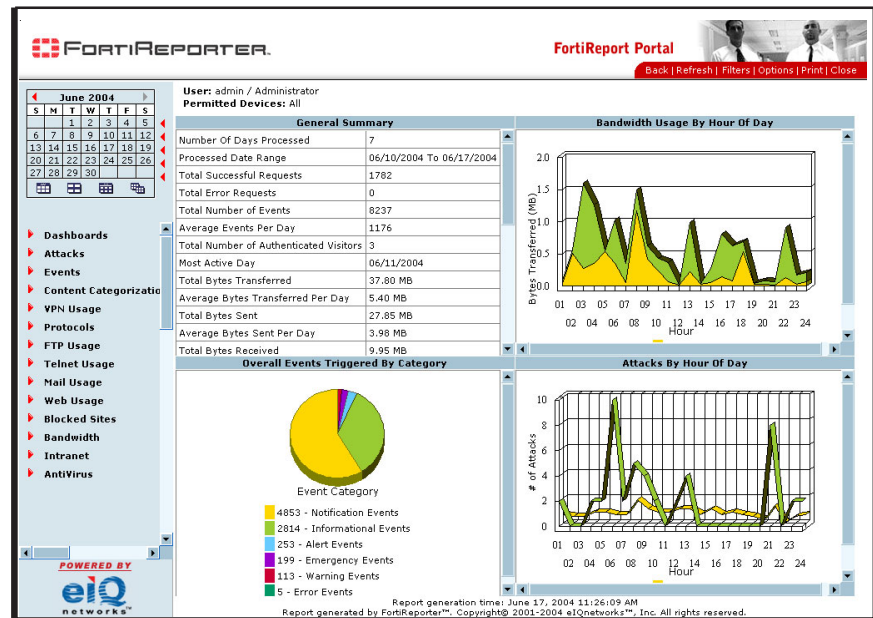


FORTIREPORTER™ SECURITY ANALYZER

Comprehensive Security Reporting and Analysis

FortiGate Antivirus Firewalls generate information on network activities through detailed syslog messages. In order to analyze and protect corporate networks, security managers/administrators and IT administrators need a comprehensive understanding of their Internet and network activities, such as network bandwidth usage, virus and intrusion attack activity, application/protocol usage as well as employee Internet use. To convert these cryptic syslog messages into meaningful information, typically requires administrators to use complex and expensive commercial analysis and reporting packages.

FortiReporter Security Analyzer is a cost-effective, browser-based, analysis, reporting and monitoring solution that generates easy-to-understand reports across all FortiGate platform functionalities and provides IT administrators, and security professionals insight into Internet, network usage and attack activities. FortiReporter Security Analyzer allows IT administrators to proactively secure their network before security threats arise, avoid network abuse, manage bandwidth requirements, monitor Web usage, and ensure appropriate employee usage of networks. FortiReporter Security Analyzer's hundreds of easily accessed reports cover the full range of network and security activity, including virus and worm activity, bandwidth usage, network attacks, Web usage, and protocol usage. FortiReporter easily installs on any system running Microsoft Windows NT, 2000, XP, or 2003.



Product Highlights

FortiReporter Security Analyzer helps:

- Analyze and understand virus and worm activity
- Understand security issues, hacker attacks and security breaches
- Identify attack type and source
- Analyze event severity and port of attack
- Understand protocol usage by user and department
- Analyze incoming and outgoing traffic/bandwidth patterns
- Identify inappropriate Internet usage by employees
- Understand bandwidth utilization by department, IP address and protocol
- Identify inappropriate Internet use from within your company
- Generate bandwidth cost allocation and utilization reports
- Find activity trends over time
- Monitor bandwidth utilization over time



System Requirements

Minimum Requirements

- Processor: Pentium III-1GHz
- Disk Space: 100MB
- RAM: 384MB
- Operating System: Windows NT/2000/XP/2003
- IIS, Netscape, or Apache

