- 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.

2

Installation

Firewall analyzer step by step installation

Step 1: Double click ManageEngine_FirewallAnalyzer_7

Step 2: Select Advanced	Install
-------------------------	---------

ManageEngine Firewall Analy	yzei 7 🔀
	Welcome to the InstallShield Wizard for ManageEngine Firewall Analyzer 7
	One-Click Install Choose this option to install Firewall Analyzer in a single step. This means that you agree to the product licensing terms, and Firewall Analyzer will be installed with the following specifications:
	C:\ManageEngine\Firewall WebServer Port 8500 Install and Start as Service Language of Installation: English
AN I	Advanced Install Choose this option to specify custom settings for the Firewall Analyzer installation.
	Note: Minimum system requirements for Firewall Analyzer is 512 MB of RAM* 1 GB of disk space* *Please visit www.fwanalyzer.com for further details
	Advanced Install > One-Click Install > Cancel

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

ManageEngine Firewall Analyzer 7			×
License Agreement Please read the following license agreeme	nt carefully.		
Press the PAGE DOWN key to see the res	st of the agreement.		
ManageEngine Firewall Analyzer 7 Copyright (c) 2010 ZOHO Corp. All rights r This License Agreement details the policy Analyzer (Licensed Software) on the follow	eserved. for license of Manage ving topics:	Engine (R) Firew	all
(1) Evaluation License (2) Commercial License (3) Technical Support			<u>~</u>
Click Yes to agree to the terms of this licer Click No to quit the installation.	ise agreement, and pro	ceed with the in	istallation.
InstallShield	< <u>B</u> ack	Yes	<u>N</u> o

Step 4: Selecting "Standalone Edition"

Lunio	Select the Edition you wish	to install		
 State 	ndalone Edition			
	Suitable for Small - Medium Bu unlimited devices with premiur	usiness (SMB) requiring s n features. Trial version (single installation expires in 30 days	Analyze :
C Dis	tributed Edition			
	Suitable for Large Enterprise I distribution capability. Provisio provides consolidated view th expires in 30 days.	for high scalability. Inclue on for multiple installation nrough Admin Server We	des all premium fe i of Firewall Analy: eb Console, Trial v	atures plus zer and version
tallShiel	d			

Step 5: Choose Destination Location

oose Destination Location	
Select folder where Setup will install fi	ïles.
Setup will install ManageEngine Firew	vall Analyzer 7 in the following folder.
To install to this folder, click Next. To	install to a different folder, click Browse and select
another tolder.	
- Destination Folder	
Destination Folder	Browse
Destination Folder C:\ManageEngine\Firewall	Bīowse
Destination Folder C:\ManageEngine\Firewall allShield	Bīowse

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.

Select the Firewal	l Analyzer WebServer p	ort and the language for	rinstallation	
Firewall Analyzer u If you want to use	ses 8500 as the default a different web server p	web server port. ort, enter the port numbe	er here.	
Web Port	8505			
Language of Installation :	English	•		
Web Protocol	http	•		
Note :Please ens	sure that your web brows	er supports the chosen	language	

Step 7: Unselect "Install Firewall Analyzer as service"

ManageEngine Firewall Analyzer 7	<
Windows Service	
This option will install ManageEngine Firewall Analyzer 7 as a Windows service	
Install Firewall Analyzer as service	
InstallShield	_
< <u>B</u> ack <u>N</u> ext > Cancel	

Step 8: Name the Program Folder

Setup will add program i	cons to the Progra	m Folder listed below rs list Click Next to r	. You may type a	new folder
Program Folders:	The children produc	To list. Click Heat to	sonande.	
ManageEngine Firewall	Analyzer 7			
Evisting Folders:				
Dell QuickSet				
Dell Tools				
D-Link VPN Client				
ESTsoft				_
FileZilla FTP Client				
Intel PRUSet 無縁 Java 2 Buntime Enviror	oment			

Step 9: Click next to start copying files

ManageEngine Firewall Analyzer 7		
Start Copying Files Review settings before copying files.		
Setup has enough information to start co change any settings, click Back. If you copying files.	pying the program files. If you want to are satisfied with the settings, click Ne	review or xt to begin
Current Settings:		
Installation Directory : C:\ManageEngine Programs Folder : ManageEngine F Web Server Port : 8505	e∖Firewall ïrewall Analyzer 7	
		<u>~</u>
		2
InstallShield		
	< <u>B</u> ack <u>Next</u> >	Cancel

