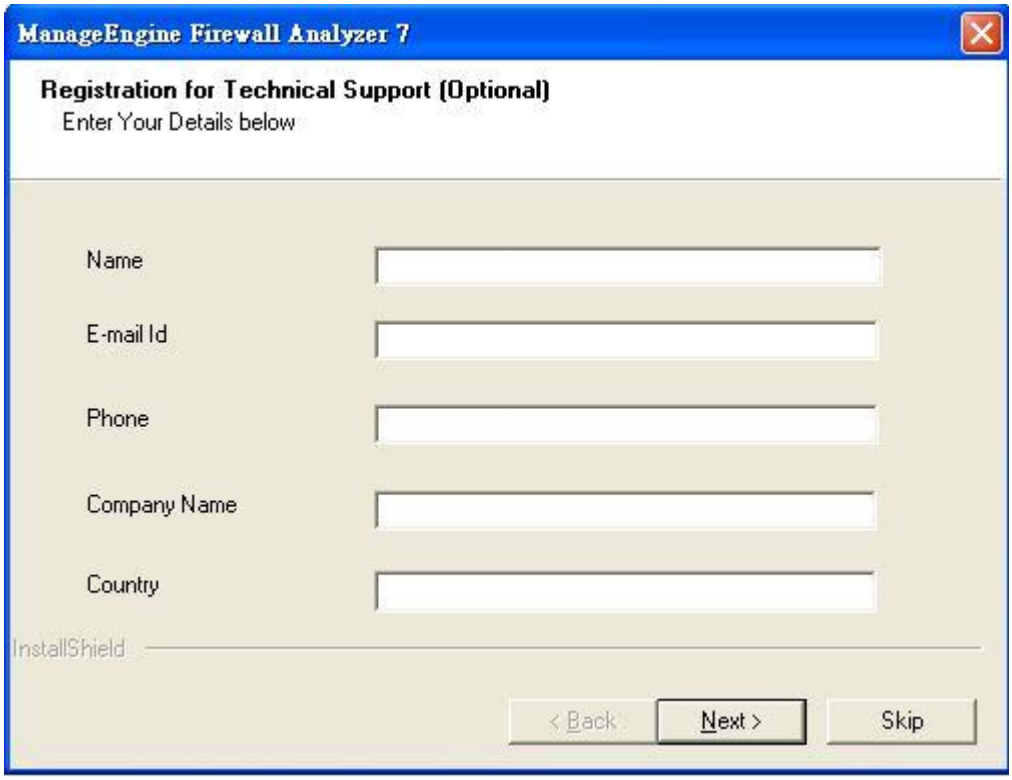


Step 8: Name the Program Folder

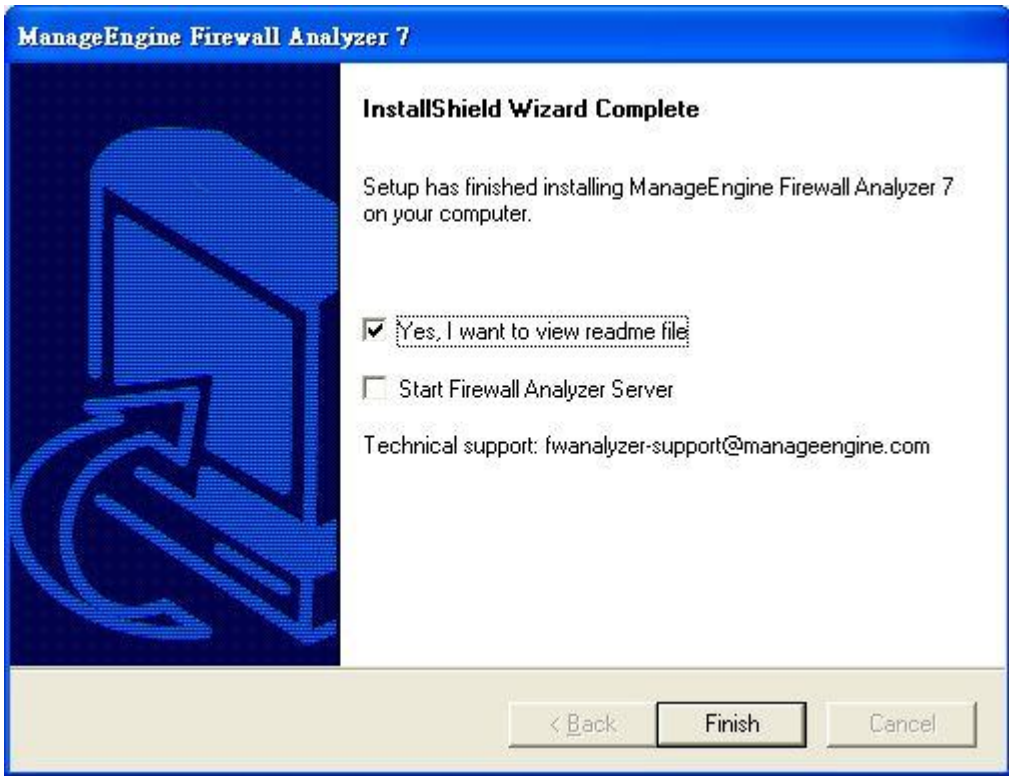
Step 9: Click next to start copying files



Step 10: Skip Registration process



Step 11: Finish Firewall Analyzer installation



Startup

Syslog and SNMP setup on firewall side

Before Firewall Analyzer can collect logs form firewall, firewall have to setup Syslog cland SNMP parameters first. You can add a syslog receiver or SNMP event receiver by navigating to **System -> Log and Event Receivers -> Add** as below Figure 1.

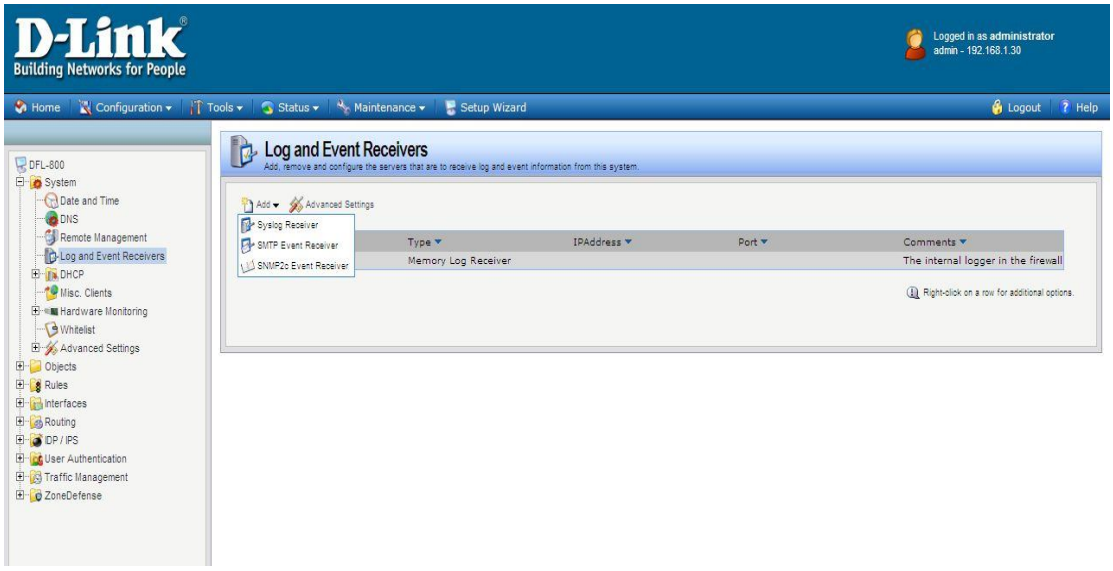


Figure 1: Log and Event Receivers

After you choose syslog receiver, more options are shown on the screen as below Figure 2.

