

The 10 Reports...

➤ Every Firewall/Security Administrator Lives For

A Free Guide to Protecting Your Network and Internet Resources

01 02 03 04 05

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR

Protecting Your Network

Your firewall is installed and configured, your security policy is in place, and your employees have agreed to the organization's Internet usage policy—using the Internet for work-related purposes only. Are you absolutely certain that your network, web site and other Internet-connected devices are secure? Can you be sure your employees are in compliance with policy?

Quite often, IT managers and security professionals like you believe they've done enough to protect the network and Internet resources but discover too late that a critical piece of managing these resources had been overlooked. Ensure the security of your network with NetIQ's Firewall Reporting products.

NetIQ's Firewall Reporting products can spare you from the stress involved with recovering from a security breach or improper usage—and prevent potentially devastating losses, including pirated intellectual property. Mining the data recorded in firewall log files, our firewall products generate more than 200 activity reports, providing summary-level and comprehensive reports to present a clear picture of network security; employee e-mail and Internet habits; bandwidth usage; and network device health. Security compromises, attempted intrusions and improper employee activity are all detailed and brought to your attention before they cause problems.



Using NetIQ's Firewall Reporting Products

(Formerly **WEBTRENDS** Firewall Reporting Solutions)

NetIQ's Firewall Reporting products supply essential firewall traffic reports, identifying suspicious incoming or outgoing activity. Using the easy-to-interpret reports, you can monitor network security, track bandwidth usage, identify inappropriate e-mail and web surfing and ensure networked resource availability.

- **Monitor Network Security**

Identify critical events and generate alerts to address vulnerabilities before hackers or other malicious individuals exploit weaknesses in your network or firewall. Rather than reacting to compromised security, hack attempts or breaches after they occur, be proactive and prevent security problems before they impact your network with NetIQ's Firewall Reporting products.

- **Track Bandwidth Usage**

Forecast effectively and respond to belt-tightening measures and the ever-present need for increasing efficiency. Reports revealing your organization's bandwidth usage trends can help you set realistic budgets based on historical data. You may uncover that your enterprise goals can be achieved with significantly decreased bandwidth or that your current bandwidth isn't sufficient. Our bandwidth usage reports help you determine if available bandwidth levels are adequate for your organization's needs. By providing reports describing bandwidth usage trends by hour, day or week, the reports let you schedule maintenance, repairs and tasks that aren't time-critical.

- **Identify Inappropriate E-mail and Web Surfing**

Are employees using company e-mail and Internet resources inappropriately? Your organization is legally responsible for e-mail sent from your networks and any material found on your servers. Even material downloaded by an employee in clear violation of company policy could expose you to expensive, time-consuming legal issues.

E-mail and Internet usage policies were created to ensure that employees use company resources for business-purposes only and to prevent employees from e-mailing or downloading questionable or offensive content. NetIQ's Firewall Reporting products track and report on e-mail trends and Internet usage, identifying frivolous or improper surfing so you can prevent abuse.

- **Ensure Networked Resource Availability**

Make sure that networked resources such as servers, web sites, and other devices and objects are always up and available. NetIQ's Firewall Reporting products monitor the state of networked resources and send alerts when they experience problems. Alerting and monitoring reports track how often networked devices fail or go down, how long they remain offline, and the events that lead to failure. IT managers can then use this knowledge to perform timely maintenance and upgrades and to minimize device downtime.

01. What is the overall activity around my firewall?



One of your primary responsibilities is to understand what's happening at your firewall.

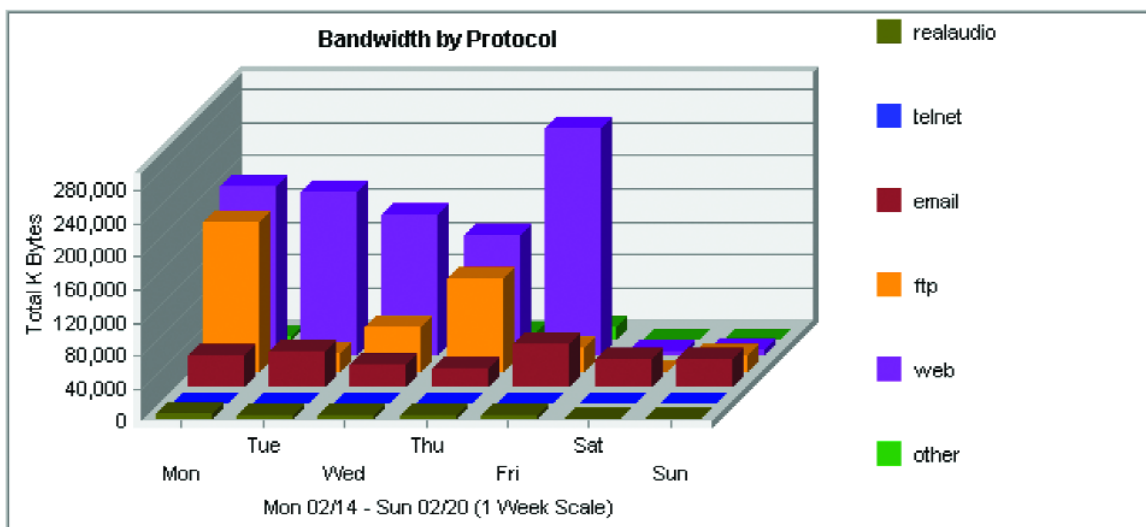
The General Statistics report provides high-level information you need to monitor activity and determine whether there are issues requiring further investigation. It includes the number of events that occurred during a specific time period and specifies which of those events may pose security threats. The report also shows how much bandwidth your organization uses, and how it's used—sending e-mail, surfing the Internet and sending files using file transfer protocol (FTP) or other purposes. In essence, this report is the first step in assessing the state of your organization's security, bandwidth usage and employee Internet usage habits.

