

SECURITY
ANALYTICS
SYSTEM



Essential Security, Application and System Analytics™

About eIQnetworks

Mission

Deliver best of breed **Security, Application and System Analytics Solutions**, and become the industry standard **Reporting SOLUTION**.

▪ Value Proposition

Allow IT Managers, and Network Administrators to make informed decisions:

- Find *who-what-when-where-how* of application, server & network activity
- Correlate, analyze and report to identify security breaches and viruses
- Improve server, network and application performance & uptime
- Trend analysis for capacity planning, forecasting and fine tuning QoS policies
- Enforce corporate policies by understanding employee web usage
- Enable cost allocation & billing

▪ Founded in 2001 & Privately Held

- 50 plus Employees
- Over 100 channel partners worldwide
- Cisco AVVID Partner & Microsoft Gold Certified Partner. Partnerships with several leading Firewall Vendors including Fortinet, TopLayer, NetContinuum, Astaro, IntelliReach, etc.

▪ Experienced Team

- Proven track record of developing enterprise class Reporting, Monitoring and Analysis solutions.



▶ What We Do...

○ Firewalls

○ VPNs

○ IDS & IPS

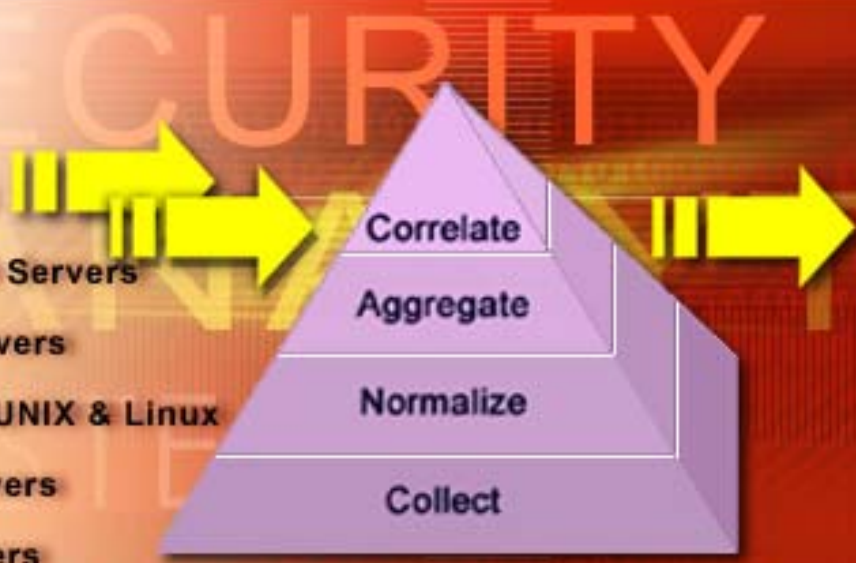
○ Anti Virus Servers

○ Proxy Servers

○ Windows, UNIX & Linux

○ eMail Servers

○ Web Servers



eIQ Security, Application and System Analytics



Role of Reporting in Security Management

- How to measure effectiveness of your current network perimeter defenses & readiness
- Using reporting to identify problem areas
- Using reporting to better tune your defenses against attacks and virus

Measuring Network Readiness – Log Analysis

- Network devices and servers like Routers, Firewalls, VPNs, IDS/IPS, Proxy servers, etc. record and stream rich activity in Syslog Messages
- Unfortunately this information is saved in **separate** and difficult to read **cryptic** logs
- Need to **correlate** data across variety of Network devices and servers to obtain actionable and valuable information

```

datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B0 interface is not protected by the anti-
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B7 interface is not protected by the anti-
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B1 interface is not protected by the anti-
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The NDISWANIP interface is not protected by the ar
datetime=21Jul2003 03:26:31 action=ctl fw_name=corp_fw dir=inbound
datetime=21Jul2003 03:26:32 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.73.103.1 rule=3 proto=tcp/Fw1_lea
datetime=21Jul2003 03:26:32 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.73.103.1 rule=3 proto=tcp/Fw1_lea
datetime=21Jul2003 03:26:58 action=accept fw_name=corp_fw dir=inbound src=10.79.109.134 dst=10.79.109.755 rule=2 proto=udp/nbr
datetime=21Jul2003 03:27:35 action=accept fw_name=corp_fw dir=inbound src=10.74.104.1 dst=10.74.104.755 rule=2 proto=udp/nbdat
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B0 interface is not protected by the anti-
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B7 interface is not protected by the anti-
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The E100B1 interface is not protected by the anti-
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound sys_msgs=The NDISWANIP interface is not protected by the ar
datetime=21Jul2003 03:27:50 action=ctl fw_name=corp_fw dir=inbound
datetime=21Jul2003 03:27:50 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.73.103.1 rule=3 proto=tcp/Fw1_lea
datetime=21Jul2003 03:27:50 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.73.103.1 rule=3 proto=tcp/Fw1_lea
datetime=21Jul2003 03:28:02 action=accept fw_name=corp_fw dir=inbound src=10.75.105.1 dst=10.75.105.755 rule=2 proto=udp/nbdat
datetime=21Jul2003 03:28:02 action=accept fw_name=corp_fw dir=inbound src=10.79.109.134 dst=10.79.109.755 rule=2 proto=udp/nbr
datetime=21Jul2003 03:28:21 action=accept fw_name=corp_fw dir=inbound src=10.76.106.1 dst=10.76.106.755 rule=3 proto=udp/nbdat
datetime=21Jul2003 03:28:21 action=accept fw_name=corp_fw dir=inbound src=10.75.105.1 dst=10.75.105.755 rule=3 proto=udp/nbnan
datetime=21Jul2003 03:28:23 action=accept fw_name=corp_fw dir=inbound src=10.74.104.1 dst=10.74.104.755 rule=3 proto=udp/nbdat
datetime=21Jul2003 03:28:23 action=accept fw_name=corp_fw dir=outbound src=10.1.3.1 dst=10.1.3.755 rule=2 proto=udp/nbname
datetime=21Jul2003 03:28:36 action=accept fw_name=corp_fw dir=inbound src=10.1.3.103 dst=10.79.109.134 rule=2 proto=tcp/135
datetime=21Jul2003 03:28:36 action=accept fw_name=corp_fw dir=inbound src=10.1.3.103 dst=10.79.109.134 rule=2 proto=tcp/1543
datetime=21Jul2003 03:28:48 action=accept fw_name=corp_fw dir=inbound src=10.78.108.1 dst=10.78.108.755 rule=3 proto=udp/nbnan
datetime=21Jul2003 03:29:03 action=accept fw_name=corp_fw dir=inbound src=10.74.104.1 dst=10.74.104.755 rule=3 proto=udp/nbnan
datetime=21Jul2003 03:29:03 action=accept fw_name=corp_fw dir=inbound src=10.79.109.134 dst=10.79.109.755 rule=3 proto=udp/nbr
datetime=21Jul2003 03:29:36 action=accept fw_name=corp_fw dir=inbound src=10.71.101.1 dst=10.71.101.755 rule=3 proto=udp/nbnan