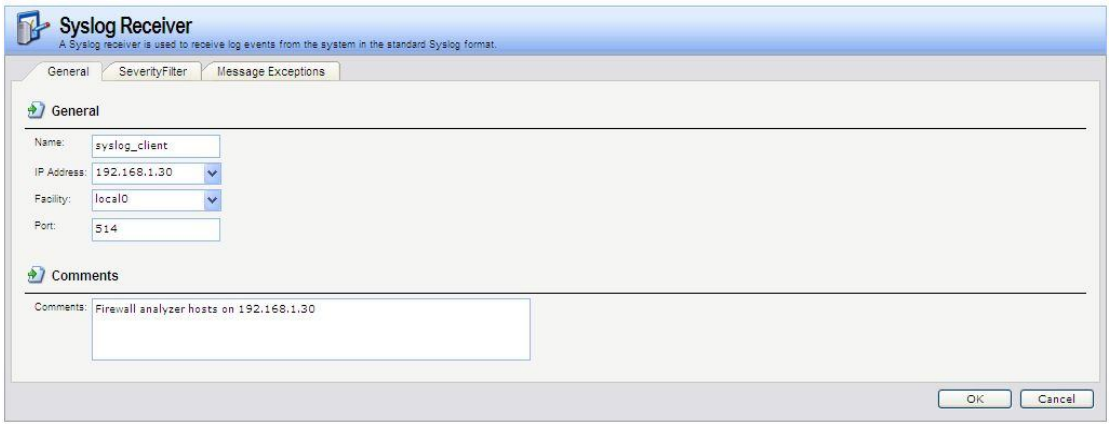


Figure 2: Syslog Receiver Configuration, General tab

In General tab (Figure 2):

Name: syslog_client

IP Address: 192.168.1.30 ---------- In this example, firewall analyzer hosts on 192.168.1.30

Facility: local0 (default)

Prot: 514 (default)

The severity of each event is predefined by NetDefendOS. For each event, the order of severity from high to low is Emergency -> Alert -> Critical -> Error -> Warning -> Notice -> Info -> Debug. You can select events which you want to send to the syslog receiver in SeverityFilter tab as below Figure 3.

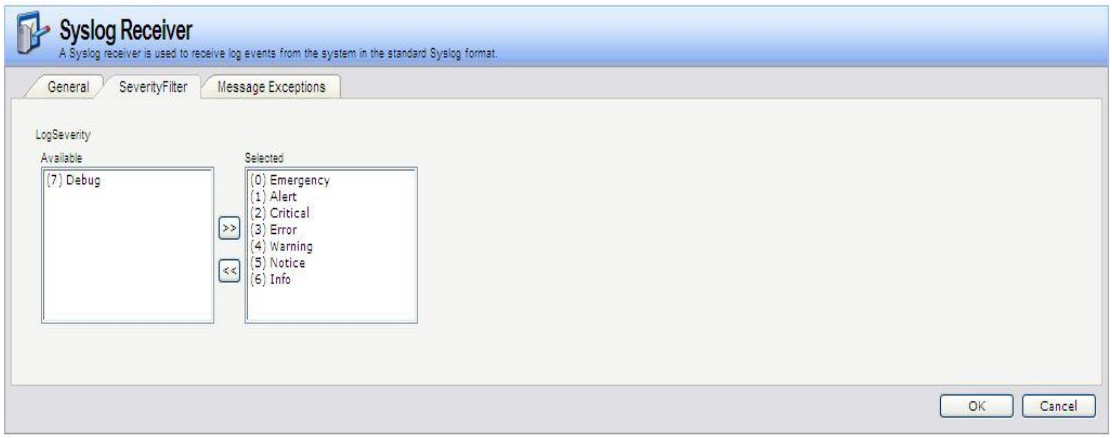


Figure 3: Syslog Receiver Configuration, SeverityFilter tab

Click OK to finish syslog receiver setting and navigate to **System -> Log and Event Receivers -> Add** again to add a SNMP2c Event receiver as below Figure 4.

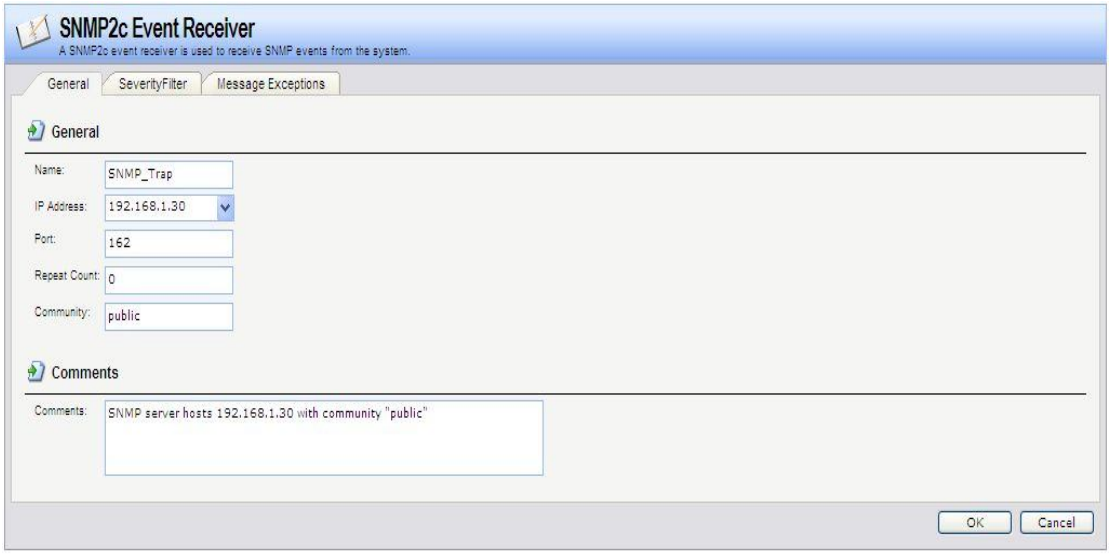


Figure 4: SNMP2c Event Receiver configuration, General tab

In General tab (Figure 4):

Name: SNMP_Trap

IP Address: 192.168.1.30 ---------- In this example, firewall analyzer hosts on 192.168.1.30

Port: 162

Repeat Count: 0

Community: public

As what we did during syslog receiver configuration, you can choose what events you want to send to SNMP2c Even receiver (Figure 5).

Figure 5: SNMP2c Event Receiver configuration, SeverityFilter tab

You can list all of receivers as below Figure 6.

Figure 6: Log and Event Receivers, listing all receivers

A situation where too many log packets firewall can send out per second may cause damages if a log receiver to which firewall sends is not active. The server will send back an *ICMP Unreachable* message, which may cause firewall to send another log message, which in turn will result in another *ICMP Unreachable* message, and so on. By limiting the number of log messages firewall sends every second, the administrator can avoid encountering such an undesirable situation where bandwidth in consumed unnecessarily; this value, however, should never be set too low, as this may lead important events not being logged.

To modify this value, please navigate to **System -> Log and Event Receivers -> Advanced Settings** as below Figure 7.

Figure 7: Log and Event Receivers, Advanced Settings

Firewall analyzer startup

There are two ways to start up Firewall Analyzer. Just click the shortcut icon on the desk or navigate Start -> Programs -> ManageEngine Firewall Analyzer 7 -> Firewall Analyzer can start up Firewall Analyzer. It may take a few minutes to initialize Firewall Analyzer, and then a web page will pop out to ask you logging in Firewall Analyzer as bellow Figure 8. The default username and password for first log in is admin/admin.

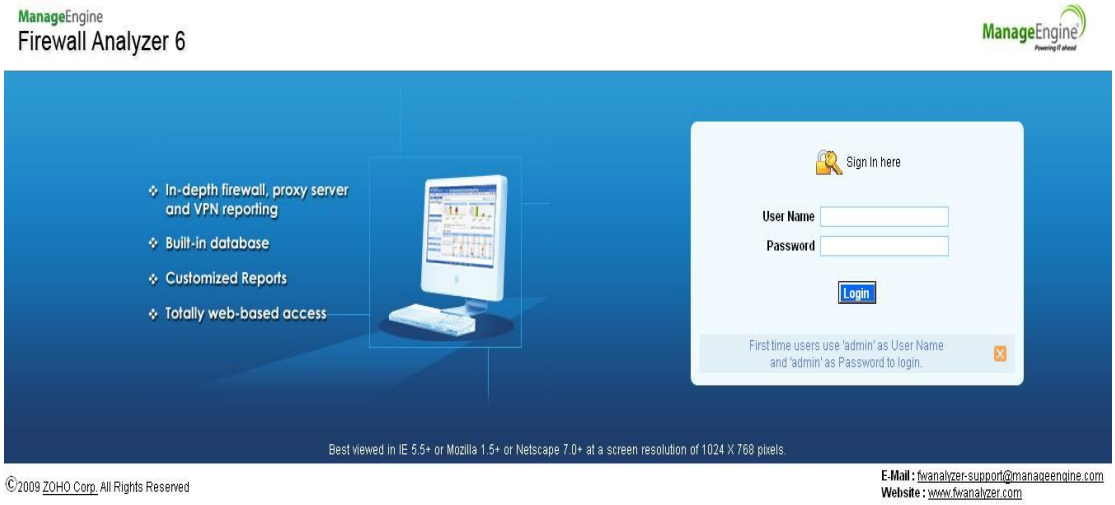


Figure 8: Firewall Analyzer log in page

If Firewall analyzer fails to start up, the reason may result form port conflictions as we describe in Step 6 of installation. To solve this problem, you can release all ports required by Firewall Analyzer but occupied by other network applications.