The General Firewall Statistics report:

- Establishes a baseline level of activity for your network and shows when aberrations warrant deeper inspection.
- Discovers if your network is experiencing an unusual number of security threats, indicating the need to double-check and shore up your firewall's protective measures or your organization's security policy.
- Determines if bandwidth usage levels suggest that employees may be taking advantage of e-mail and Internet resources for personal use.

General Firewall Statistics

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



General Firewall Statistics	
Date & Time This Report was Generated	Thursday February 28, 2002 - 13:39:22
Timeframe	02/14/2000 00:00:01 - 02/20/2000 23:59:23
Total # of events	120289
Total # of critical events for log file	361
Total # of errors and warnings	9792
Total # of VPN events for log file	433
Total # of bytes for outgoing connections	1,145,544K
Total # of bytes for incoming connections	626,717K
Average # of events per day	17184
Average # of bytes per day, outgoing connections	163,648K
Average # of bytes per day, incoming connections	89,531K
% of bandwidth devoted to web activity	57.02%
% of bandwidth devoted to email activity	14.66%
% of bandwidth devoted to FTP activity	24.22%
% of bandwidth devoted to Telnet activity	0.21%
% of bandwidth devoted to other activity	3.87%
Number of addresses behind firewall	542

02. Am I wasting money on Internet access?



The Outgoing Protocol Usage report measures bandwidth usage coming into your network, specifying what percentage of bandwidth is used by various protocols.

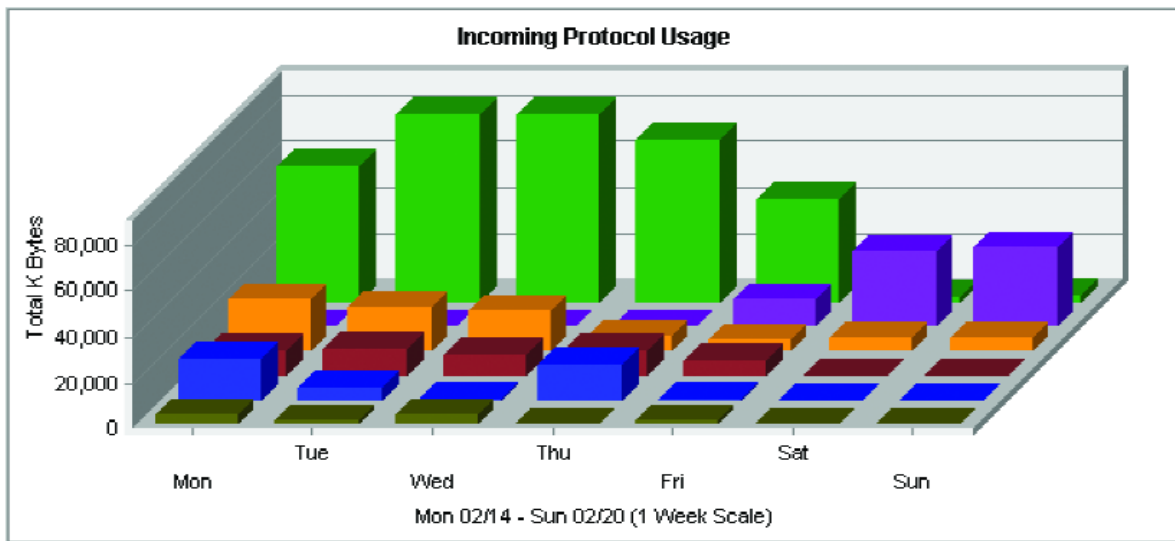
Similarly, the Incoming Protocol Usage report measures bandwidth used outside your organization, catalogued by protocol. Because you incur bandwidth expenses, protocol usage reports help you spend wisely. If reports indicate that your bandwidth needs are low, you can safely cut back. Or, you can find out if it's not cost-effective to struggle with inadequate bandwidth, which can lead to employee frustration or even worse, impaired web site performance. Deterioration in your web site performance can result in negative site experiences for your visitors and/or delayed or aborted Web and e-mail interactions. The Incoming and Outgoing Protocol Usage reports enable you to understand and efficiently manage your organization's bandwidth requirements.

Incoming/Outgoing Protocol Usage reports:

- Provide detailed bandwidth measurements so you can create a bandwidth budget tailored to your organization's needs.
- Reveal how much bandwidth employees in your organization are using and track improper and non-business usage.
- Help you determine bandwidth so you can allocate adequate bandwidth usage for Web initiatives to ensure a positive user experience.

Incoming/Outgoing Protocol Usage

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



Incoming Protocol Usage						
	Protocol	# of Events	% of Total Events	Kbytes	Cost	
1	http	42856	70.96%	347,224	\$6,844.48	
2	110/tcp	3184	5.23%	79,825	\$1,596.50	
3	smtp	1353	2.24%	73,056	\$1,461.12	
4	ftp	321	0.53%	51,405	\$1,028.11	
5	ftp-data	193	0.31%	44,164	\$883.28	
6	80/tcp	2808	4.64%	13,510	\$270.20	
7	http-ftp	15	0.02%	10,942	\$218.84	
8	443/tcp	224	0.37%	2,875	\$57.50	
9	3765/tcp	294	0.48%	2,223	\$44.46	
10	telnet	66	0.1%	954	\$19.08	
	Total	51294	100%	626,717	\$12,534.34	

03. Do I have sufficient network and Internet capacity?



When your network is flooded with activity, employee work pace slows down.