```

Measuring Network Readiness – Reporting

Attack Reports

Attack Source	Event Code	Description	# of Attacks	% of Attacks
172.18.1.55	103284777	web-iis: asp-dot attempt	36	0.16
	103284790	web-iis: fpcount attempt	6	0.03
	102957134	web-cgi: calendar access	4	0.02
	103284791	web-iis: fpcount access	4	0.02
	103481353	web-php: content-disposition	2	0.01

Virus Reports

Virus	Virus SubType	Severity Level	# of Occurrences
W32/MyDoom-mm	infected	Warning	145
W32/Netsky.D-mm	infected	Warning	61
W32/PetTick-mm	infected	Warning	33
W32/Netsky.K-mm	infected	Warning	32
W32/Bagle.O-zip	infected	Warning	28
			299

Internal User Reports

User	Site	Hits	% of Hits	Bytes Transferred
192.168.100.2	bannerserver.gator.com	13	1.01	58.56 KB
	216.217.36.143	4	0.31	46.49 KB
	us.f99.mail.yahoo.com	3	0.23	25.82 KB
	updateserver.gator.com	3	0.23	4.80 KB
	login.yahoo.com	3	0.23	3.53 KB
	windowsupdate.microsoft.com	2	0.16	34.54 MB

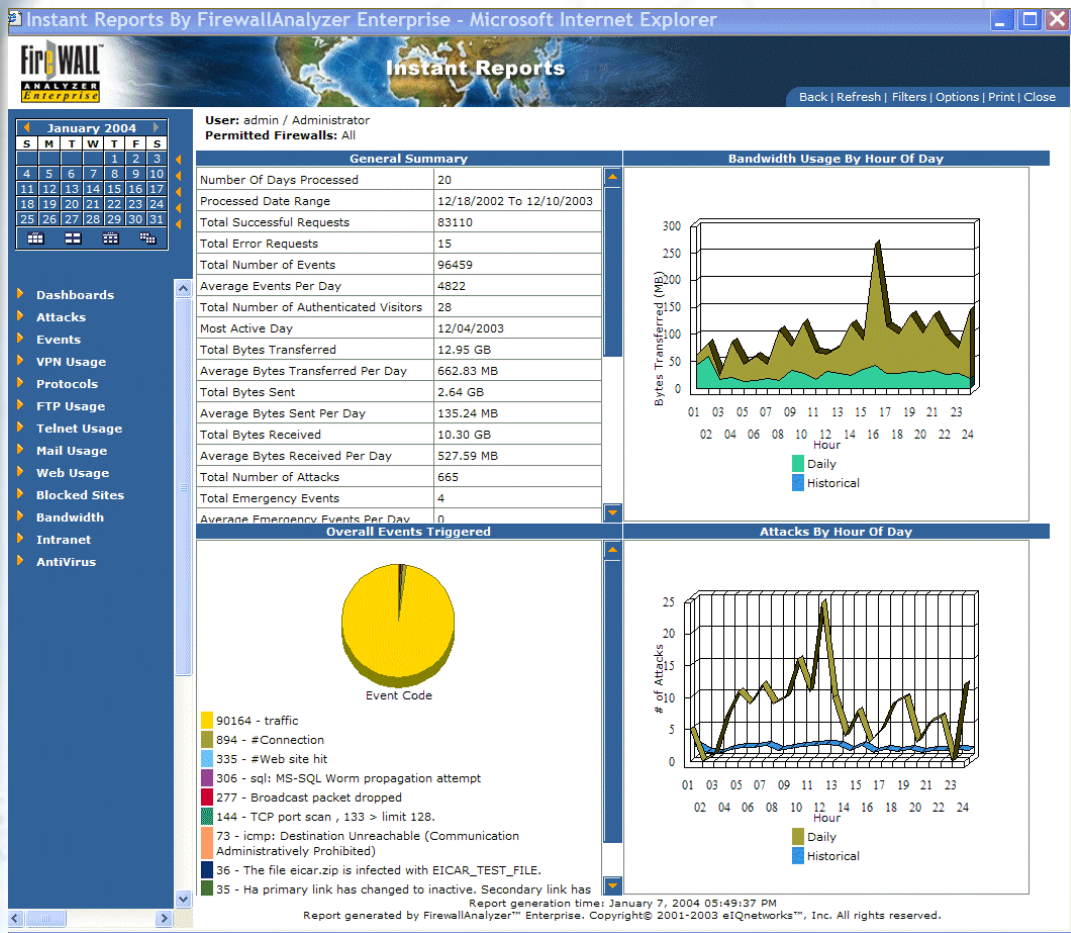


What You Can Get From Analyzing Logs

- Correlate to find security issues, hacker attacks, and security breaches
- Identify attack & virus details – type, source, destination, date & time, etc
- Analyze event severity and port of attack
- Understand protocol usage by user and department
- Understand employee/departmental web & protocol usage
- Find activity trends over time
- Audit firewall rules and events triggering the rules
- Audit VPN usage
- Utilize firewall logs for network and virus forensics
- Measure effectiveness of your Firewalls and ROI



Use Reporting to Identify Problem Areas



- Do you see a high % of Emergency, Critical or Error events?
- Is the same attack appearing across the entire network from same source?
- What is the bandwidth utilization by protocol and inbound vs outbound?
- Fine tune your QoS based on protocol bandwidth utilization.
- Is it time to upgrade your Firewall?
- Who is the rogue employee that is using your network to download large files?



Use Reporting to Identify Problem Areas

29	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	1	2	3

- ▶ Dashboards
- ▶ Attacks
 - Hourly Attack Type and
 - Daily Attack Type and
 - Attacks By Hour of Day
 - Attacks By Day
 - Attacks on Firewall
 - Attacks By Category
 - Top Attackers By Attack
 - Top Sources of Attacks
- ▶ Events
- ▶ VPN Usage
- ▶ Protocols
- ▶ FTP Usage
- ▶ Telnet Usage
- ▶ Mail Usage
- ▶ Web Usage
- ▶ Blocked Sites
- ▶ Bandwidth
- ▶ Intranet

Attacks By Category

Attacks By Category provides information about the Attacks on the Firewall for a certain category. Percentage columns percentage of Events.