Recommended Requirements

- Processor: Pentium 4 - 2.4GHz
- Disk Space: 100MB
- RAM: 512MB
- Operating System: Windows 2000/XP/2003
- IIS
- Modern I/O
- SCSI or Fast ATA

FortiReporter Security Analyzer Report

Complete Report
Print

- Summary Details
 - General Summary
- Attacks
 - Hourly Attack Type and Att
 - Daily Attack Type and Att
 - Attacks By Hour Of Day
 - Attacks By Day
 - Attacks on Devices
 - Attacks By Category
 - Top Attackers By Attack T
 - Top Sources Of Attacks
 - Top Attacks
 - Top Destinations of Attack
 - Top Attacks by Protocol
 - Top Attacks by Destination
 - Top Destinations by Attac
 - Top Internal Attackers
 - Top Sources by Attack
 - Top Internal Attacks
 - Top External Attackers
 - Top External Attacks
 - External Attacks by Sourc
 - Internal Attacks by Sourc
 - Inbound IP Spoofing
 - Inbound IP Fragmentation
- Events

| Top Attacks | | | | | |
|-------------|-----------|-----------|-----------------------|---|--------------|
| | Date | Attack ID | Description | Attack Details | # of Attacks |
| 1 | 6/17/2004 | 287178790 | sql: slammer | http://www.fortinet.com/ids/id287178790 | 2 |
| | | 17956867 | icmp: ping.nmap | http://www.fortinet.com/ids/id17956867 | 2 |
| 2 | 6/16/2004 | 17956867 | icmp: ping.nmap | http://www.fortinet.com/ids/id17956867 | 30 |
| | | 287178790 | sql: slammer | http://www.fortinet.com/ids/id287178790 | 22 |
| | | 100663396 | top syn flood | http://www.fortinet.com/ids/id100663396 | 1 |
| 3 | 6/15/2004 | 287178790 | sql: slammer | http://www.fortinet.com/ids/id287178790 | 14 |
| | | 17956867 | icmp: ping.nmap | http://www.fortinet.com/ids/id17956867 | 14 |
| 4 | 6/13/2004 | 287178790 | sql: slammer | http://www.fortinet.com/ids/id287178790 | 22 |
| | | 17956867 | icmp: ping.nmap | http://www.fortinet.com/ids/id17956867 | 14 |
| | | 17432668 | backdoor: g_door.icmp | http://www.fortinet.com/ids/id17432668 | 12 |
| 5 | 6/12/2004 | 17432668 | backdoor: g_door.icmp | http://www.fortinet.com/ids/id17432668 | 18 |
| | | 287178790 | sql: slammer | http://www.fortinet.com/ids/id287178790 | 14 |
| 6 | 6/11/2004 | 17956867 | icmp: ping.nmap | http://www.fortinet.com/ids/id17956867 | 12 |
| | | 17432668 | backdoor: g_door.icmp | http://www.fortinet.com/ids/id17432668 | 22 |
| | | 17956867 | icmp: ping.nmap | http://www.fortinet.com/ids/id17956867 | 10 |
| 7 | 6/10/2004 | 287178790 | sql: slammer | http://www.fortinet.com/ids/id287178790 | 8 |
| | | 17432668 | backdoor: g_door | http://www.fortinet.com/ids/id17432668 | 3 |
| | | 17956867 | icmp: ping.nmap | http://www.fortinet.com/ids/id17956867 | 14 |
| | | 17432668 | backdoor: g_door | http://www.fortinet.com/ids/id17432668 | 12 |
| | | 287178790 | sql: slammer | http://www.fortinet.com/ids/id287178790 | 6 |
| | | 100663396 | top syn flood | http://www.fortinet.com/ids/id100663396 | 1 |

FortiReporter Security Analyzer provides:

- Comprehensive and easy to read and understand reports
- Powerful drill down links show more information, in this case, a link to FortiProtect Center's Attack Encyclopedia for more details on detected attacks