And if your server is busy, customers can't access your web site. Monitoring bandwidth usage to assess your organization's current requirements and plan for its future needs is another area that falls under your responsibility. To properly and accurately monitor bandwidth usage, you need to fine-tune your bandwidth budget by mapping bandwidth allocations to usage trends.

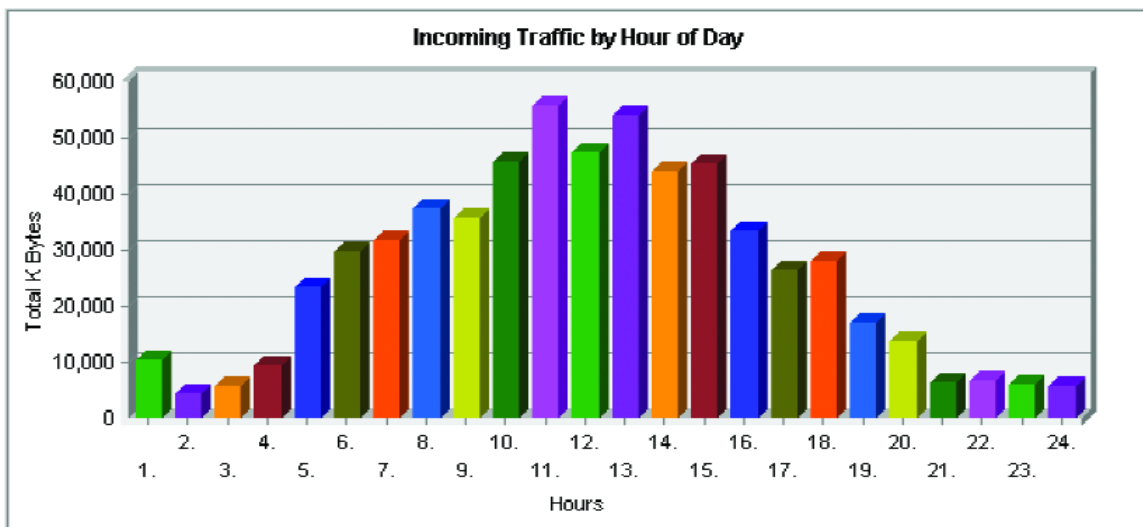
The Incoming Traffic by Hour of Day report reveals which hours of the day handle the most and fewest incoming events. In addition, this report presents the number of incoming events that occur and the amount of incoming data received each hour. Similarly, the Outgoing Traffic by Hour of Day report explains how employees inside the firewall use bandwidth to send data outside. Both reports can be configured to break down bandwidth usage information during working and non-working hours, which are defined by your configuration settings.

Incoming/Outgoing Traffic by Hour of Day reports:

- Identify periods of reduced activity so you can schedule server and web site maintenance that won't interfere with Web visitors' experience and employee productivity.
- Display peak bandwidth usage during high-traffic periods so you can determine if you're too close to the limits of your capacity.
- Reveal hour by hour when your web site traffic peaks and dips, enabling you to plan major mailings or large data transfers during traffic lulls.

Incoming/Outgoing Traffic by Hour of Day

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



Incoming Traffic by Hour of the Day

Most Active Incoming Hour of the day	11:00-11:59
Least Active Incoming Hour of the day	20:00-20:59

Incoming Traffic by Hours Details

Hour	# of Events	% of Total Events	Kbytes
00:00-00:59	1536	2.54%	10,636
01:00-01:59	1098	1.81%	4,577
02:00-02:59	836	1.38%	5,983
03:00-03:59	2392	3.96%	9,433
04:00-04:59	3893	6.44%	23,508
05:00-05:59	1054	1.74%	28,990
06:00-06:59	3541	5.86%	31,893
07:00-07:59	3469	5.74%	37,480
08:00-08:59	3075	5.09%	35,983
09:00-09:59	3688	6.1%	46,677
10:00-10:59	3805	6.3%	55,765
11:00-11:59	4884	8.25%	47,691
12:00-12:59	3307	5.47%	54,222
13:00-13:59	3329	5.51%	44,257
14:00-14:59	3196	5.29%	46,536
15:00-15:59	2238	3.7%	33,461
16:00-16:59	2649	4.38%	26,582
17:00-17:59	3004	4.97%	28,261

04. Are hackers attacking my organization's network or web site?



Firewalls are a vital part of every security perimeter, but without the right analysis and reporting tools, it's impossible to accurately track security events at the perimeter of your network.

Even with a firewall protecting your network and web site, a hacker or malicious individual can still infiltrate and wreak havoc. Additionally, employees within the organization pose as great a threat to security as external hackers do. Remember, individuals intent on doing harm are always looking for ways to exploit vulnerabilities in your organization's security.

The Summary of Critical Events report monitors events that your firewall deems as critical to security—such as unauthorized remote connections or access attempts from a computer whose return IP address doesn't sync up with the IP address of the original request. This report alerts you to events to examine more closely and helps you take preventative security measures, such as setting up firewall rules that deny access when IP addresses are from suspicious sources.

