

*How To Guide*

# **XRoads** Networks

Edge Network Appliance How To Guide:

Reporting

## Edge Configuration Series Reporting Overview

The Reporting portion of the Edge appliance provides a number of enhanced network monitoring and reporting capabilities.

WAN Reporting – Provides detailed usage reporting for WAN links.

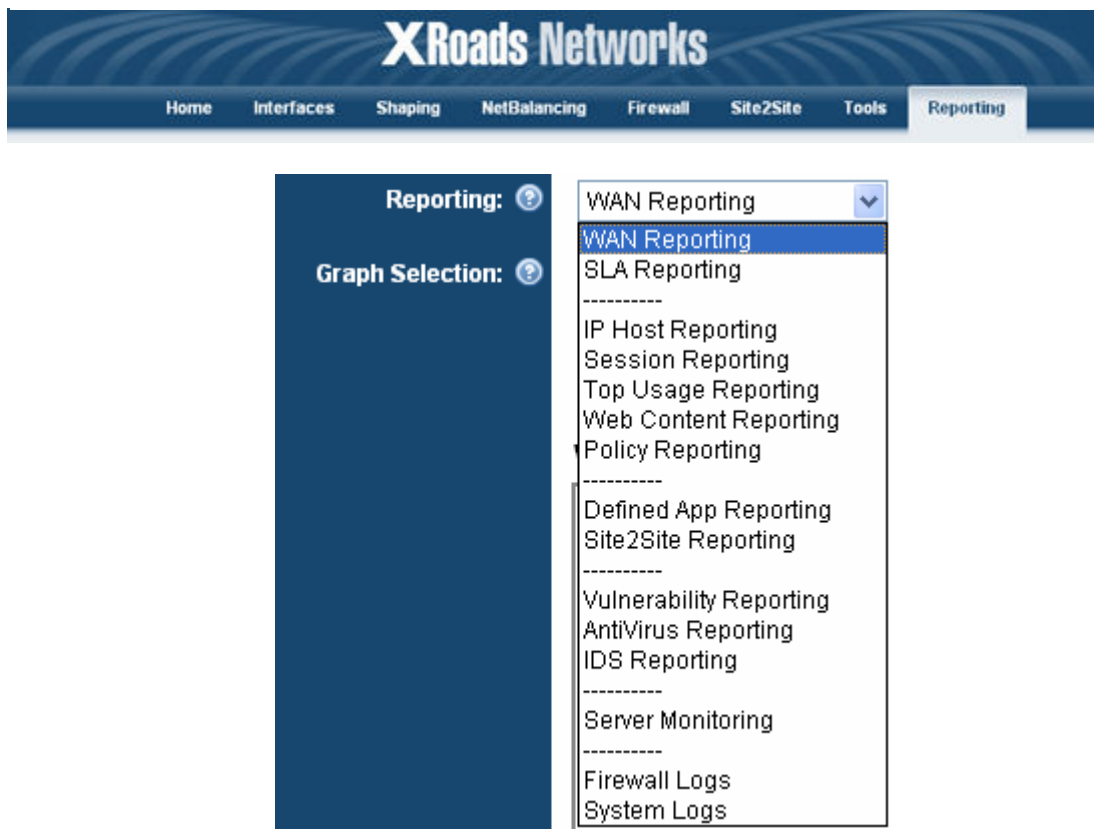
SLA Reporting – Provides service level statistics for remote networks.

XFlow Reporting – Shows top users, applications and pairs.

Shaping Policy Statistics – Useful for determining per user bandwidth access.

Server Monitoring - Alert when a node is down, monitor latency.

Syslog Server – Send syslog messages for outages or when thresholds are exceeded.