Configuration

Syslog server add and check

If you don't follow instructions described in the chapter of Startup, Syslog and SNMP setup on firewall side or change the default syslog port 514 to another one, you will see the home page as bellow Figure 9 after successfully logging in Firewall Analyzer.

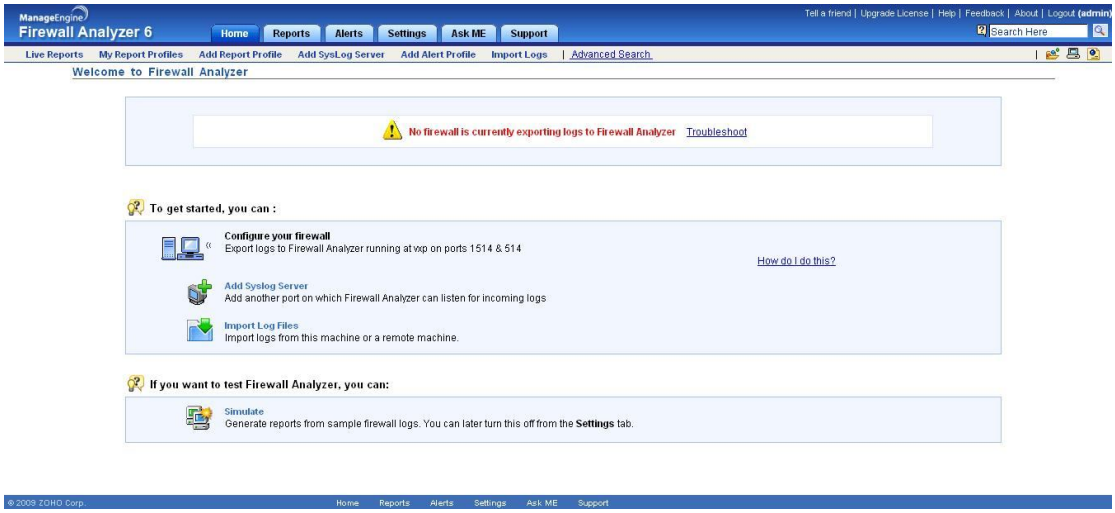


Figure 9: Firewall Analyzer first start up page

To receive logs from firewall and active Firewall Analyzer, please follow instructions described in the chapter of Startup, Syslog and SNMP setup on firewall side or click "Add Syslog Server" at the sub-bar or in the middle of Figure 9 to setup the correct syslog server listening port as Figure 10.

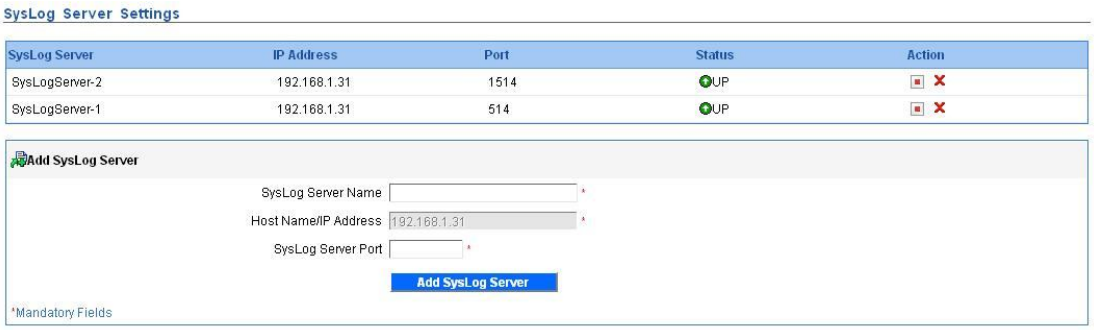


Figure 10: Syslog Server Settings

After you input right syslog settings, Firewall Analyzer starts to synchronize with and receive logs from servers as Figure 11. Firewall Analyzer will begin to generate the first reports after receiving 5000 logs from firewall. It means that you will see "No Data available" in all charts of all reports before Firewall Analyzer receives the 5000th log. The time waiting for the

first reports depends on the generating rate of logs (Please refer to Figure 7: Log and Event Receivers, Advanced Settings).

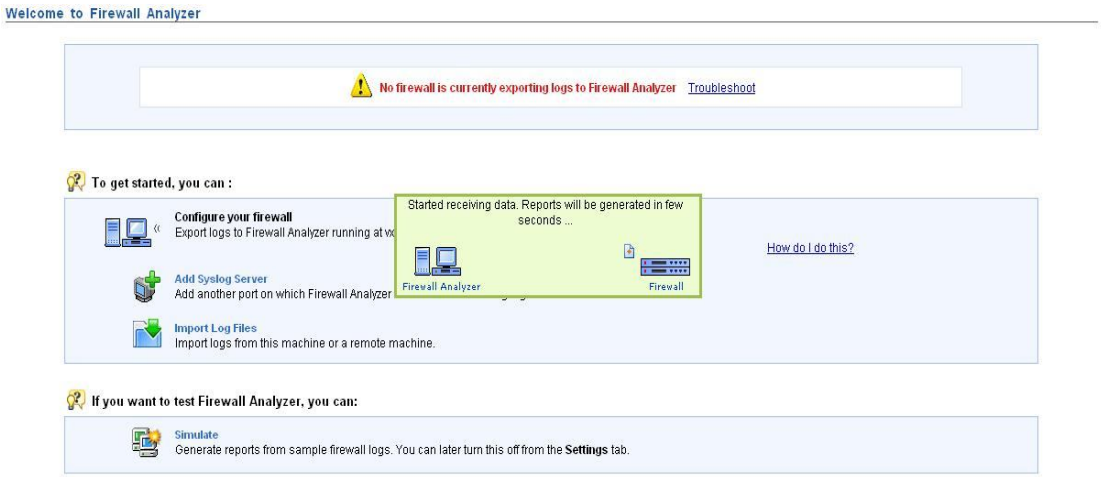


Figure 11: Started receiving logs form firewall

If Firewall Analyzer successfully synchronizes with firewall, you will find the IP address of firewall in the home page as Figure 12.

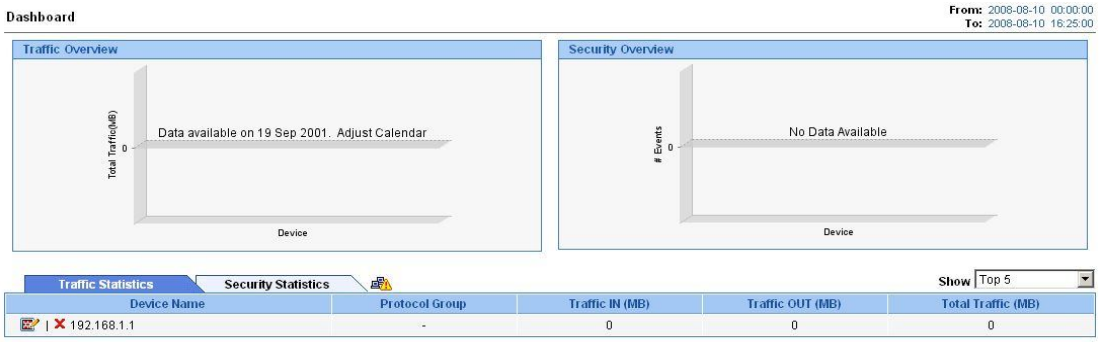


Figure 12: a synchronized firewall shown in the home page

You can click the icon  to set Display Name, Down link Speed and UP link Speed of firewall as below Figure 12.