Step 10: Skip Registration process

Registration for Technic Enter Your Details below	cal Support (O	ptional)		
Name				
E-mail Id				
Phone				_
Company Name	<u> </u>			
Country	_			
allShield				
		/ Back	Neuts	Skip

Step 11: Finish Firewall Analyzer installation

ManageEngine Firewall Analy	zer 7
	InstallShield Wizard Complete Setup has finished installing ManageEngine Firewall Analyzer 7 on your computer.
	✓ Yes, I want to view readme file ✓ Start Firewall Analyzer Server Technical support: fwanalyzer-support@manageengine.com
	K <u>B</u> ack Finish Cancel

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.

Building Networks for People	Augged in as administrator admin - 192.168.1.30
🗞 Home 🛛 💥 Configuration 🗸 🖌 Tools 🗸 🛛 🔕 Status 🗸 🐁 Maintenance 🗸 🛛 😸 Setup Wizard	🗳 Logout 👔 Help
Pr1-800 Image: Data and Time Image: Data and Time	Comments V The internal logger in the firewall (Right-slok on a row for additional options.



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

Sys	log Receiver	receive log events from the	em in the standard Syslog	format.		
General	SeverityFilter	Message Exception				
🕑 Gener	al					
Name:	syslog_client					
IP Address:	192.168.1.30	*				
Facility:	localO	~				
Port:	514					
🛃 Comm	ents					
Comments:	Firewall analyzer	iosts on 192.168.1.30				
	7.					
						OK Cancel

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.

Severity	Message Exceptions	
ailable	Selected	
') Debug	(1) Emergency (1) Alert (2) Critical (3) Error (4) Warning (5) Notice (6) Info	

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.

	P2c Event Receiver 20 event receiver is used to receive SNMP events from the system.	
General	SeverityFilter Message Exceptions	
🛃 General	I. Contraction of the second se	
Name:	SNMP_Trap	
IP Address:	192.168.1.30 🗸	
Port:	162	
Repeat Count	0	
Community:	public	
🛃 Comme	ents	
Comments:	SNMP server hosts 192,168,1.30 with community "public"	
		OK Cancel

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).

A SNMF2c event receiver is us General SeverityFilter	to receive SNUP events from the system. Message Exceptions	
yseventy Available	Selected	
(7) Debug	() Emergency (1) Alert (2) Critical (3) Error (4) Warning (≤) Notice (6) Info	

Figure 5: SNMP2c Event Receiver configuration, SeverityFilter tab

You can list all of receivers as below Figure 6.

🚹 Add 👻 🚿 Advanced Settir	ngs			
Vame 🔻	Туре 🔻	IPAddress 💙	Port 💌	Comments 🔻
MemLog	Memory Log Receiver			The internal logger in the firewall
SNMP_Trap	SNMP2c Event Receiver	9 192.168.1.30	162	SNMP server hosts 192.168.1.30 with community "public"
yslog_client	Syslog Receiver	9 192.168.1.30	514	Firewall analyzer hosts on 192.168.1.30
				(T) Right click on a row for additional option

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.

Kog Settings		
General		
🔊 General		
Send Limit: 2000	Limits how many log packets the security gateway may send out per second.	
		OK Cancel

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.

ManageEngine Firewall Analyzer 6		ManageEngine)
 In-depth firewall, proxy server and VPN reporting Built-in database Customized Reports Totally web-based access 	E 5.5+ or Mozilla 1.5+ or Nelscape 7.0+ at a screen resolution	Sign In here User Name Password Login First time users use 'admin' as User Name and 'admin' as Password to login. of 1024 X 768 pixels.
\mathbb{C} 2009 <u>ZOHO Corp.</u> All Rights Reserved		E-wall : <u>twanaiyzer-supportigimanageengine.com</u> Website : <u>www.fwanalyzer.com</u>

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.