Filters Applied

Date: 3/19/2004 To 3/24/2004

Event Code	Description	# of Attacks
1 287113220	SNMP public access udp	16342
2 102367238	scan: FIN	7050
3 6553601	portscan: 172.18.0.1 is port-scanning to port 15868 on internal (STEALTH)	3720
	portscan: 172.18.0.1 is port-scanning to port 15868 on external (STEALTH)	3707
4 103350293	web-misc: webdav propfind request	1927
5 17956879	icmp: Destination Unreachable (Communication Administratively Prohibited)	1131
6 6553603	portscan: Port-scan from 172.18.0.1 ends, total time(6s) hosts(2) TCP(0) UDP(0) STEALTH	1119
	portscan: Port-scan from 172.18.0.1 ends, total time(8s) hosts(2) TCP(0) UDP(0) STEALTH	930
	portscan: Port-scan from 172.18.0.1 ends, total time(5s) hosts(2) TCP(0) UDP(0) STEALTH	732
	portscan: Port-scan from 172.18.0.1 ends, total time(16s) hosts(2) TCP(0) UDP(0) STEALTH	505
7 286064643	dns: SPOOF query response with ttl: 1 min. and no authority	443
8 6553603	portscan: Port-scan from 172.18.0.1 ends, total time(4s) hosts(2) TCP(0) UDP(0) STEALTH	429
	portscan: Port-scan from 172.18.0.1 ends, total time(7s) hosts(2) TCP(0) UDP(0) STEALTH	402
9 7274504	topreassembly: STEALTH ACTIVITY (FIN scan)	395
10 102957134	web-cgi: calendar access	266
11 6553603	portscan: Port-scan from 172.18.0.1 ends, total time(15s) hosts(2) TCP(0) UDP(0) STEALTH	222
	portscan: Port-scan from 172.18.0.1 ends, total time(3s) hosts(2) TCP(0) UDP(0) STEALTH	209
	portscan: Port-scan from 172.18.0.1 ends, total time(16s) hosts(3) TCP(0) UDP(0) STEALTH	137
	portscan: Port-scan from 172.18.0.1 ends, total time(9s) hosts(2) TCP(0) UDP(0) STEALTH	114

- What are the most frequent attack types?
- What is the source and destination of attacks?
- Are attacks originating externally or internally?
- What Firewall and port # are the attacks appearing on?

▶ Attack Severity Details

- Attacks range from low risk to high risk.
 - An SNMP UDP request may pose a low risk,
 - Denial of Service attack is usually a high risk.

○ Firewalls

○ VPNs

○ IDS & IPS

○ An

○ Pr

○ Wi

○ et

○ We

>>> Attack Search

Search By ID...

Go

Public.Accesss.UDP

Attack Information

ID: 287113220

Class: SNMP

In-Depth Analysis

Description

Attackers can take advantage of SNMP v1 communities to gain access to a SNMP daemon.

Impact

Remote attackers to cause a denial of service or gain privileges on the victim system

Vulnerability

Any unprotected SNMP daemon system is vulnerable to the attack

References

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0012>

▶ Attack Severity Analysis

- Port Scans and IP/DNS spoofs are common attacks (moderate risk)
- IIS and CGI web based attacks are also common moderate to high risk threats
- In this real world example, Denial of Service (DOS) attacks were found from internal client address against a Cisco Router

172.18.8.53	102957134	web-cgi: calendar access	16
172.20.8.23	17956867	icmp: PING NMAP	16
172.18.8.160	103350435	web-misc: cisco /%% DoS attempt	15

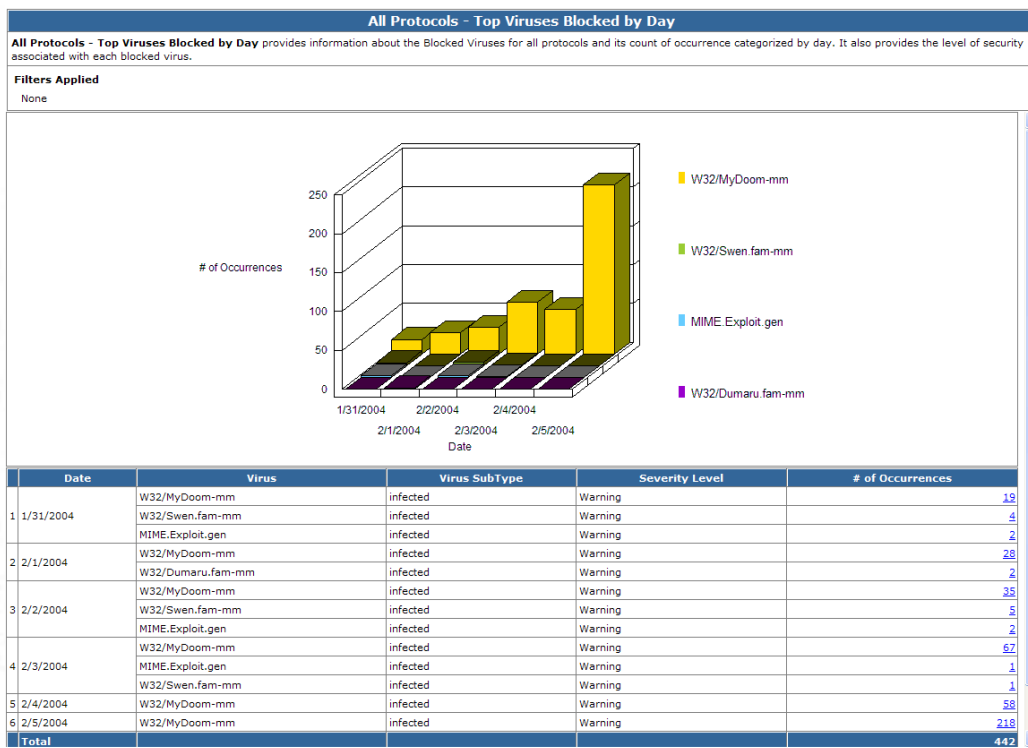
More information on Attack ID's →

Description	The IOS HTTP service in Cisco routers and switches running IOS 11.1 through 12.1 allows remote attackers to cause a denial of service by requesting a URL that contains a %% string.
-------------	--