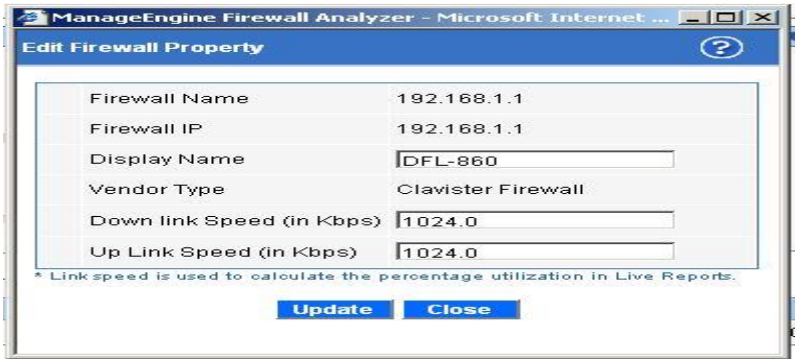


Figure 13: Firewall settings

Configure SNMP on FireWall Analyzer side

Live reports and traffics of each interfaces, e.g. WAN, LAN, are gathered through SNMP traps send by firewall. Before Firewall Analyzer can collect live data, remember to setup the SNMP parameters described in the chapter of Startup, Syslog and SNMP setup on firewall side and also configure FireWall Analyzer as follows:

1. Click ”Live Reports” at the sub-bar
2. Click “Set Global SNMP Parameters”

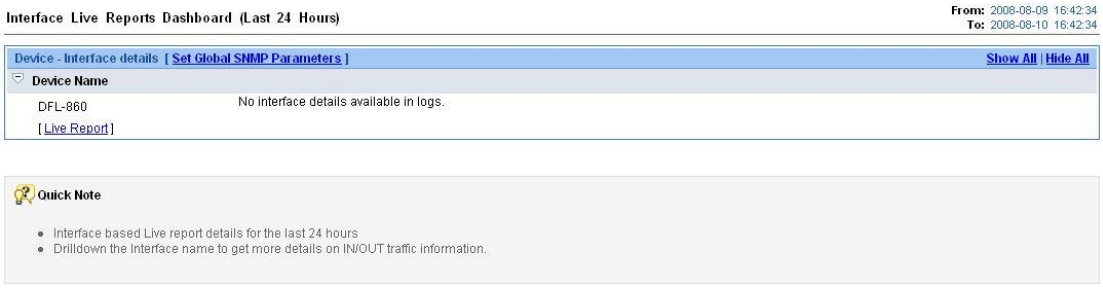


Figure 14: Interface Live Reports Dashboard

3. Input “SNMP Community” and “SNMP port” configured at firewall side as below Figure 15.

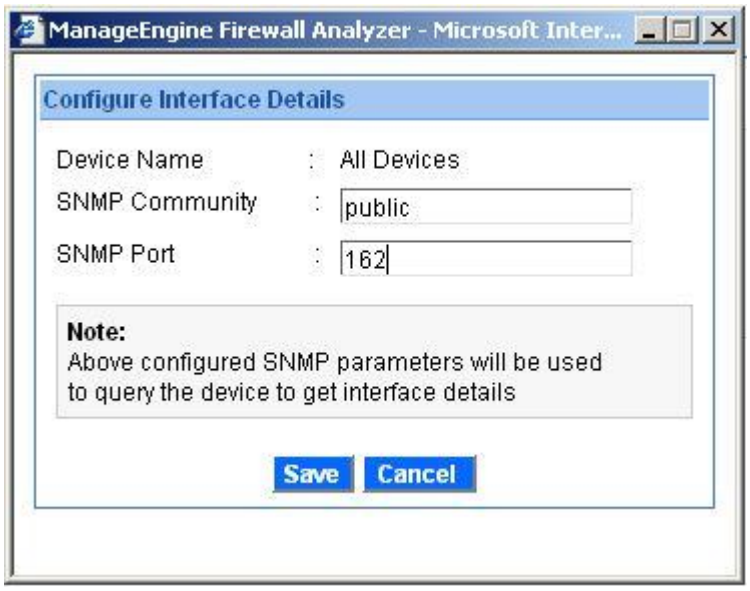


Figure 15: Configure Interface Details

Note: Live reports may not work due to SNMP OIDs inconsistence. We are dealing with it now.

Configure intranet

For network analysis purposes, traffic engineers may want to differentiate internal traffics with external ones. We can achieve this by using Intranet Settings. Please navigate to **Settings -> Admin Settings -> Intranet Settings** as Figure 16.

Figure 16: Settings

In Intranet Settings, click **Action -> Change** as Figure 17.

Figure 17: Intranet Settings

Please choose your firewall and IP Network, filling out Network and Net Mask and then clicking Save Settings. In this example, my firewall DFL-860 (192.168.1.1) and syslog receiver (192.168.1.30) locate in the internal subnet 192.168.1.0/24 as Figure 18. If your firewall has more internal subnets, click “more” to add them.

Figure 18: Intranet Settings Detail

Configure reporting plan

Firewall Analyzer can automatically generate a summary report at any periods you designated, e.g. one day, one week or one month. You can activate this service by following steps.

Step 1: Click Add Report Profile at the sub function bar as Figure 19.

Figure 19: sub function bar

Step 2: Give a report profile name, selecting your desired firewall and then clicking Next as Figure 20.

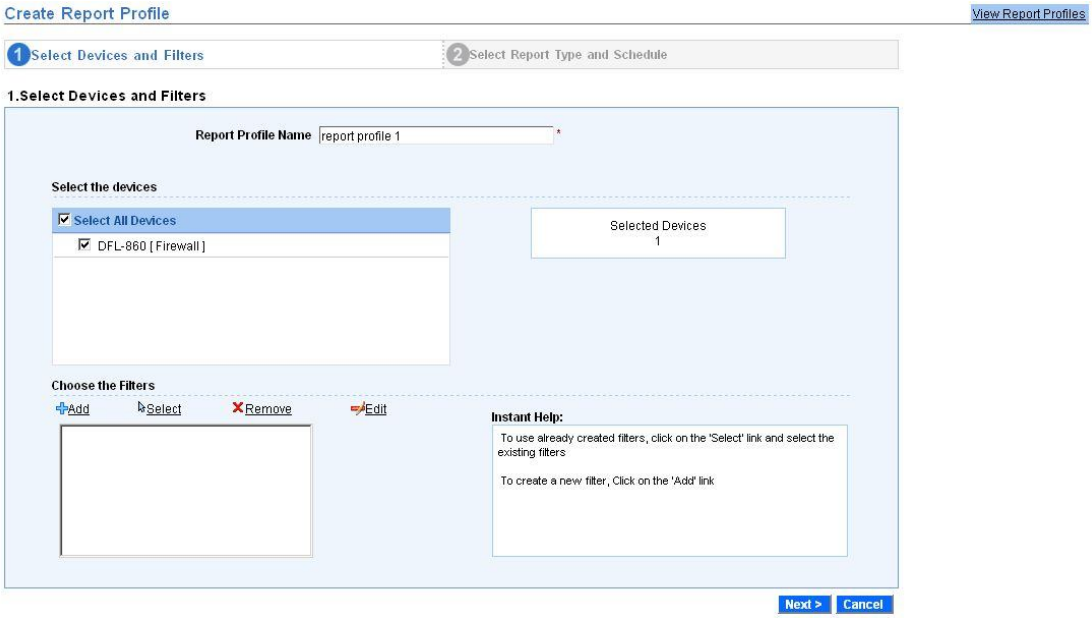


Figure 20: create report profile – select devices and filters

Step 3: Choose report type shown in summary report and which file type the summary report will be saved, scheduling when the summary report will be generated and then click save as Figure 21.