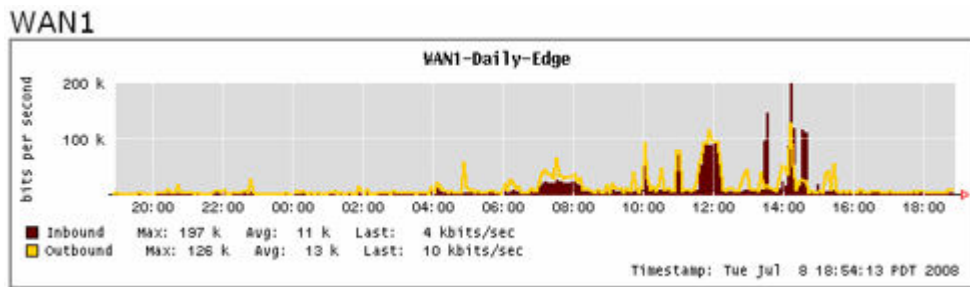


## WAN Reporting

Our WAN reporting module provides complete traffic statistics for the Edge appliance. Both inbound and outbound usage is displayed on a continuous graph. Statistics are available on a daily / weekly / monthly and yearly basis.

Graphs can be cleared by clicking the 'Reset Graphs' button. Statistical information is updated every fifteen minutes. All statistics are provided in BITS PER SECOND measurements. The bottom of the graph also displays the MAX/AVG/CURRENT bps throughput.

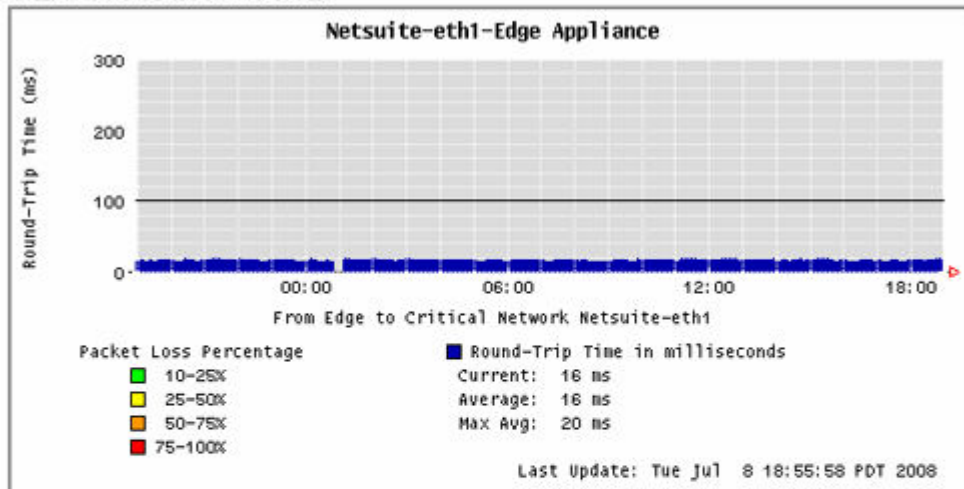
The WAN reporting displays each interface separately so that comparisons can be made of the utilization of each link. These graphs are helpful in determining how application traffic should be routed to achieve the best overall usage of bandwidth.



## SLA Reporting

Our SLA reporting module can confirm service level agreements and show which network paths are providing the best path to a remote destination.

## SLA-Netsuite-eth1



Time	Avg	Min	Max	Packet Loss	Jitter	Status
Current	16.480	15.974	16.986	0%	0.506	●
Fifteen Minutes Ago	16.492	15.517	17.468	0%	0.983	●

The statistics produced by the SLA reporting provide detailed analysis of each WAN connection to a remote destination, as defined in the Best Path Routing module.

### Display Critical Networks (Latency, Packet Loss, Responsiveness)

When using Best Path Routing™ these graphs are available via the Reporting module. These graphs provide detailed network path information based on the critical network defined in the Best Path Routing menu option.

These graphs provide useful SLA (Service Level Agreement) information and have been proven effective in obtaining rebates from service providers when SLAs are not met. Additionally, these graphs are helpful in determining which WAN interface a critical application should be routed.

These graphs are also helpful in identifying poor performing WAN link. When a link is under performing there will be gaps in the report (as seen above) or the color of the reports will be green/yellow/orange or red. The higher the packet loss, the more critical the color becomes on the graph.