Use Reporting to Identify Problem Areas

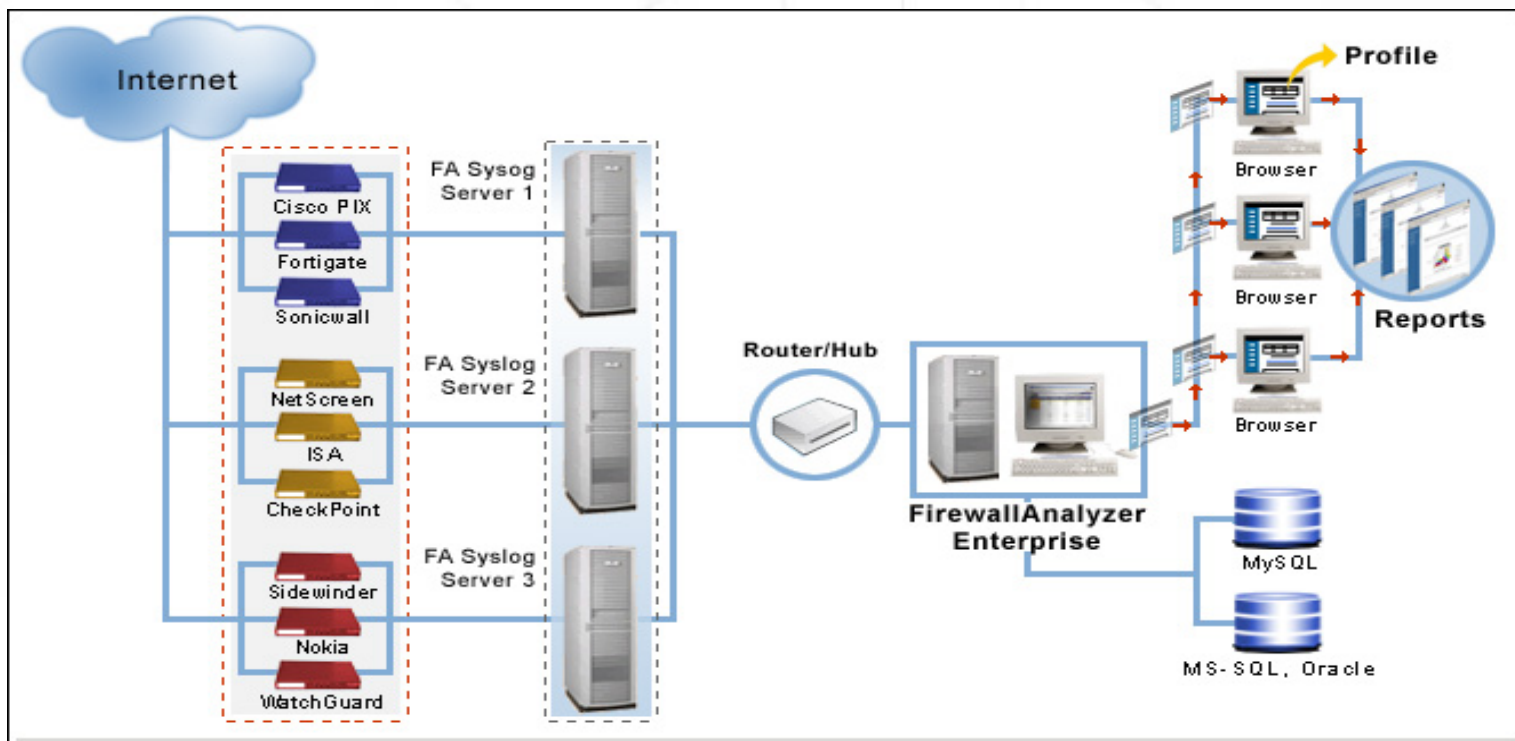
Cisco PIX with TrendMicro VirusWall AV server



Hour	Virus	Severity Level	# of Occurrences
11:00	W32.Bolgi.Worm	Warning	2
12:00	Backdoor.Tinydog	Warning	2
16:00	W32.Widare	Warning	9
	W32.Randex.AT	Notification	3

- What email aliases is the attacker using to send viruses?
- What are sources of viruses, file types, etc.
- Who is the rogue employee that is downloading large files? And what are they?
- What are frequent Virus destinations?
- What are protocol level virus activity details?

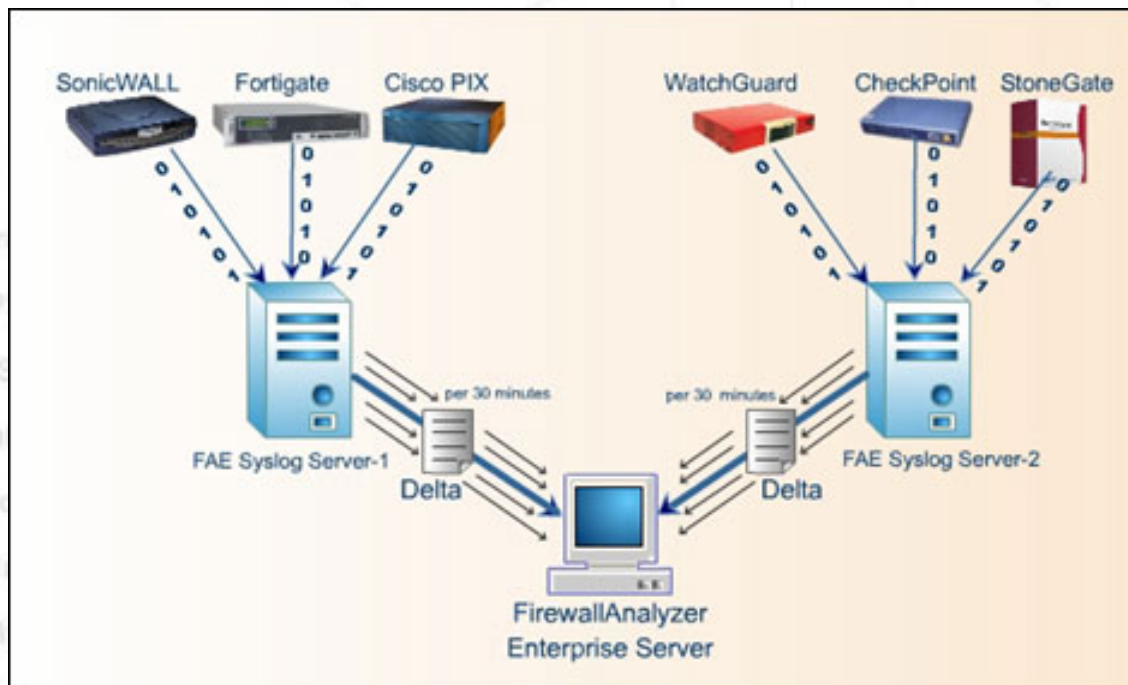
▶ FirewallAnalyzer



Robust, Distributed Data Collection – Built-in eIQ Syslog Data Collectors.