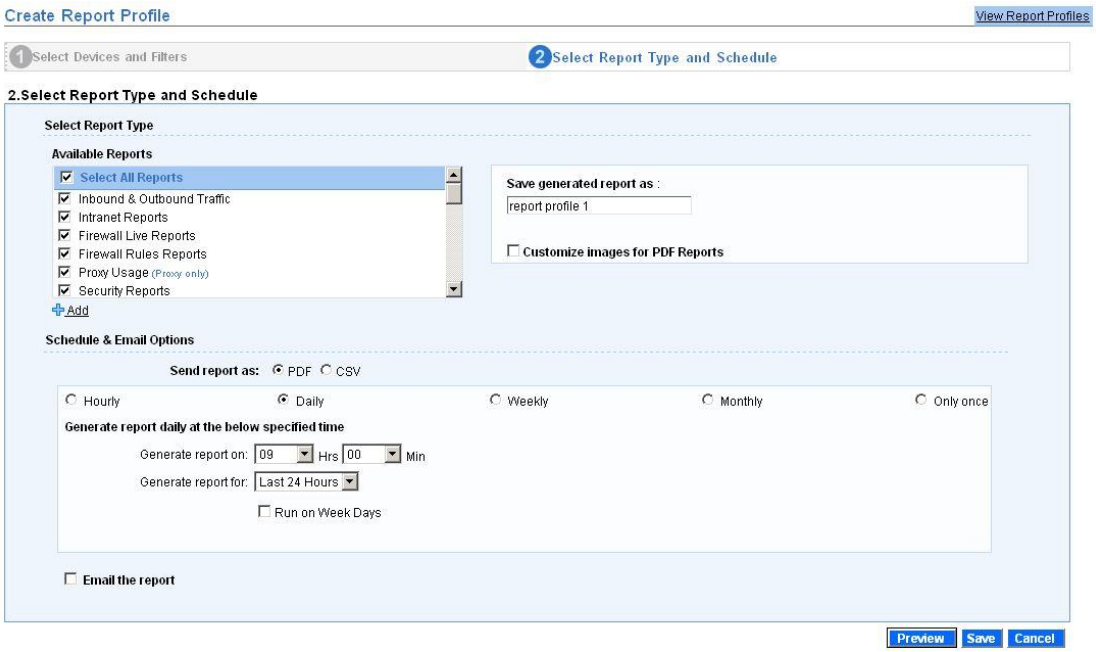


Figure 21: create report profile – select report type and schedule

Step 4: Click as My Report Profiles at the sub function bar to check reports status as Figure 22 and Figure 23.

Figure 22: sub function bar

Figure 23: My Report Profiles

Configure DNS

By default, all source and destination are shown in IP address format. You may feel inconvenient and can change this setting to manually or automatic translation. By navigating to **Settings -> System Settings -> Configure DNS**, you can choose options you want as Figure 24 and Figure 25.

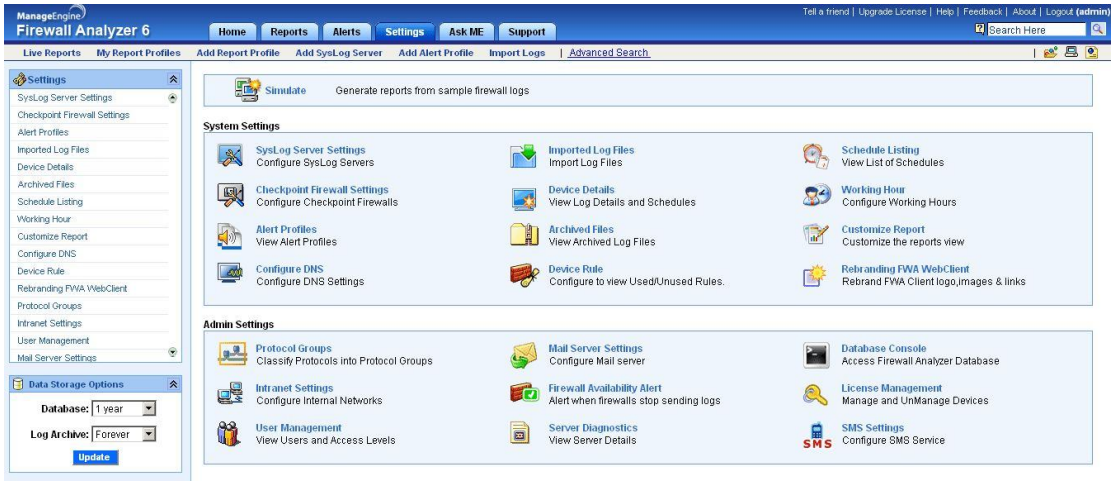


Figure 24: Settings

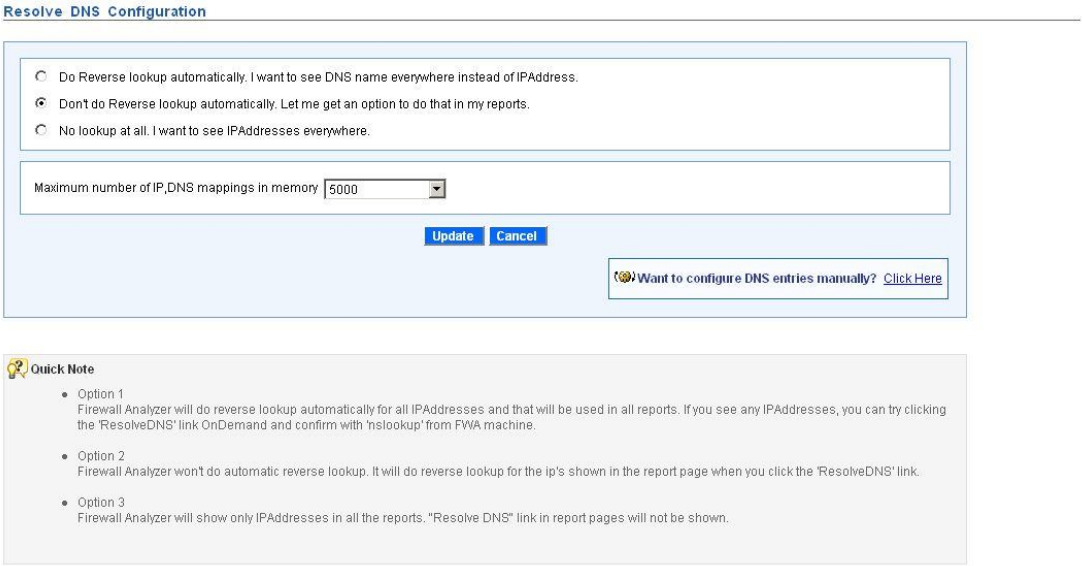


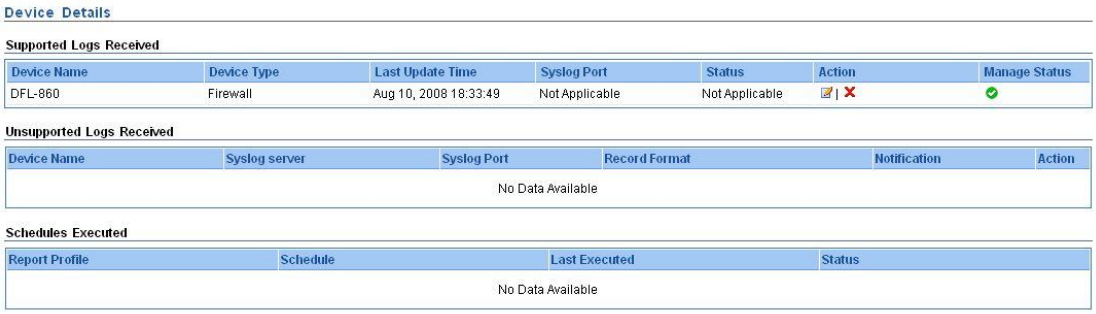
Figure 25: Resolve DNS configuration

If choosing manually resolve DNS, you can click the icon 

at the top right side in any reports when you want to resolve DNS.

View firewall status and schedules

If you want to review all firewall and schedule executed status, you can navigate to **Settings -> System Settings -> Device Details** as Figure 26.



Report Browsing

Types of Reports

There are many predefined reports and all of them can be categorized into real-time and non real-time reports. Only Live Reports belongs to real-time reports and others are non real-time reports. Real-time reports are gathered through SNMP traps, while non real-time reports are received from syslog clients. No matter whether real-time or non real-time reports, you have to correctly configure them before browsing them.