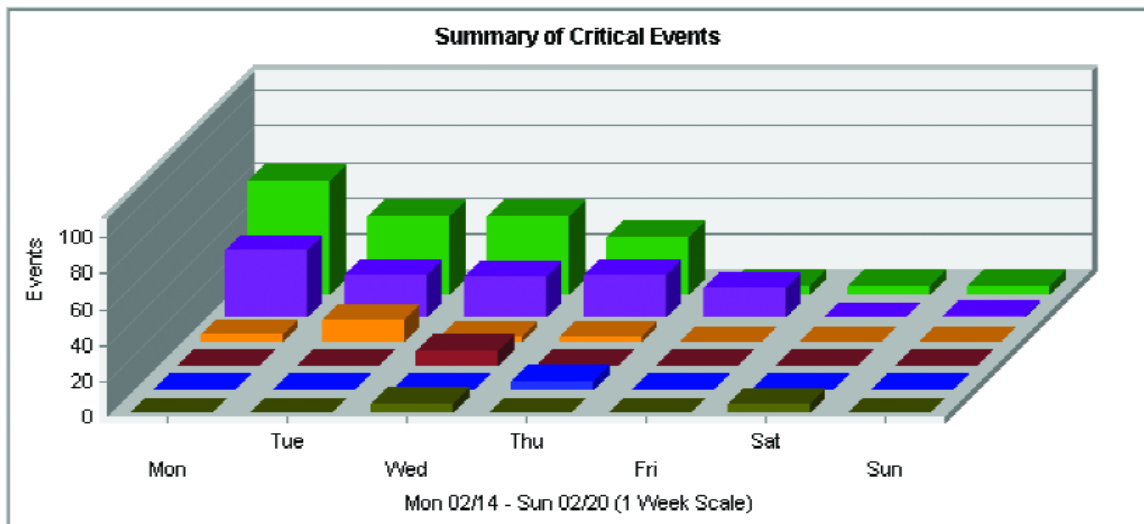
The Summary of Critical Events report:

- Reveals if your network or web site is experiencing a significant number of critical events that may identify a hacker or internal user trying to breach security.
- Can be configured to enhance protection against specific critical events you've catalogued.
- Provides detailed information about suspicious activities, allowing you to make more informed decisions about setting firewall rules.

04

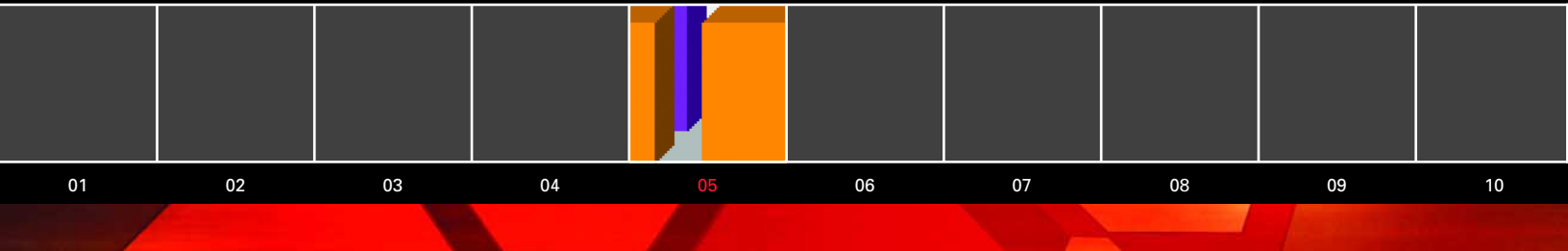
Summary of Critical Events

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



Summary of Critical Events			
	Description	# of Events	% of Total
1	512: Unauthorized remote connect attempt.	190	52.63%
2	508: Reverse address doesn't match.	128	35.46%
3	Firewall Log Message Code: 516	13	3.6%
4	611: User count limit reached.	9	2.49%
5	515: Attempt to use firewall proxies to connect to Eagle control ports.	6	1.66%
6	505: Unauthorized process killed.	6	1.66%
7	606: Failed to notify.	4	1.1%
8	501: Access from incoming to outgoing.	2	0.55%
9	514: Protocol violation.	2	0.55%
10	Firewall Log Message Code: 508	1	0.27%
Total number of critical events for logfile		361	100%

05. Should I monitor non-critical security events?



While your firewall may not define some activities as critical, events such as denied access attempts, possible port scans or invalid passwords can indicate attempts to compromise your security.

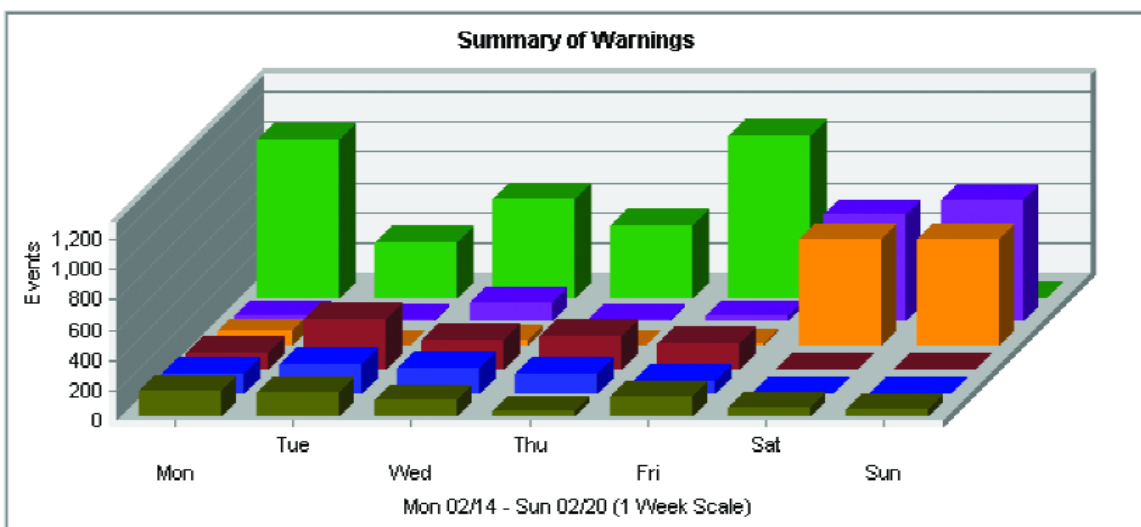
The Summary of Warnings report lists events that might expose a security threat and measures how often they occur. Typically, the events are benign; for example, an unrecognized password is likely an innocent typo. However, you can investigate the activity associated with warnings after discovering an increase in the incident rates of any specific warning.