SLA reports which consistently show yellow to red graphs show that the link is not operating very well and the customer should consider changing providers.

## XFlow Reporting

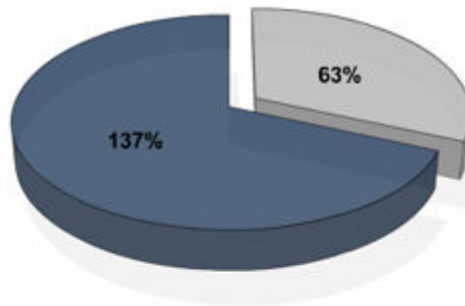
XFlow is a technology developed by XRoads Networks to track network connections and gather network statistics which can be used to generate 3D graphs for easy viewing. The following reports were generated by using XFlow reporting.

### IP Session Reporting

These reports provide high level network usage information. They show how much traffic is inbound vs outbound and which protocols are being used.

**Inbound / Outbound Usage**

■ Outbound 63%



■ Inbound 137%

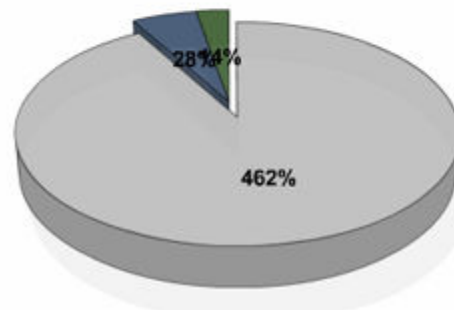
**Protocol Statistics**

■ TCP 462%

■ UDP 28%

■ ICMP 14%

■ Other 0%



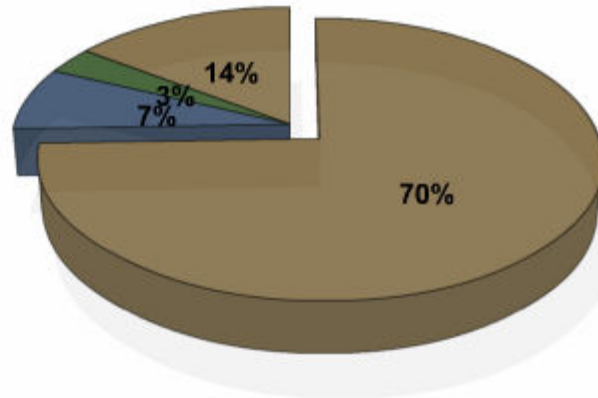
### Per User Application Reporting

The network administrator can then drill-down on a per user basis to see which applications are being used most often by individual end-users.

### Top Applications (per user)

192.168.168.2 - Past Month - 06:50:50 PM\_07/08/08

- WebSSL
- WebHTTP
- 35666
- 58046
- 58993
- 21744
- 64549
- 14336
- 25961
- 27825
- Other



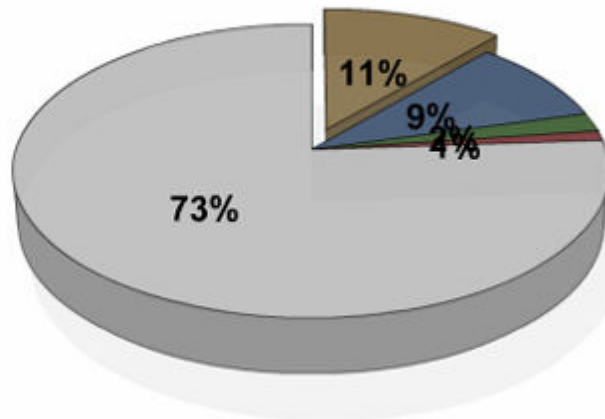
### Top Session Reporting

This reports shows which peer-to-peer connections are using the most bandwidth. This report is helpful for identifying high traffic usage and to see which servers / remote networks are used most often. In the graph below we see that port 5060 is the top session, this is a VoIP PBX located at 192.168.167.7.