Time Range of reports

When browsing non real-time reports, e.g. traffic reports or protocol usage reports, you can change the time scale of all charts by choosing the day or time range you prefer as below Figure 27.

Figure 27: Date and Time Range

Work hours allocation

In trend reports like traffic or protocol trend reports, there are charts for working and non working hours. You can configure working hour details by navigating to **Settings -> System Settings -> Working Hour** as Figure 28.

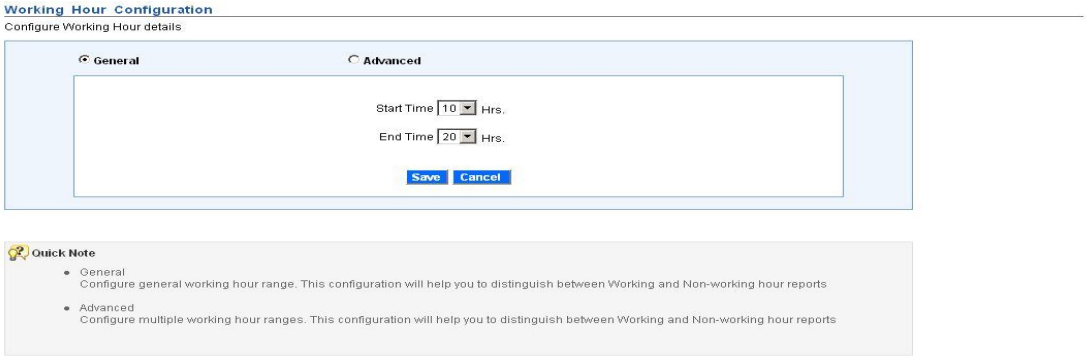


Figure 28: Working Hour Configuration

Protocol category for reports

Firewall Analyzer distinguishes various protocols by TCP/UDP port numbers or tag names in logs. There are may predefined protocols in Firewall Analyzer. You can refer all of them through navigating **Settings -> Admin Settings -> Protocol Groups** as Figure 29.

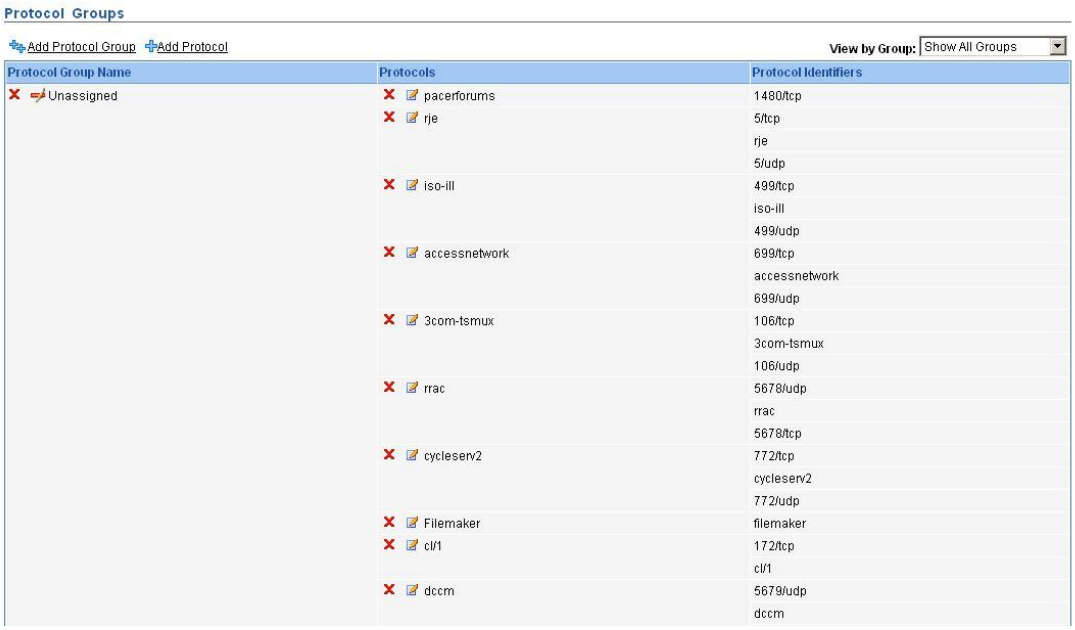


Figure 29: Protocol Groups

You can add a new protocol by following below steps.

Step1: click Add Protocol to open add new protocol pop out.

Step2: fill out group name and choose proper protocol group as Figure 30.

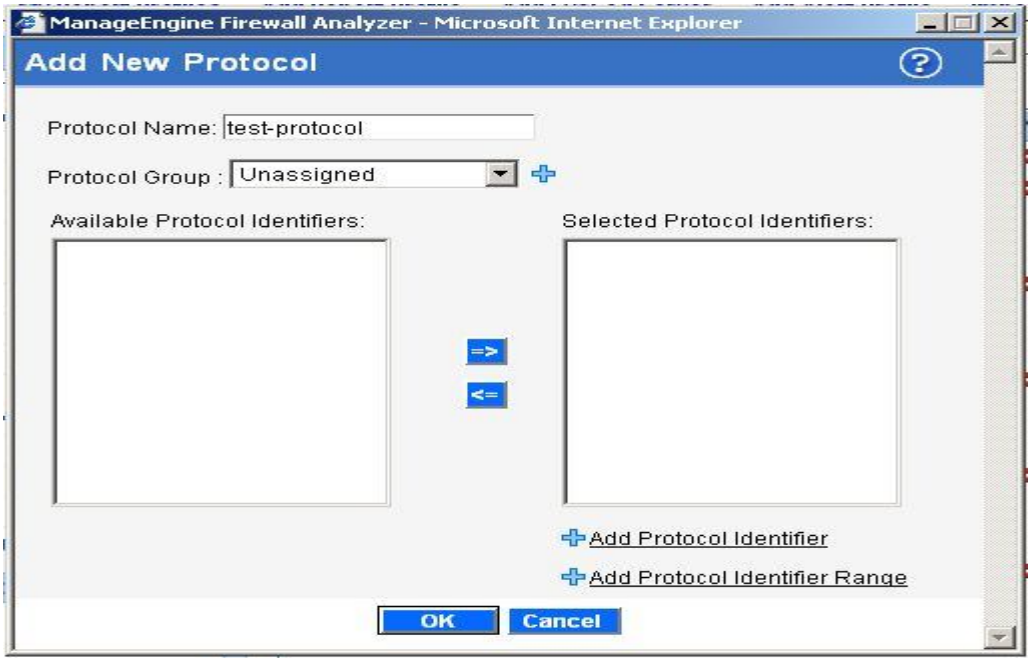


Figure 30: Add New Protocol

Step3: Click Add Protocol Identifier and input identifier in pop out. The identifier 1863/TCP means TCP port 1863 and 1863/UDP is for UDP port 1863 as Figure 31. You also can input tag names directly.