Flexible Data Storage & Reporting –built-in MySQL database. FScale Architecture results in significant disk space savings. Process once & reports any # of times.

▶ FWASyslog



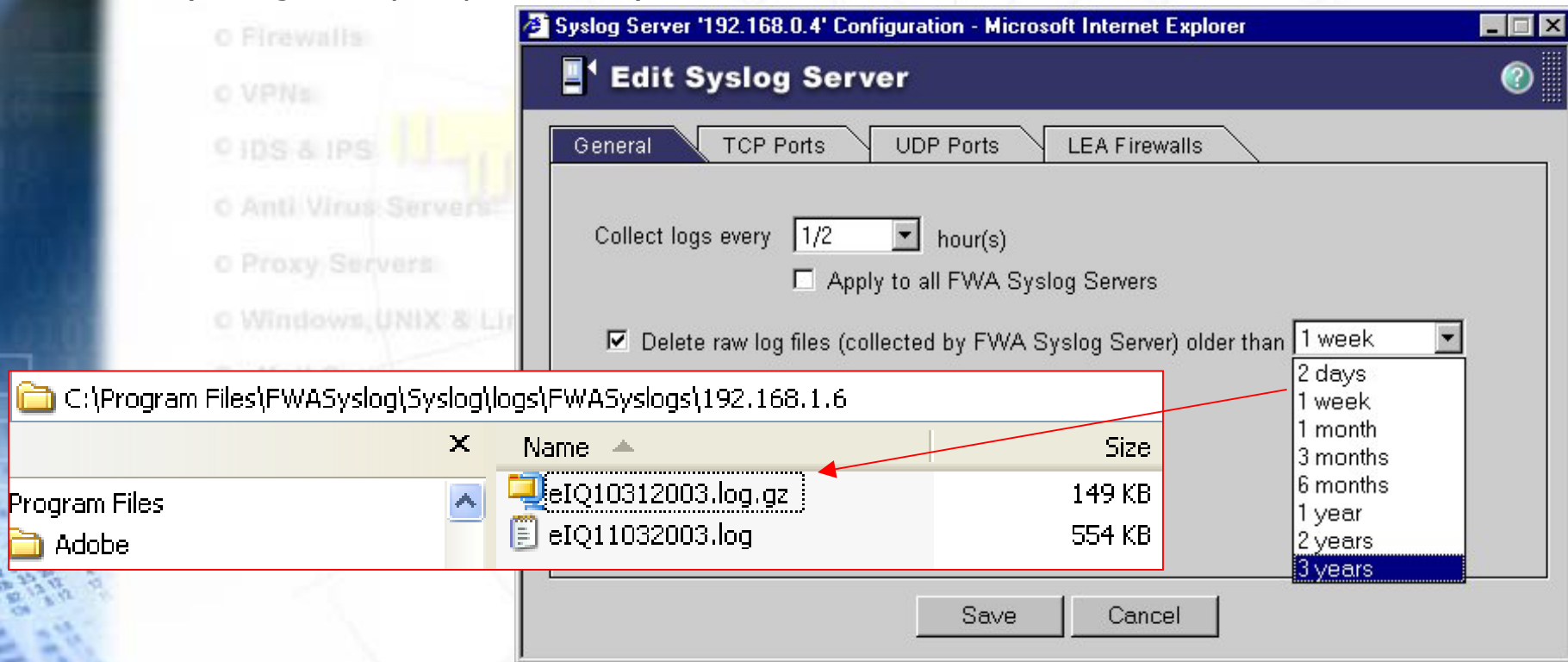
Native Syslog Data Collected – for archival and forensic purposes. (files are automatically compressed in .gz format, typically a 14:1 ratio)

Delta Files –written in eIQ’s OLF format. This is what the analysis engine processes in production mode. Delta files are rotated and sent for analysis every 30 minutes.

▶ Automated Data Mgmt

➤ User Configurable Log Management allows

- administrator to decide how long log data should be kept
- automated management based on corporate or industry standards (or regulatory requirements)



The screenshot displays the 'Edit Syslog Server' configuration window for 'Syslog Server '192.168.0.4''. The 'General' tab is active, showing the following settings:

- Collect logs every: 1/2 hour(s)
- Apply to all FWA Syslog Servers
- Delete raw log files (collected by FWA Syslog Server) older than: 1 week

A file explorer window is overlaid on the configuration window, showing the directory path: C:\Program Files\FWASyslog\Syslog\logs\FWASyslogs\192.168.1.6. The file explorer displays a table of files:

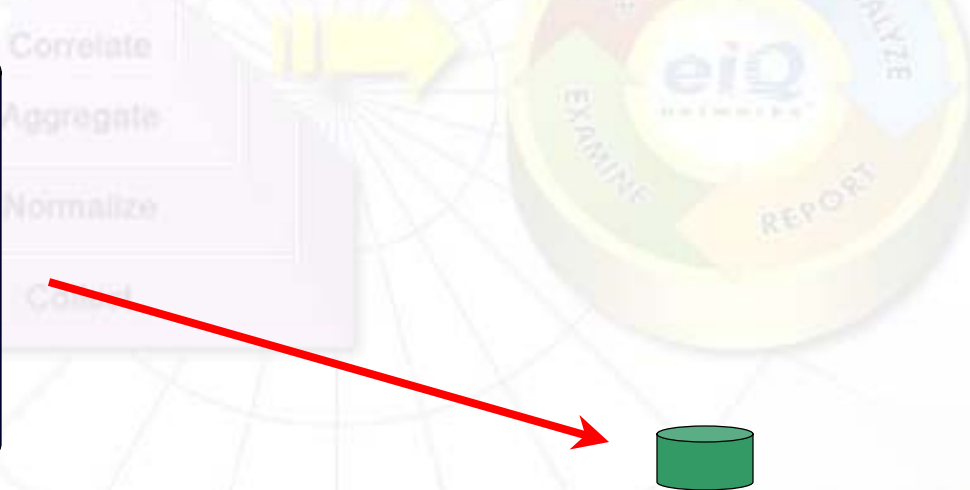
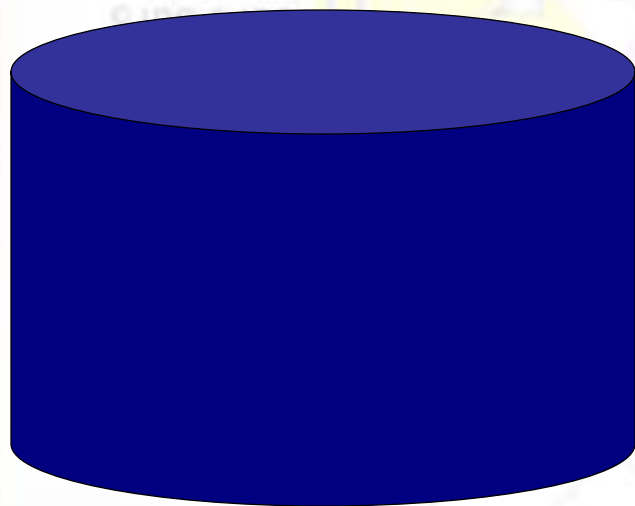
Name	Size
eIQ10312003.log.gz	149 KB
eIQ11032003.log	554 KB

A red arrow points from the '3 years' option in the dropdown menu to the file 'eIQ10312003.log.gz' in the file explorer.