Features and Benefits

| Feature | Benefit |
|---|--|
| Comprehensive reports - 400 reports covering security events, Web filtering, bandwidth utilization, and protocol usage | Provides a view of network and security activity with a single reporting and analysis tool |
| Scalability - Allows users to combine data and report on multiple geographically distributed security devices | Provides a reporting solution to meet the needs of small businesses and scale to meet the needs of large multinational organizations |
| Performance - Generates instant reports in real-time without having to wait for the log file processing to complete | Report users can view the latest data in real-time, instead of waiting hours for report processing |
| Correlation - Provides critical correlation analysis information on virus/worm outbreaks and network attacks | Minimize incident response time and maximize the ability to take a proactive and preventative action to improve security information management and reduce network vulnerabilities |
| Multi-vendor support - supports over 30 different firewall appliances and servers | Allows organizations with multiple vendor security environments to consolidate network and security activity events on a single report |
| Remote access - Browser-based access lets you generate reports from any computer on the local network or remotely via secure Internet connection | Anytime, anywhere access and management |
| Enterprise/MSSP Portal - Provides a portal for on-demand reporting service to managed services customers | Limits report users to view information pertaining to their security devices only |
| Efficient data collection and storage - Collect up to 40GB of syslog data a day from hundreds of security devices at user defined intervals | Decreases report generation processing time to provide instant reports |
| Comprehensive virus, worm, and attack analysis - Identifies and provides details on virus/worm activity including virus type, protocol, source, destination, frequency, and file extension by hour, day, or month. | Helps organizations understand virus and worm activity in their networks |
| Automated report generation - Automatically generates over 400 pre-defined reports with tables and graphs in different languages | Reduces management costs through automatic report generation |
| Multiple reporting format and distribution - Generate and view reports in HTML, MS Word, MS Excel, plain text, and PDF formats with options to email reports to multiple recipients | An easy mechanism to email reports automatically to multiple recipients in various formats |
| Multiple language support - Furnishes reports in English, French, Spanish, German, Italian, Swedish, Korean, Portuguese, Mandarin Chinese, and Japanese. | Seamless integration for multinational organizations that require multiple language support |

**Australia**

Level 17, 201 Miller Street
North Sydney 2060
Australia

Tel: +61-2-8923-2555

Fax: +61-2-8923-2525

China

Suite B-903
Zhongdian Information Building
2 Zhongguancun Nan Ave.
Beijing 100086, China

Tel: +8610-8251-2622

Fax: +8610-8251-2630

France

69 rue d'Aguesseau
92100 Boulogne Billancourt
France

Tel: +33-1-4610-5000

Tech Support: +33-4-9300-8810

Fax: +33-1-4610-5025

Germany

Feringapark
Feringastrasse 6
85774 München-Unterföhring
Germany

Tel: +49-(0)-89-99216-300

Fax: +49-(0)-89-99216-200

Hong Kong

Room 3206, 32/F
Convention Plaza - Office Tower
1 Harbour Road, WanChai
Hong Kong

Tel: +852-3171-3000

Fax: +852-3171-3008

Japan

32nd floor
Shinjuku-Nomura Building
1-26-2 Nishi-Shinjuku
Shinjuku-Ku
Tokyo, Japan 163-0532
Japan

Tel: +81-3-5322-2813

Fax: +81-3-5322-2929

Korea

27th Floor
Korea World Trade Center
159 Samsung-Dong
Kangnam-Ku
Seoul 135-729
Korea

Tel: +82-2-6007-2007

Fax: +82-2-6007-2703

Taiwan

18F-1, 460 SEC.4
Xin-Yi Road
Taipei, Taiwan, R.O.C.

Tel: +886-2-8786-0966

Fax: +886-2-8786-0968

United Kingdom

1 Farnham Road
Guildford, Surrey GU2 4RG
United Kingdom

Tel: +44-(0)-1483-549061

Fax: +44-(0)-1483-549165

United States

920 Stewart Drive
Sunnyvale, CA 94085
USA

Tel: +1-408-235-7700

Fax: +1-408-235-7737

Email: sales@fortinet.com