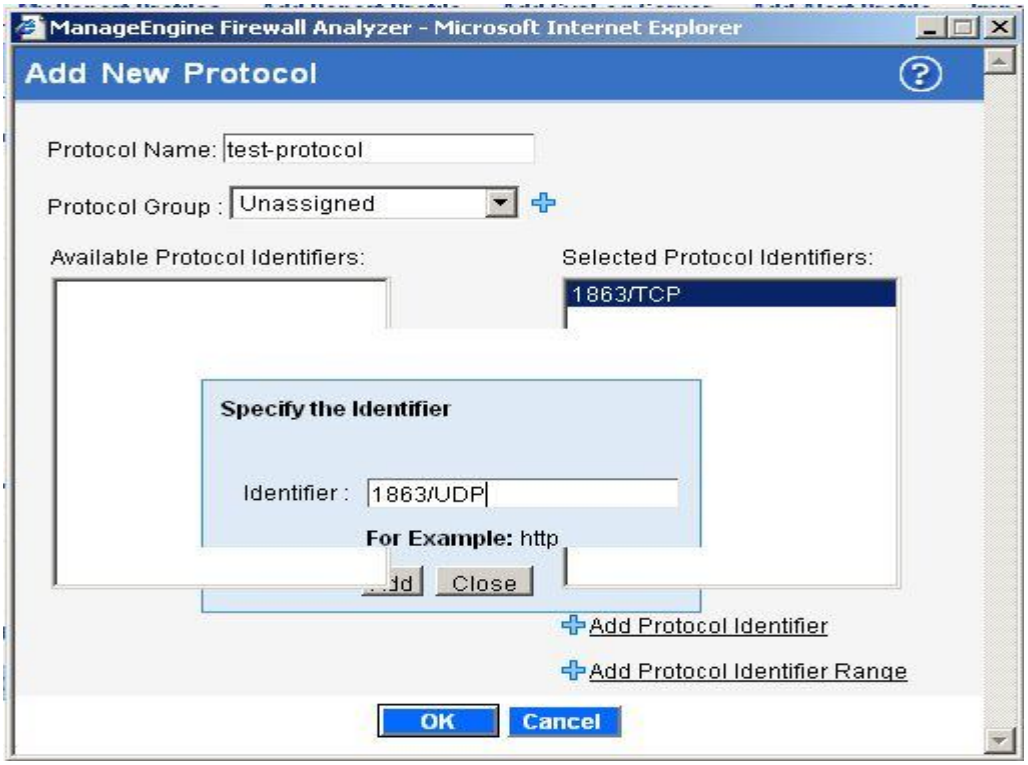


Figure 31: Specify Protocol Identifier

Step4: review all selected protocol identifiers as Figure 32. If you want to remove a protocol identifier, just move it to the left side – Available Protocol Identifiers.

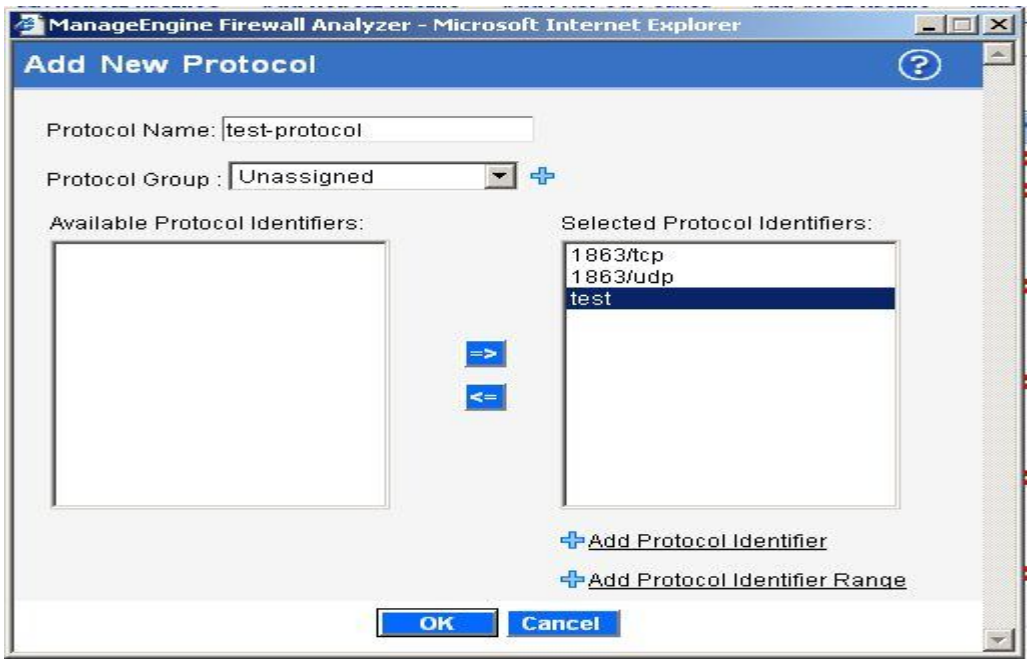


Figure 32:

Appendix

Configure user authentication for Internet access

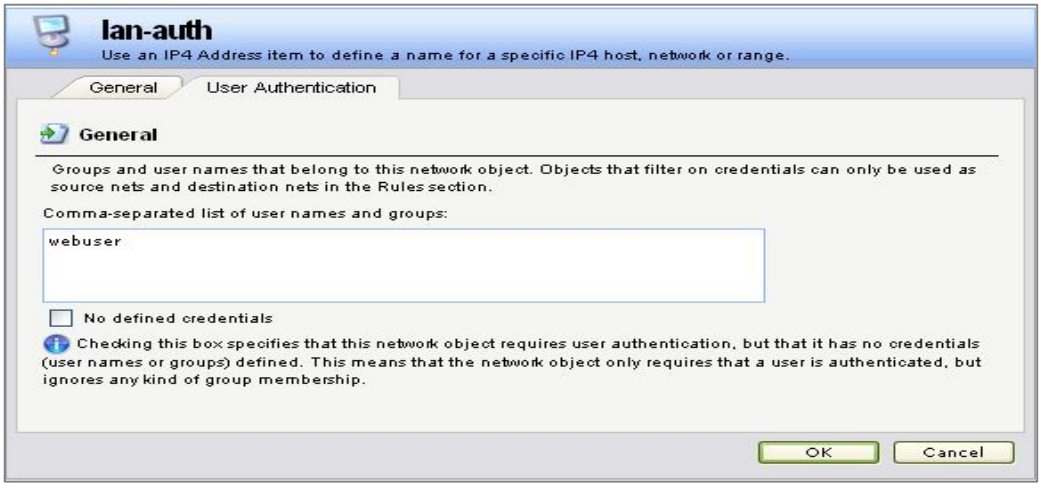
Here we only summarize the key steps of authentication configuration. Please refer to *Configure User Authentication for Internet Access* for more details.

1. Create a new network object for authenticated users –

   Refer to STEP 1 in *Configure User Authentication for Internet Access*

   Navigate to **Object->Address Book->Interface Address** and add a new IP4 address.

   Remember to add authenticated user names or groups in *User Authentication tab*.



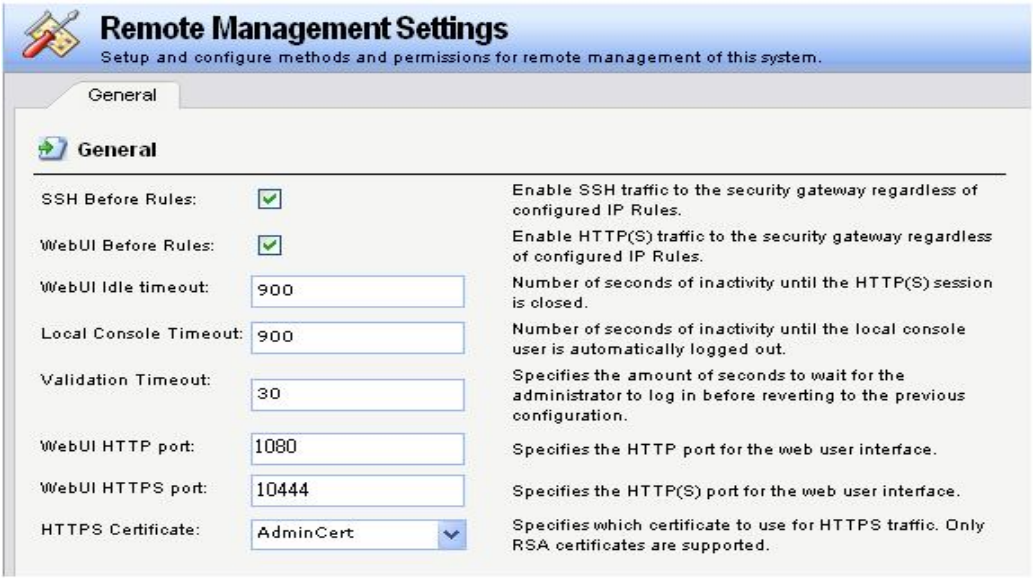
2. Change the port of Web console for latter Web access