▶ Data Mgmt Architecture

- **Fscale™ Results in enterprise-class processing speed**
 - Up to 40 GB/ day of Syslog data on a 2.4 GHz processor with 512MB of RAM
- **Dramatic Reduction in size of the database**
 - Small initial size (potentially 4GB of raw data to 4MB in database size on day 1)
 - Small incremental increase in DB (4GB of data on day 2 results in 5MB db)

Bottom Line: FScale is a highly scalable Architecture



Example: 4GB of syslog data was > 4Mb after processing!

▶ User Mgmt

➤ **FortiReporter provides authentication based on either**

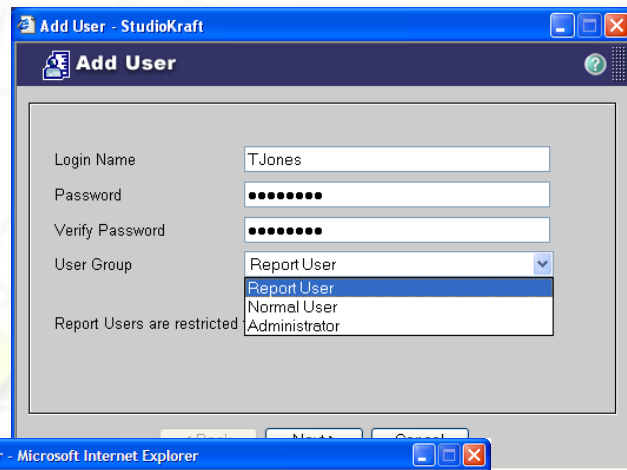
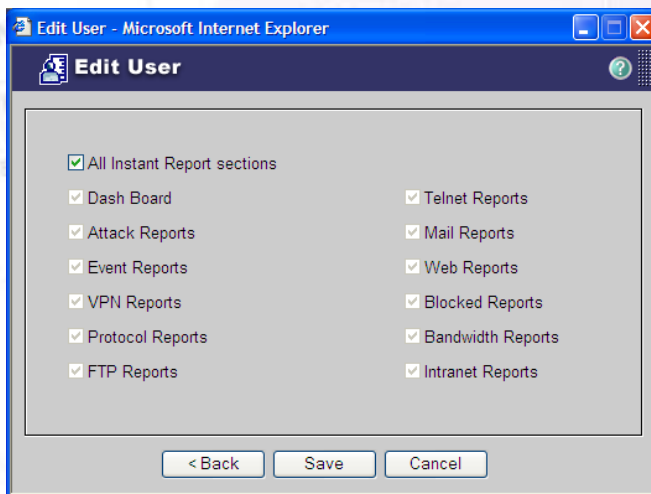
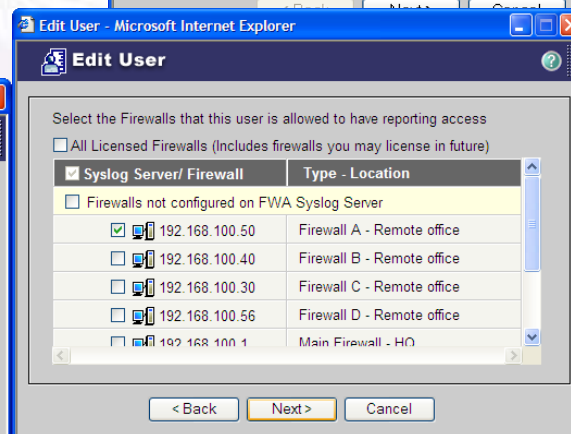
- Windows OS
- Native user rights management (recommended)

➤ **3 levels of report reader access are available**

- Administrator
- Normal user can create profile(s) and run report(s)
- Report user is restricted to viewing of instant reports only

➤ **Report access can be set on roles based granular level**

- per firewall
- per report section

Firewall	Type - Location
<input type="checkbox"/> All Licensed Firewalls (Includes firewalls you may license in future)	
<input checked="" type="checkbox"/> Syslog Server/ Firewall	
Firewalls not configured on FWA Syslog Server	
<input checked="" type="checkbox"/> 192.168.100.50	Firewall A - Remote office
<input type="checkbox"/> 192.168.100.40	Firewall B - Remote office
<input type="checkbox"/> 192.168.100.30	Firewall C - Remote office
<input type="checkbox"/> 192.168.100.56	Firewall D - Remote office
<input type="checkbox"/> 192.168.100.1	Main Firewall - HQ

Instant Reports

http://localhost:8216/cgi-bin/instantreportdefault.cgi -

FireWALL ANALYZER Enterprise

Instant Reports

Back | Refresh | Filters | Options | Print | Close

User: admin / Administrator
Permitted Firewalls: All

February 2004

S	M	T	W	T	F	S
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						

- ▶ Dashboards
- ↳ Executive
- ▶ Attacks
- ▶ Events
- ▶ VPN Usage
- ▶ Protocols
- ▶ FTP Usage
- ▶ Telnet Usage
- ▶ Mail Usage
- ▶ Web Usage
- ▶ Blocked Sites
- ▶ Bandwidth
- ▶ Intranet
- ▶ AntiVirus

General Summary	
Number Of Days Processed	20
Processed Date Range	12/04/2003 To 01/30/2004
Total Successful Requests	83112
Total Error Requests	15
Total Number of Events	96460
Average Events Per Day	4823
Total Number of Authenticated Visitors	28
Most Active Day	12/04/2003
Total Bytes Transferred	12.95 GB
Average Bytes Transferred Per Day	662.83 MB
Total Bytes Sent	1.88 GB
Average Bytes Sent Per Day	96.05 MB
Total Bytes Received	11.07 GB

Bandwidth Usage By Hour Of Day

Overall Events Triggered

Event Code

- 90166 - traffic
- 2677 - #Connection
- 1435 - #Web site hit
- 1159 - Broadcast packet dropped
- 306 - sql: MS-SQL Worm propagation attempt

Attacks By Hour Of Day

Report generation time: February 5, 2004 03:28:53 PM
Report generated by FirewallAnalyzer™ Enterprise. Copyright© 2001-2004 eIQnetworks™, Inc. All rights reserved.