The Summary of Warnings report:

- Uncovers potential network/Internet security threats so you can investigate and take any needed action.
- Determines when someone inside or outside the organization may be performing port scans or other malicious behavior to gain unauthorized access.
- Identifies repeated failed efforts to gain access so you can take steps to stop the problem, either by locking an individual out or, more likely, by simply reacquainting a known user with log-in procedures.

Summary of Warnings

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



Summary of Warnings			
	Return Value	# of Events	% of Total
1	344: Non-transparent call.	3736	38.15%
2	201: Access denied.	1689	17.24%
3	226: IP packet dropped.	1518	15.5%
4	310: Can't verify reverse address.	1053	10.75%
5	228: Can't connect to port.	775	7.91%
6	347: Possible port scan.	758	7.74%
7	301: Internal warning.	85	0.88%
8	457: System timezone, time, or date is not correctly set.	55	0.56%
9	218: Invalid protocol.	36	0.36%
10	308: Can't lookup host name.	26	0.26%
Total for the Warnings Above		9711	99.17%
Total number of Warnings for logfile		9792	100%

06. Which firewall rules are most commonly triggered from the Internet?

					# of Events				
01	02	03	04	05	4518	07	08	09	10
					3164				
					1920				
					1420				

Firewall rules specify who may or may not enter the network.

There are two approaches to setting up these rules, and of these, the most secure method is to only allow in those who meet the specifications of a firewall rule. For example, a rule may only allow network or web site access to specific IP addresses. If an attempt is made by an IP address not on the list, they are denied. A less secure approach is to deny access to those who break a firewall rule. An example of this is when a rule blocks a specific IP address from gaining access.

In firewall management, you can determine if your network is under attack from external sources by identifying deviations from baseline levels of firewall activity—in particular, when an individual firewall rule is triggered an abnormally high number of times.

Consider the first example, in which only IP addresses on a list are given network or web site access. If the rule is triggered more often for a given period than is normal, it's likely that someone is attempting to gain entry into an area of the network or web site they do not have permission to access.

The External Addresses Triggering Firewall Rules report tracks the rules triggered the most by external computers and tells you how frequently they were triggered for a given time period. This information lets you identify potential issues and handle them before they turn into devastating problems.

Use the External Addresses Triggering Firewall Rules report to:

- Identify behavior that indicates a potential attempt to break into the network.
- Re-examine firewall rules that are being triggered the most frequently to ensure they don't leave any holes in network security.

06

External Addresses Triggering Firewall Rules

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR

External Addresses Triggering Firewall Rules		
Rule	Address	# of Events
4	www.aol.com	4518
	206.58.83.196	3164
	FPENDELTON	1920
	209.180.166.12	1420
	199.97.97.162	793
8	hd38-112.hil.compuserve.com	1266
	168.126.98.32	1113
	ppp43.pressroom.com	1095
	pm2p20.iohk.com	840
	DUI35.N196.ResNet.QueensU.CA	831
2	www.alphasoftware.com	1065
	www.suck.com	223
	204.164.100.21	180
	web.zdnet.com	165
	www1.telepart.com	112
46	172.31.0.10	1631
	172.31.0.8	1437
	172.31.0.3	329
	172.31.0.9	93
	204.91.242.80	48
7	143.155.103.254	156
	189.239.46.55	102
	194.243.67.5	94
	130.225.25.218	86
	182.9.51.3	66
8	Sales@webtrends.com	124
	owner-ntsecurity@ss.net	30
	206.58.83.191	28
	davep@webtrends.com	26
	nobody	22
11	atbeach.com	25
	195.46.160.108	20
	ns1.albatros.dk	19
	ns.technojunkie.com	17
	espresso.mwi.com	15
5	202.98.163.28	122
	sf-pm10-27-251.dialup.slip.net	97

07. How can I be alerted to suspicious behavior?



If you wait until after security has been breached, you may have to deal with the costly consequences—files lost or corrupted, computers and servers infected with viruses, customer complaints and, perhaps most damaging of all, losing your credibility with customers and partners.