### Top Sessions (percentage of total traffic)

Past Month - 06:52:40 PM\_07/08/08

- 192.168.167.7-5060
- 192.168.168.7-5060
- 192.168.168.140-123
- 192.5.41.41-123
- 192.168.168.10-138
- 192.168.168.10-137
- 192.168.168.3-138
- 192.168.168.2-WebSSL
- 192.168.168.50-137
- 192.168.168.2-14336
- Other

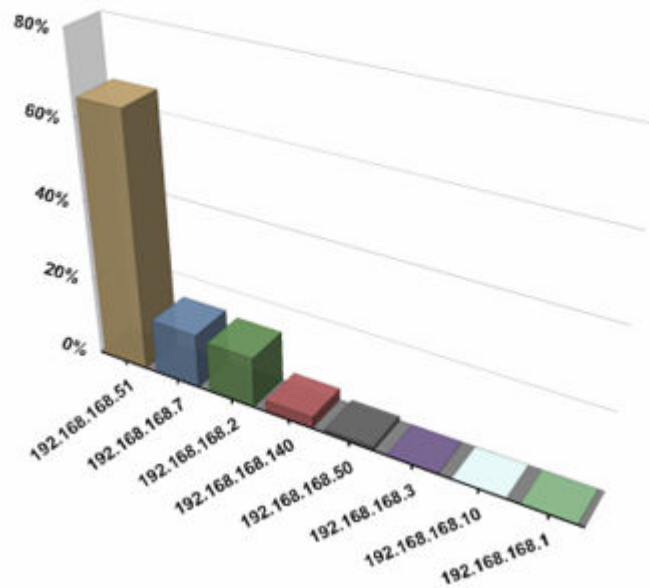


## Top Usage Reporting

These are the most used reports, they show who the top talkers are. Once a network administrator understands who the top talkers are, they can more easily determine how to shape the bandwidth. In this graph we see that 192.168.168.51 is using 4x the amount of bandwidth as the other nodes. In the graph below we can see exactly how much bandwidth each of these devices is using.

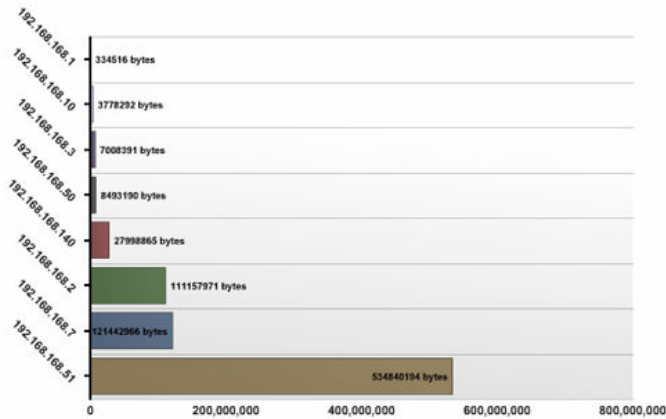
### Top Users/Devices

INTERNAL - Past Month - 06:44:42 PM\_07/08/08



### Top Usage Per User/Device

INTERNAL - Past Month - 06:44:42 PM\_07/08/08



## Top Applications

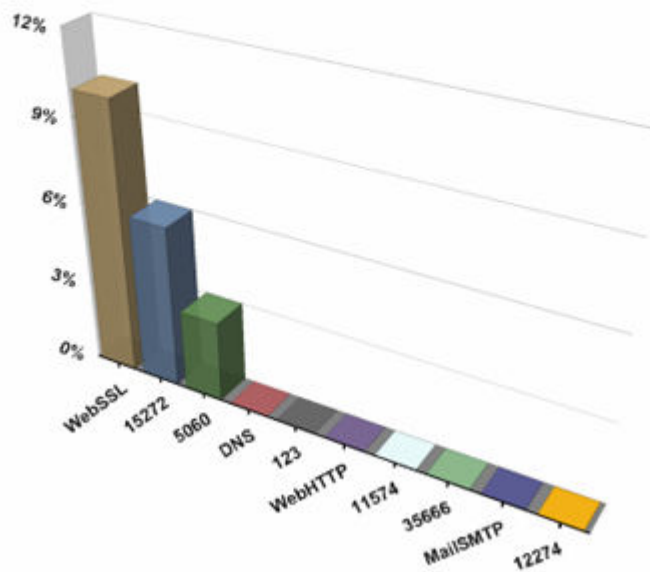
In order to quickly see whether any unauthorized applications are using a large amount of bandwidth use the top applications graph. With this report network administrators can quickly see whether any unwanted applications are being used, and if they are how much bandwidth they are using.