▶ Drill-down reporting

http://localhost:8216/cgi-bin/instantreportdefault.cgi -

Instant Reports

Back | Refresh | Filters | Options | Print | Close

User: admin / Administrator
Permitted Firewalls: All

Attacks on Firewalls

Attacks on Firewalls provides information about the Top N sources of Attacks on each Firewall. Percentage columns represent the percentage of Events.

Filters Applied: None

Firewall	Attack Type	# of Attacks	% of Attacks
	sql: MS-SQL Worm propagation attempt	306	46.02
	TCP port scan , 133 > limit 128.	83	12.48
1 FGT1002803030595	icmp: Destination Unreachable (Commu		
	TCP port scan , 166 > limit 128.		
	dns: SPOOF query response with ttl: 1 r		
2 192.168.100.1	Land Attack Dropped		
	Forbidden E-mail attachment deleted		
	Illegal LAN address in use		
	Ping of death blocked		
	IP spoof detected		
3 192.168.100.56	Forbidden E-mail attachment deleted		
	Land Attack Dropped		
4 192.168.100.40	IP spoof detected		

This report presents you information on the firewalls attack

Report generation time: February 05, 2004 03:51:02 PM
Report generated by FirewallAnalyzer™ Enterprise

http://localhost:8216/cgi-bin/instantreportdefault.cgi -

Instant Reports

Back | Refresh | Filters | Options | Print | Close

User: admin / Administrator
Permitted Firewalls: All

Attacks on Firewalls

Attacks on Firewalls provides information about the Top N sources of Attacks on each Firewall. Percentage columns represent the percentage of Events.

Filters Applied: Firewall: FGT1002803030595
Attack Type: sql: MS-SQL Worm propagation attempt

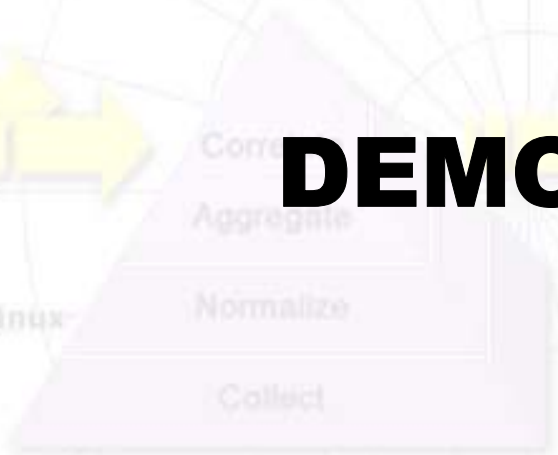
Firewall	Date	Attack Source	Attack Type	# of Attacks	% of Attacks
	12/06/2003	218.201.54.9	sql: MS-SQL Worm propagation attempt	4	
	12/08/2003	218.201.70.194	sql: MS-SQL Worm propagation attempt	4	
	12/09/2003	220.97.211.160	sql: MS-SQL Worm propagation attempt	4	
	12/04/2003	194.30.228.83	sql: MS-SQL Worm propagation attempt	3	
	12/05/2003	200.203.120.200	sql: MS-SQL Worm propagation attempt	3	
	12/06/2003	200.203.120.200	sql: MS-SQL Worm propagation attempt	3	
	12/07/2003	200.203.120.200	sql: MS-SQL Worm propagation attempt	3	
	12/04/2003	210.13.22.79	sql: MS-SQL Worm propagation attempt	3	
	12/04/2003	211.137.255.3	sql: MS-SQL Worm propagation attempt	3	
	12/07/2003	211.137.255.3	sql: MS-SQL Worm propagation attempt	3	

Report generation time: February 05, 2004 03:51:02 PM

Blue links indicate that more information is available. In this case, Attack Source and date.

▶ Instant Reports

- Firewalls
- VPNs
- IDS & IPS
- Anti Virus Servers
- Proxy Servers
- Windows, UNIX & Linux
- eMail Servers
- Web Servers



DEMO





FirewallAnalyzer - Features

Auto-discovery of Firewalls - FirewallAnalyzer automatically recognizes all configured firewalls.

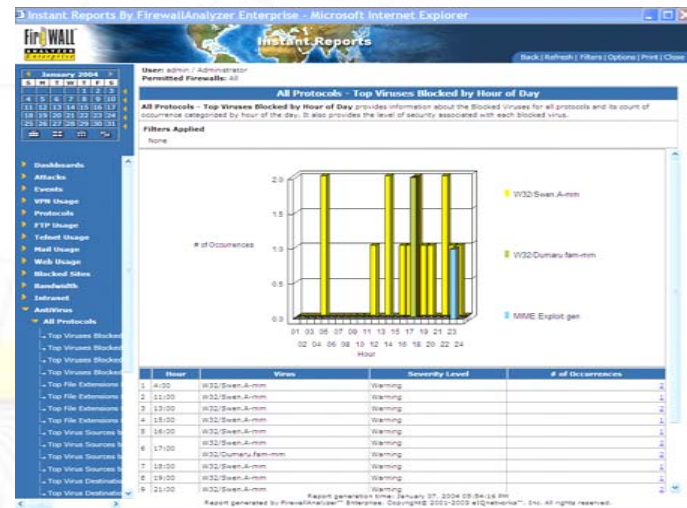
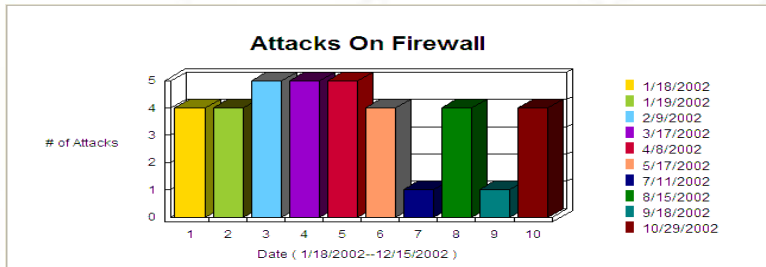
Intelligent Data Correlation - Combines and Correlates variety of data from heterogeneous firewalls & AVS.

Advanced Log Collection, Update and Management - Automatically recognizes & Collects log data; Saves significant disk space and network bandwidth.

Policy-Based Data Update - Allows for automatic transfer of delta log files and updates the data into a central repository.

Scalable and Comprehensive Data Management - FScale™ architecture allows efficient processing & storing of current and historical log data from 100s of firewalls.