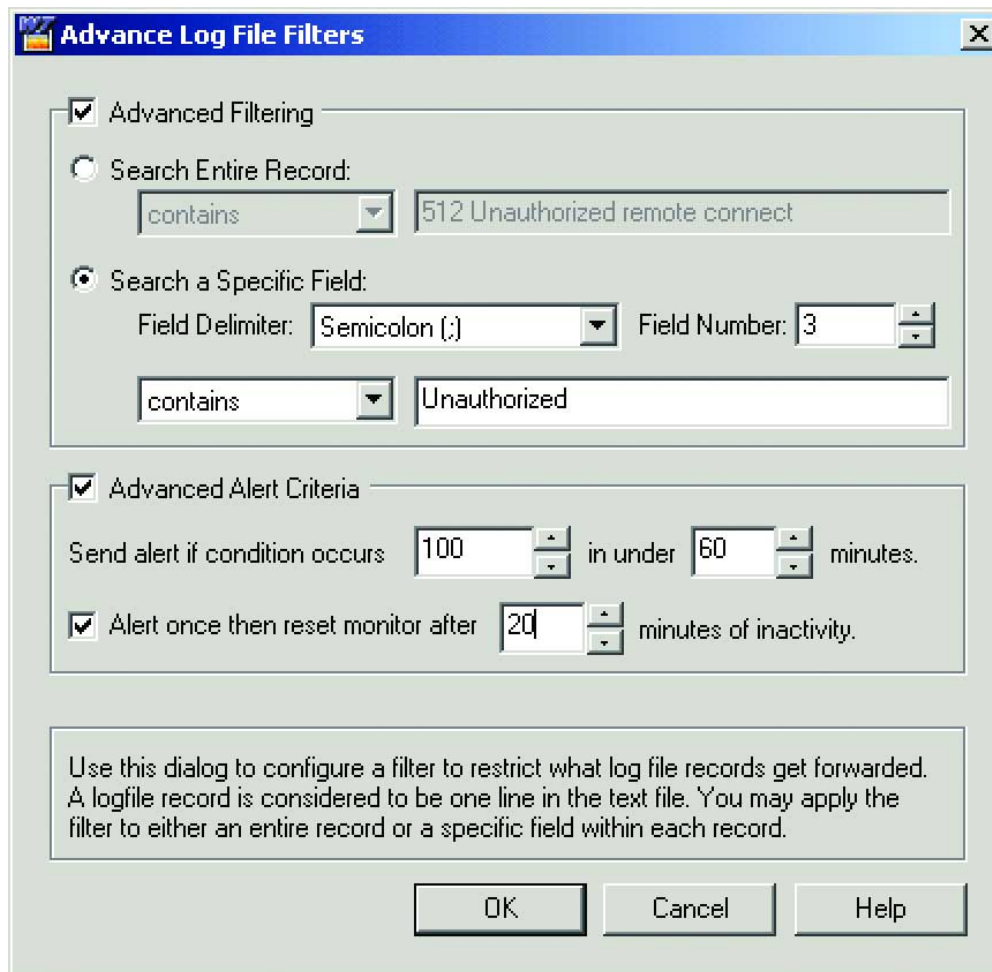
The Alert on N Events over Time from the Alerting and Monitoring module of NetIQ's Firewall Reporting products can be configured to monitor the frequency of certain activities and alert you the instant something suspicious happens. A small number of non-critical events in a day are meaningless, but a sudden steady barrage of a typically innocent activity can indicate trouble. You can configure Alert on N Events over Time for an event, such as indexing scans, and define the tolerable frequency, letting you ignore the "noise" of every-day non-critical events and still be confident that reporting alerts will tip you off if there's a security threat.

The Alert on N Events over Time report:

- Monitors trends in non-critical events.
- Monitors the frequency of specified events according to rules you set, sending an alert before a full-blown security breach occurs.
- Prevents problems so you don't have to suffer the consequences afterwards.

Alert on N Events over Time

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



08. Are employees using e-mail for business purposes?

01

02

03

04

05

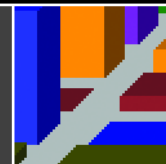
06

07

08

09

10



Measuring e-mail trends helps your organization optimize traffic flow and enforce policies.

A carefully drafted e-mail and Internet usage policy is worthless if you can't prove employees are abusing network resources.

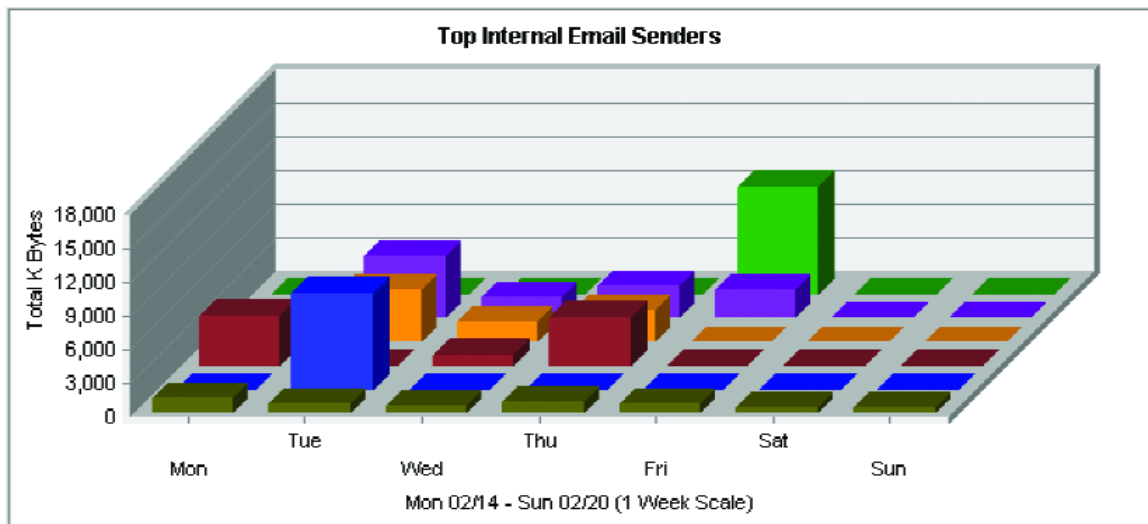
The Top Internal E-mail Senders report shows who is sending the most e-mail. Typically, you'll see that accounts dedicated to communication with customers, suppliers and partners are the top e-mail senders, and heavy mail traffic for any individual may justify closer inspection. If you determine that someone is violating e-mail usage agreements, you have the evidence you need.

The Top Internal E-mail Senders report:

- Shows which employees are sending the most e-mail and helps you determine if traffic levels warrant an investigation.
- Provides e-mail traffic data to support any action taken against an employee violating e-mail and Internet usage policies.
- Helps you stagger mass mailings—such as sales and support newsletters—to prevent e-mail traffic jams.