ewall Analyzer 6	Home Reports Alerts Settings Ask ME Support	2 Search Here
e Reports My Report Profiles	Add Report Profile Add SysLog Server Add Alert Profile Import Logs Advanced Search	I 🗳 🗄
Welcome to Firewall	Analyzer	
	No firewall is currently exporting logs to Firewall Analyzer Troubleshoot	
2 To not at	arted you can i	
₩¥¥ To get st	inea, you can :	
EC	Configure your firewall Configure your firewall Configure your firewall Analyzer running at two on ports 1514 & 514	
	How do I do this?	
6	Add Syslog Server	
	Y Aud anomer port on which Friewan Analyzer can insten for incoming logs	
	Import Log Files Import logs from this machine or a remote machine.	
😢 If you wa	nt to test Firewall Analyzer, you can:	
🗭 lf you wa	nt to test Firewall Analyzer, you can:	
😵 If you wa	Init to test Firewall Analyzer, you can: Simulate Generate reports from sample firewall logs. You can later turn this off from the Settings tab.	

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.

SysLog Server	IP Address	Port	Status	Action
SysLogServer-2	192.168.1.31	1514	OUP	x
SysLogServer-1	192.168.1.31	514	OUP	• ×
Add SysLog Server				
	SysLog Server Name	*		
	Host Name/IP Address 192.1	68.1.31 *		
	SysLog Server Port	*		
	А	dd SysLog Server		
*Mandatory Fields				

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).

	No firewall is currently exporting logs to Firewall Analyzer <u>Troubleshoot</u>	
🎗 To get starte	ed, you can :	
🗐 🥅 «	Configure your firewall Started receiving data. Reports will be generated in few seconds	
	How do I do this?	
6	Add Systog Server Add another port on which Firewall Analyzer	
	Import Log Files Import logs from this machine or a remote machine.	
? If you want t	to test Firewall Analyzer you can	

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.

Dashboard				From: 2008-08-10 00:00:00 To: 2008-08-10 16:25:00
Traffic Overview		Security Overview		
Data available on 19 Sep 2001.	Adjust Calendar	E Events	No Data Available	
Device			Device	
Traffic Statistics Security Statistics				Show Top 5
Device Name	Protocol Group	Traffic IN (MB)	Traffic OUT (MB)	Total Traffic (MB)
🖾 🗙 192.168.1.1	÷-	0	0	0

Figure 12: a synchronized firewall shown in the home page

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

irewall Name	192.168.1.1
irewall IP	192.168.1.1
)isplay Name	DFL-860
endor Type	Clavister Firewall
own link Speed (in Kbps)	1024.0
Jp Link Speed (in Kbps)	1024.0

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"

Interface Live Reports	Dashboard (Last 24 Hours)	From: 2008-08-09 16:42:3 To: 2008-08-10 16:42:3
Device - Interface details	[Set Global SNMP Parameters]	Show All Hide All
🗢 Device Name		
DFL-860	No interface details available in logs.	
Ouick Note Interface based Live Drilldown the Interface	report details for the last 24 hours ce name to get more details on IN/OUT traffic information.	
	Figure 14: Interface Live Reports Da	ashboard

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

onfigure Interface D	etails
Device Name SNMP Community SNMP Port	: All Devices : public : 162
Note: Above configured SI to query the device t	NMP parameters will be used o get interface details
	Save Cancel

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.

ManageEngine)			Teira mena upgrade License Heip Feedback About Logout (adm
Firewall Analyzer 6	Home Reports Alerts Settings Ask ME	E Support	2 Search Here
Live Reports My Report Profiles	Add Report Profile Add SysLog Server Add Alert Profile	Import Logs <u>Advanced Search</u>	I 💕 🗏 😫
Settings			
SysLog Server Settings 🛞	Simulate Generate reports from sample fir	rewall logs	
Checkpoint Firewall Settings			
Alert Profiles	System Settings		
Imported Log Files	SysLog Server Settings	Imported Log Files	Schedule Listing
Device Details	Configure SysLog Servers	Import Log Files	Marcon View List of Schedules
Archived Files	Checknoint Firewall Settings	Device Details	Working Hour
Schedule Listing	Configure Checkpoint Firewalls	View Log Details and Schedules	Configure Working Hours
Working Hour			
Customize Report	View Alert Profiles	View Archived Log Files	Customize Report Customize the reports view
Configure DNS			
Device Rule	Configure DNS	Device Rule	Rebranding FWA WebClient
Rebranding FWA WebClient	- Conligure DNS Seturigs	Conligare to view Osed/Onused Rales.	Rebrand FWA Client logo,images & links
Protocol Groups			
Intranet Settings	Admin Settings		
User Management	Protocol Groups	Mail Server Settings	Database Console
Mail Server Settings	Classify Protocols into Protocol Groups	Configure Mail server	Access Firewall Analyzer Database
Data Storage Options	Intranst Cottings	Growall Availability Mort	C Licence Management
	Configure Internal Networks	Alert when firewalls stop sending logs	Manage and UnManage Devices
Database: 1 year 💌			
Log Archive: Forever 💌	User Management View Users and Access Levels	Server Diagnostics View Server Details	SMS Settings Configure SMS Service
Update			3113