With this report in hand the network administrator can create shaping policies to limit access to those applications which are unauthorized and thus remove them from this list.

### Top Applications

Outbound Initiated - Past Month - 06:46:42 PM\_07/08/08

WebSSL 15272 5060 DNS 123 WebHTTP  
11574 35666 MailSMTP 12274



## Web Content Reporting

When web content filtering is enabled via the Firewall menu these reports become active. The network administrator may view Live Requests, search the web usage log, or generate high level reports for top allowed and denied sites.

Reporting:

Web Filter Reports:    (Reset URL Logs)

(Top Usage Based On Activity Timeframe)

Select a report and click the Generate Report button.

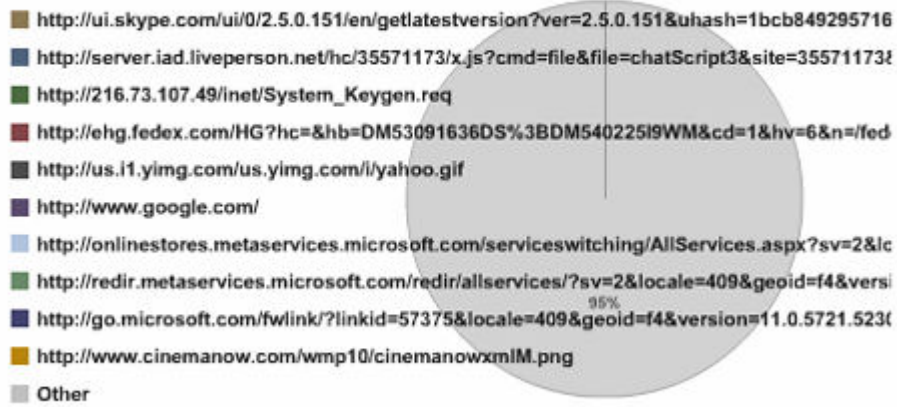
Note: This graph requires web content filtering.

Web content filtering is currently: Enabled

These graphs shows the top allowed and denied sites accessed by end-users on the network. These graphs are helpful to see where most of the web traffic is going within the network and which denied sites are being attempted.

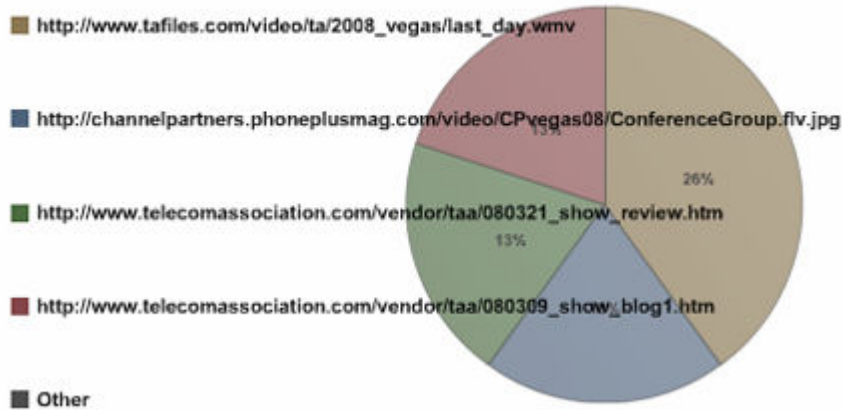
### Top Allowed Sites

Monthly - 02:05:48 PM\_06/02/08



### Top Denied Sites

Monthly - 02:05:48 PM\_06/02/08



Live Requests – The live requests report show the live “real-time” URL requests being made through the web filter. This report is useful for troubleshooting web related issues and to get a quick look at who is going where.