Rules-Based Alerts - Send threshold based alerts.



Executive Dash Board - Provides summary of activity across firewalls, while giving the drill down option.

Role Based Access - Limits what each user can view based on their role and firewalls.

Managed Security Service Providers (MSSP) Support - offer value-added reporting service to using Reporting Portal, and allows each customer to view only their firewall data.



FirewallAnalyzer - Features

Automated Report Generation & Distribution

– generates over 400 reports with an easy mechanism to e-mail reports automatically to multiple recipients.

Multiple Report Formats – reports available in HTML, MS Word, MS Excel, Text and PDF



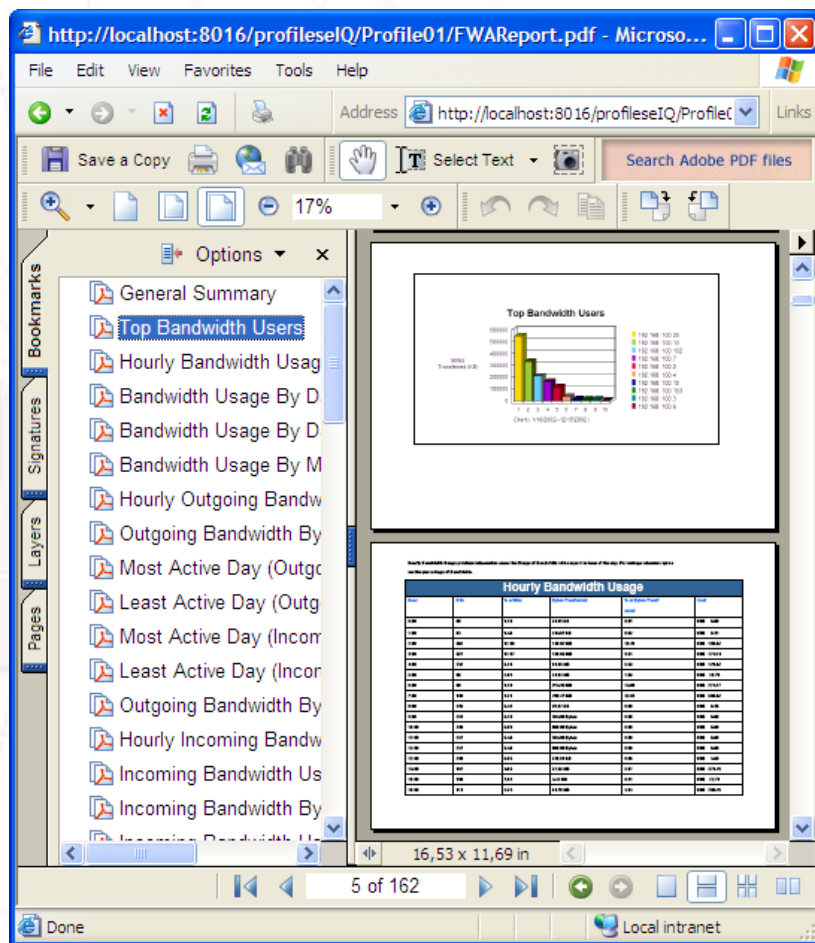
Automated Syslog Collection – from Firewall, AVS, ISA servers and VPN appliances.

Multiple Firewall Vendor Support – supports all leading firewalls appliances and servers

Instant Reports with Powerful Drill Down – generates reports in real time without having to wait for the processing of log files. Powerful drill down feature displays 2nd and 3rd level details with a single click.

Reduced Network Traffic – reduces network traffic between syslog server and FirewallAnalyzer by using delta log files in compressed format.

Archiving – save disk space by archiving processed log files.



▶ Pricing

FirewallAnalyzer

- \$795 per Device

- \$160 per year maintenance and support

○ Firewalls

○ VPNs

○ IDS & IPS

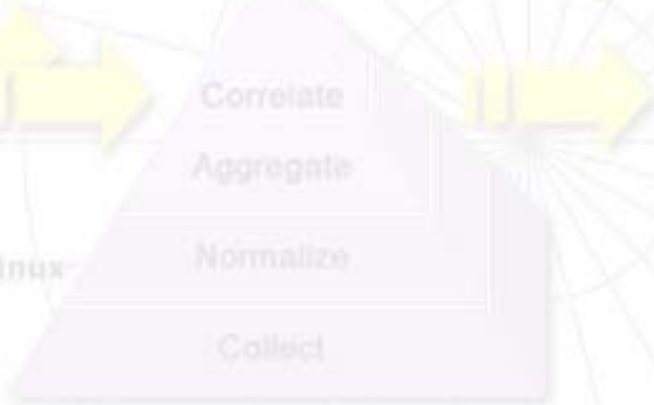
○ Anti Virus Servers

○ Proxy Servers

○ Windows, UNIX & Linux

○ eMail Servers

○ Web Servers



▶ Supported Devices

Support Firewalls / IDS / IPS/ Routers / Anti-Virus Servers/ Proxy / Web Security*

- ✓ Cisco PIX
- ✓ Cisco IOS Router Firewall
- ✓ Cisco VPN 3000 series
- ✓ Fortinet FortiGATE
- ✓ NetScreen
- ✓ Checkpoint
- ✓ NetContinuum
- ✓ Astaro
- ✓ BlueCoat
- ✓ Microsoft ISA
- ✓ Nokia appliances
- ✓ Sidewinder G2
- ✓ StoneGate

- ✓ SonicWALL
- ✓ Symantec Enterprise
- ✓ TopLayer
- ✓ WatchGuard Firebox
- ✓ Trend Micro InterScan
VirusWall
 - ✓ w/ NetScreen
 - ✓ w/Cisco PIX
 - ✓ w/CheckPoint
- ✓ McAfee VirusScan
 - ✓ w/SonicWALL
 - ✓ w/Cisco PIX
 - ✓ w/CheckPoint

▶ Configuring Devices

Cisco PIX is typically configured with the CLI. Issue the following commands:

- logging on
 - logging facility 20
 - logging trap informational
 - logging host interface_name FirewallAnalyzer_machine_IP
- Example: logging host inside 192.168.2.12



firewall_config
guide.pdf

- where interface_name is typically either "inside" or "outside" and
- where FirewallAnalyzer_machine_IP is the IP address of the FWA machine where the FWAsyslog server is enabled.

▶ Summary

FirewallAnalyzer Enterprise

- 21-day trial available from www.eiqnetworks.com

- Leader in Firewall and Perimeter Security reporting

- Enterprise-class solution, affordable pricing

Contact Info

Cameron Nelson cnelson@eiqnetworks.com (805) 687-6402