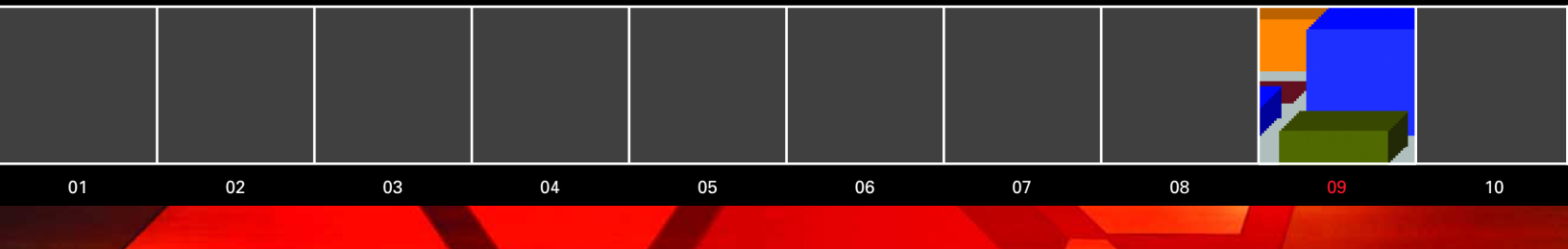
Top Internal E-mail Senders

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



Top Internal Email Senders				
	Internal Email Sender	# of Emails	% of Total Emails	Kbytes
1	jimh@webtrends.com	4	0.08%	17,433
2	joe@test.domain.com	47	1.03%	13,101
3	webmaster@test.domain.com	110	2.41%	10,538
4	Frank@webtrends.com	20	0.43%	10,145
5	jelicott@webtrends.com	18	0.39%	8,819
6	WebtAnnounce@webtrends.com	819	17.96%	6,381
7	JBahr@webtrends.com	4	0.08%	5,556
8	webmaster@webtrends.com	18	0.39%	4,801
9	host@test.domain.com	53	1.16%	4,558
10	kerr@test.domain.com	132	2.89%	4,546
	Subtotal for Users Above	1225	26.86%	85,881
	Total for the Log File	4539	100%	106,942

09. Who are the top Web surfers in the organization?



High-speed Internet connections in the workplace can be a useful business tool, but all IT professionals recognize the potential for abuse.

While e-mail and Internet usage policies are designed to limit recreational Web surfing, some users may overstep or even ignore your well-defined agreements and guidelines.

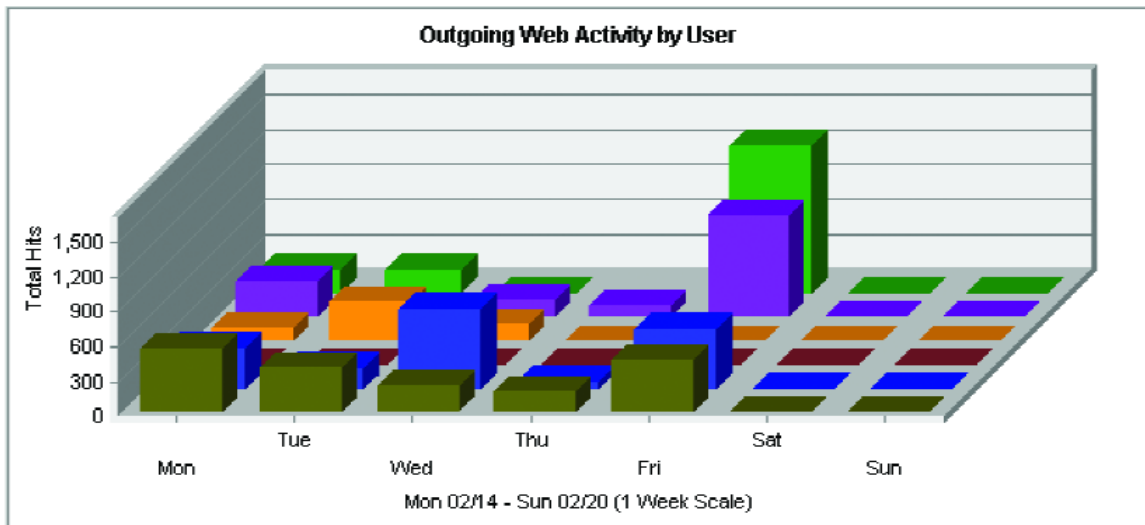
The Outgoing Web Activity by User report shows who logged the most hits to web pages, how many site visits they made and how much time they spent surfing the Web. By pinpointing users who request the most data, in kilobytes, the Top Users (for Outgoing Web Activity) report identifies the top Web surfers. Detailed reports let you see when employees are visiting sites that are not work-related and provide specific evidence of any non-business use.

The Outgoing Web Activity by User and Top Users reports:

- Identify your organization's top Web surfers and top data downloaders.
- Show exactly which sites an employee is visiting.
- Compile detailed statistics to support any action taken against an employee violating e-mail and Internet usage policies.

Outgoing Web Activity by User and Top Users

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



Outgoing Web Activity by User				
	User	# of Hits	% of Total Hits	Kbytes
1	dfunk.webtrends.com	1918	4.56%	77,370
2	andyk.webtrends.com	1818	4.32%	49,123
3	yuriz.webtrends.com	630	1.49%	43,710
4	lukew.webtrends.com	10	0.02%	22,929
5	jimp.webtrends.com	1835	4.36%	22,479
6	wendyb.webtrends.com	2296	5.45%	18,363
7	support.webtrends.com	1334	3.17%	18,032
8	lucyvp.webtrends.com	1127	2.67%	18,013
9	andyx.webtrends.com	42	0.09%	15,397
10	evitad.webtrends.com	980	2.35%	13,934
Subtotal for Users Above		12000	28.52%	297,355
Total for the Log File		42072	100%	644,448

10. Are employees using the Internet legally and productively?

01

02

03

04

05

06

07

08

09

10

Recreational surfing isn't just a drain on productivity, and employees using business resources for personal surfing and downloading can expose your organization to liabilities.