   Refer to STEP 3 in *Configure User Authentication for Internet Access*

   Navigate to **System->Remote Management->Advanced Setting** and change

   WebUI HTTP port to any unused port beyond 1024, e.g. 1080

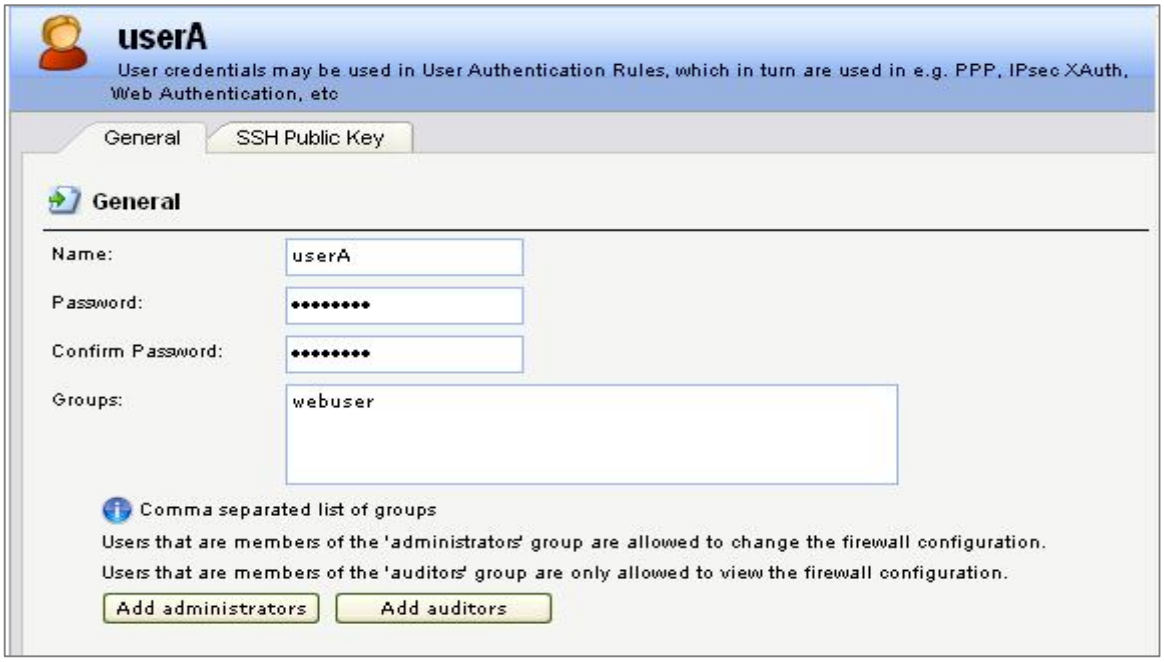
   WebUI HTTPS port to any unused port beyond 1024, e.g. 10444



3. Add authenticated users in Local User Database

   Refer to STEP 4 in *Configure User Authentication for Internet Access*

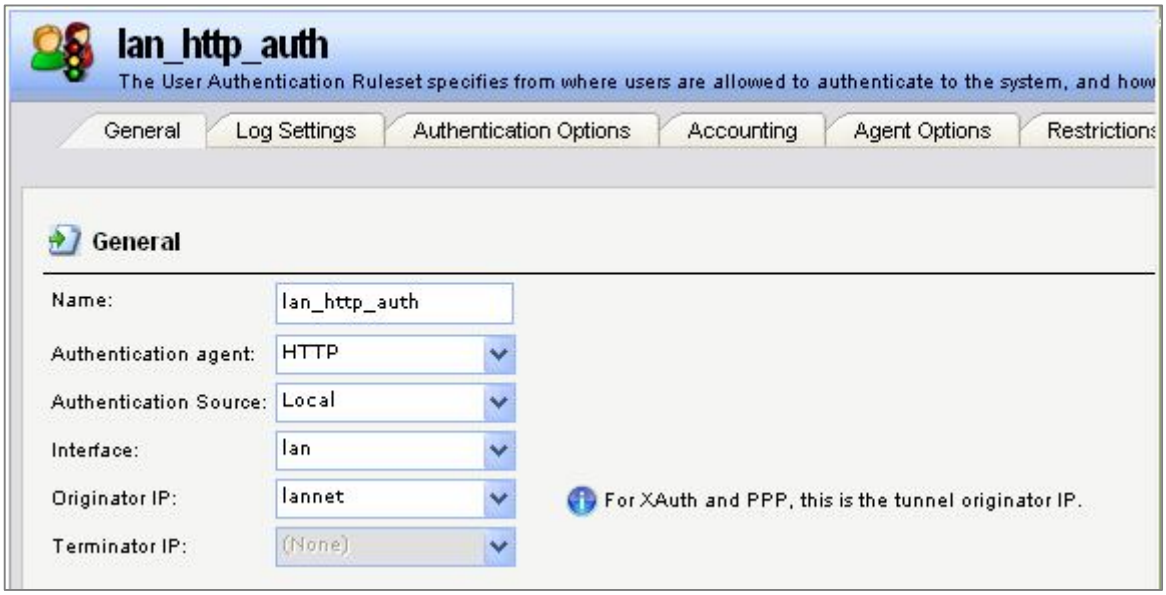
   Navigate to **User Authentication -> Local User Database** and create the user authentication database for user name and password. Remember groups of a new user should be the same as the group marked in the *User Authentication* of the network object in step 1.



4. Set User Authentication Rules

   Refer to STEP 5 in *Configure User Authentication for Internet Access*

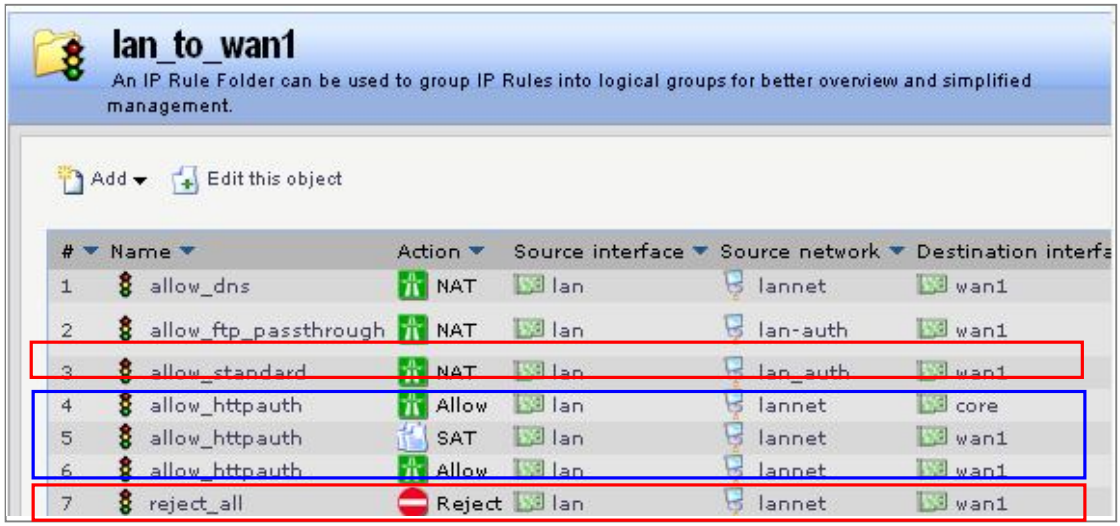
   For reporting accuracy, I recommend select “allow one login per username, disallow the rest” in Restrictions tab when you create the user authentication rule.



5. Set IP Rules

   Refer to STEP 6 in *Configure User Authentication for Internet Access*

   There are three HTTP services IP rules relative to authentication process – one defines the internal connections to firewall and the others regulate the connections to external network (rule 4, 5 and 6, grouping with blue border). Two additional rules are set to allow that only authenticated traffic can pass through firewall (rule 3 and 7, grouping with red border). lan-auth is the Interface address of authenticated users set in step 1. The SAT action of IP rules, allow_httpauth, transfers unauthenticated HTTP traffics to firewall for further authentication process.



   Remember the order of IP rules is very important to the authentication process.

6. Save and active the configuration

   Bare in mind that next time you want to connect to the web console page, add port number in the address, for example, http://192.168.1.1:1080 or https://192.168.1.1:10443 in this example.

Retrieve the saved logs from database

Firewall Analyzer archives all original logs received from syslog server to save disk space and also works like a logs database for further reference. If a IT staff wants to retrieve saved logs for depth analysis, they can navigate to Settings -> System Settings -> Archived Files to obtain them.