Figure 16: Settings

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

Intranet Settings		
Configure all devices		
Device Name	Intranet Settings	Action
DFL-860	No Intranets configured.	Change



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.

	No Intra-Network is configured.
pecify Network , IP Ra	ange, or IP Address
FL-860 💌	
	Network 1921681.0
	1000001 00.100.100 100000 (200.200.200.0000
lore Fewer	
	Save Settings Cancel
ρ	
IMPORTANT : Tr	ry to give minimum ranges/networks as much as possible.
For Everaple : 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 have the separately and the separately
FUI Example . II	
recommend you	I to give the entire private IP network . To.o.o.o with Net Mask 255.0.0.0 , as this would improve the performance.

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.

Irewall An	alyzer 6	Home	Reports	Alerts	Settings	Ask ME	Support	
Live Reports	My Report Profiles	Add Report Pr	rofile Add S	SysLog Serve	er Add Ale	rt Profile	Import Logs	Advanced Search

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

ect Devices and Filters		Select Report Type and Schedule	
ct Devices and Filters			
Report Profile Name	report profile 1		
Select the devices			
Select All Devices		Selected Devices	
DFL-860 [Firewall]		1	
Choose the Filters			
Choose the Filters 슈 <u>Add 타Select XRemove</u>	<mark>⇔∕Edit</mark>	Instant Help:	
Choose the Filters 슈 <u>Add 타Select XRemove</u>	<mark>⊯≯Edit</mark>	Instant Help: To use already created filters, click on the 'Select' link and select the existing filters To create a new filter, Click on the 'Add' link	

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.

ct Devices and Filters		2 Select Repo	ort Type and Schedule	
t Report Type and Schedu	le			
ect Report Type				
vailable Reports				
✓ Select All Reports ✓ Inbound & Outbound Traffic ✓ Intranet Reports ✓ Firewall Live Reports ✓ Freewall Live Reports ✓ Freewall Reports ✓ Froxy Usage (Prexy only) ✓ Security Reports PAdd Chedule & Email Options		Save generated report	t as : for PDF Reports	
Send report a	as: © PDF C CSV			
		C 10/a alder	C. Manuficha	C Only once

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.

ManageEngine	nalvzer 6	Home	ports Alerts	Settings	Ask ME	Supp	ort
Live Reports	My Report Profiles	Add Report Profile	Add SysLog Serve	er Add Ale	rt Profile In	nport Lo	gs Advanced Search
		Figure	22: sub func	tion bar			
I Reports	Add Report Profile 😘 Export	Report Profiles I 🐼 Import Re	mort Profiles				Show
Report Profile Name	Created or		Last Ger	nerated Reports		Action	
							Scheduler Assigned

Figure 23: My Report Profiles

¥

Reports Across Devices

Firewall Reports

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

urts.
incel
Want to configure DNS entries manually? <u>Click Here</u>
that will be used in all reports. If you see any IPAddresses, you can try clicking hine.
for the ip's shown in the report page when you click the 'ResolveDNS' link.

Figure 25: Resolve DNS configuration

If choosing manually resolve DNS, you can click the icon Resolve DNS 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.

Device Details						
Supported Logs Receiv	ed					
Device Name	Device Type	Last Update Time	Syslog Port	Status	Action	Manage Status
DFL-860	Firewall	⊘ X	0			
Unsupported Logs Reco	aived					
Device Name	Syslog server	Syslog Port	Record Fe	ormat	Notification	Action
		No	Data Available			
Schedules Executed						
Report Profile	Schedule		Last Executed		Status	
		No	Data Available			

19

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.