Though most employees know not to visit sites with objectionable content, IT professionals recognize that this type of Web surfing still happens frequently. Instead of wasting your time digging through logs to see if employees are using company time, violating policy or introducing legal issues, use NetIQ's Firewall Reporting products to scrutinize surfing and help you solve any misuse problems.

The Most Popular Core Categories* report tracks user sessions in five Core Categories: Sexually Explicit, Gambling, Hate Speech, Drugs/Alcohol and Violence. NetIQ's Firewall Reporting products embed a URL categorization database from SurfControl, one of the leaders in Web content filtering software. Core categories consist of URLs that are potentially liability threats to an organization, and General categories—including news, sports, job search, etc.—are non-productive sites. The Most Popular Core Web Pages report lists the URLs and names of the Web pages employees visit most often and provides details of inappropriate surfing. Armed with this information, you can decide if an employee merely needs a reminder, or if disciplinary action is required. Similarly, the Most Popular General Categories and Most Popular General Web Pages reports reveal when employees are visiting web sites that detract from productivity.

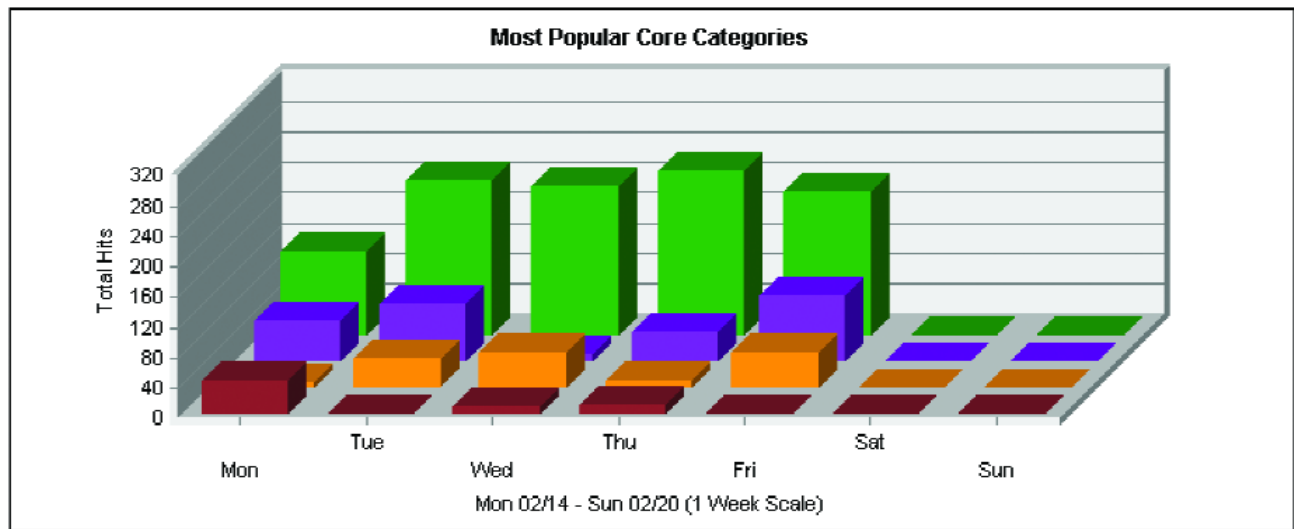
The Most Popular Core/General Categories/Web Pages reports:

- Uncover whether employees visit inappropriate or objectionable web sites and reveal any questionable, offensive or actionable downloads.
- Discover when employees are surfing in violation of established policies, including counter-productive recreational surfing.
- Provide detail so you can take appropriate steps, ranging from reminder messages about policy to serious disciplinary action.

*Two SurfControl databases index Web sites associated with the Core categories and General categories. You can update these databases with a one-click step from the Firewall Suite user interface. Future versions of Security Reporting Center will also offer this feature.

Most Popular Core Categories

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



Most Popular Core Categories				
	Web Site Category	Hits	% of Total	Visits
1	Sexually Explicit	6005	11.74%	220
2	Gambling	880	1.72%	60
3	Drugs/Alcohol	405	0.79%	75
4	Hate Speech	375	0.73%	50
5	Violence	10	0.02%	5
Subtotal for Categories Above		7675	14.85%	410
Total for Log File		51187	100%	4538

To download FREE NetIQ Firewall Reporting product trials,
visit www.netiq.com/go/firewall



Contacts

Worldwide Headquarters

NetIQ Corporation
3553 North First Street
San Jose, CA 95134
713.548.1700
713.548.1771 fax
888.323.6768 sales
info@netiq.com
www.netiq.com

NetIQ EMEA
+44 (0) 1784 454500
info@netiq.com

NetIQ Japan
+81 3 5909 5400
info-japan@netiq.com
www.netiq.com/japan

For our offices in Latin America & Asia Pacific,
please visit our web site at www.netiq.com/contacts

06 07 08 09 10

THE 10 REPORTS...EVERY FIREWALL/SECURITY ADMINISTRATOR LIVES FOR



WebTrends, the WebTrends logo, NetIQ and the NetIQ logo are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names may be trademarks or registered trademarks of their respective companies.