1.543		Aug	ust 2	008			
«	<	ridg	Today	000	> +	* .	
Sun Mon		on Tue Wed		Thu	Fri	Sat	
					1	2	
3	4	5	6	7	8	9	
10	11	12	13	14	15	16	
17	18	19	20	21	22	23	
24	25	26	27	28	29	30	
31							
		Se	lect da	te			

Date	Time Range	
	Select Range	
Time: 🔽	ustom Range 📃	•
From: 20	008-08-13 00:00:00	
To: 2	08-08-13 12:30:00	-

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.

gure Working Hour details		
General	C Advanced	
	Start Time 10 💌 Hrs.	
	End Time 20 💌 Hrs.	
	Save Cancel	
Quick Note		
 General Configure general working h 	our range. This configuration will help you to distinguish between Working a	nd Non-working hour reports
Advanced Configure multiple updation is	european This configuration will belonge to distinguish between Washing	and Non-working hour reports

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.

Add Protocol Group		View by Group: Show All Groups	
Protocol Group Name	Protocols	Protocol Identifiers	
🗙 🥩 Unassigned	🗙 📝 pacerforums	1480/tcp	
	🗙 📝 rje	5/tcp	
		rje	
		5/udp	
	🗙 📝 iso-ill	499/tcp	
		iso-ill	
		499/udp	
	🗙 📝 accessnetwork	699/tcp	
		accessnetwork	
		699/udp	
	🗙 📝 3com-tsmux	106/tcp	
		3com-tsmux	
		106/udp	
	🗙 📝 rrac	5678/udp	
		rrac	
		5678/tcp	
	🗙 📝 cycleserv2	772/tcp	
		cycleserv2	
		772/udp	
	🗙 📝 Filemaker	filemaker	
	🗙 📝 cl/1	172/tcp	
		cl/1	
	🗙 📝 dccm	5679/udp	
		dccm	

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.

	?
▼ ♣	
Selected Protocol I	dentifiers:
~	
	Selected Protocol I

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.

ManageEngine Firewall Ana	lyzer - Microsoft Internet Explorer	
Add New Protocol		2
Protocol Name: test-protoco	[]	
Protocol Group : Unassigne	d 🔄 🛧	
Available Protocol Identifiers	: Selected Protocol Identifiers:	
	1863/TCP	
	л. н	
Specify the l	dentifier	
Identifier :	[1863/UDP]	
	For Example: http	
I		
	Add Protocol Identifier	
	Add Protocol Identifier Ran	qe
	OK Cancel	

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.

Retard Name: test-protocol		3
Protocol Group : Unassigned	• •	
Available Protocol Identifiers:	Selected Protocol Identifie 1863/tcp 1863/udp test	ers:
	♣ <u>Add Protocol Identifier</u> ♣ <u>Add Protocol Identifier</u>	Range

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*.

s can only be used as
s can only be used as
t it has no credentials r is authenticated, but
-

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

General		
🛃 General		
SSH Before Rules:		Enable SSH traffic to the security gateway regardless of configured IP Rules.
WebUI Before Rules:		Enable HTTP(S) traffic to the security gateway regardles of configured IP Rules.
WebUI Idle timeout:	900	Number of seconds of inactivity until the HTTP(S) sessio is closed.
Local Console Timeout:	900	Number of seconds of inactivity until the local console user is automatically logged out.
Validation Timeout:	30	Specifies the amount of seconds to wait for the administrator to log in before reverting to the previous configuration.
WebUI HTTP port:	1080	Specifies the HTTP port for the web user interface.
WebUI HTTPS port:	10444	Specifies the HTTP(S) port for the web user interface.
HTTPS Certificate:	AdminCert	Specifies which certificate to use for HTTPS traffic. Only RSA certificates are supported.

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.

General	H Public Key	
シ General		
Name:	userA	
Password:	•••••	
Confirm Password:	•••••	
Groups:	webuser	
🚯 Comma sepa	rated list of groups	

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.

General	Settings Auth	henticatio	on Options Accounting Agent Options Restriction
🔊 General			
Name:	lan_http_auth		
Authentication agent:	нттр	~	
Authentication Source:	Local	~	
Interface:	lan	~	
Originator IP:	lannet	*	OF For XAuth and PPP, this is the tunnel originator IP.

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). Ian-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, <u>http://192.168.1.1:1080</u> or <u>https://192.168.1.1:10443</u> 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.