Reporting: Web Content Reporting

Live Web Requests: << Back Refresh

Most Recent Requests

Time	User Address	Domain URL
Tue Jul 8 16:46:32 2008	192.168.168.2	http://www.netbrite.com/portal/home.html
Tue Jul 8 16:46:32 2008	192.168.168.2	http://www.netbrite.com/portal/javascript/NLP/portal.js
Tue Jul 8 16:46:32 2008	192.168.168.2	http://www.netbrite.com/portal/home.html
Tue Jul 8 16:46:32 2008	192.168.168.2	http://www.netbrite.com/portal/javascript/NLP/portal.js
Tue Jul 8 16:45:48 2008	192.168.168.10	http://www.ups.com/stylsheet/stylesheet.css?V=0108
Tue Jul 8 16:45:48 2008	192.168.168.10	http://zdc.ups.com/ContentServer?cid=271jv&lc_2v&cd=gif?&=1&cdat=12155606852746&cdp=www.ups.c
Tue Jul 8 16:45:47 2008	192.168.168.10	http://www.ups.com/img/1.gif
Tue Jul 8 16:45:47 2008	192.168.168.10	http://www.ups.com/stylsheet/stylesheet.css?V=0108
Tue Jul 8 16:45:47 2008	192.168.168.10	http://zdc.ups.com/ContentServer?cid=271jv&lc_2v&cd=gif?&=1&cdat=12155606852746&cdp=www.ups.c
Tue Jul 8 16:45:47 2008	192.168.168.10	http://www.ups.com/img/1.gif

## Defined Application Reports

In order to monitor a specific end-user, server or application you can create a “user defined report” which will begin monitoring a specific set of criteria as defined below.

Simply enter the name of the report, whether you are monitoring an inbound service, whether you wish this data to be included as part of the application pie chart, and then define the IP address and/or service to be monitored.

Reporting: Defined App Reporting

User Defined Reports: Test80 Daily Generate Report (Select Report)

Select a report and click the Generate Report button.

Select	Name	Host
<input type="radio"/>		

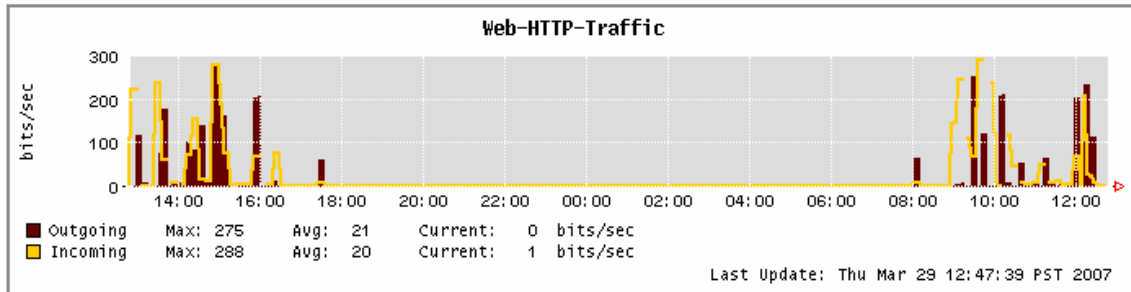
<< Add UDR Select Delete

Name	Last Count In	Last Count Out
------	---------------	----------------

Report Listing: Statistics

Once a report has been created it will begin monitoring the define device/application. After five minutes the follow graph will be created and will continue to show utilization on a per port or per user basis. This report can be generated on a Daily, Week, Monthly or Yearly basis.

Web-HTTP ▼ Daily ▼  [\(Select Report\)](#)



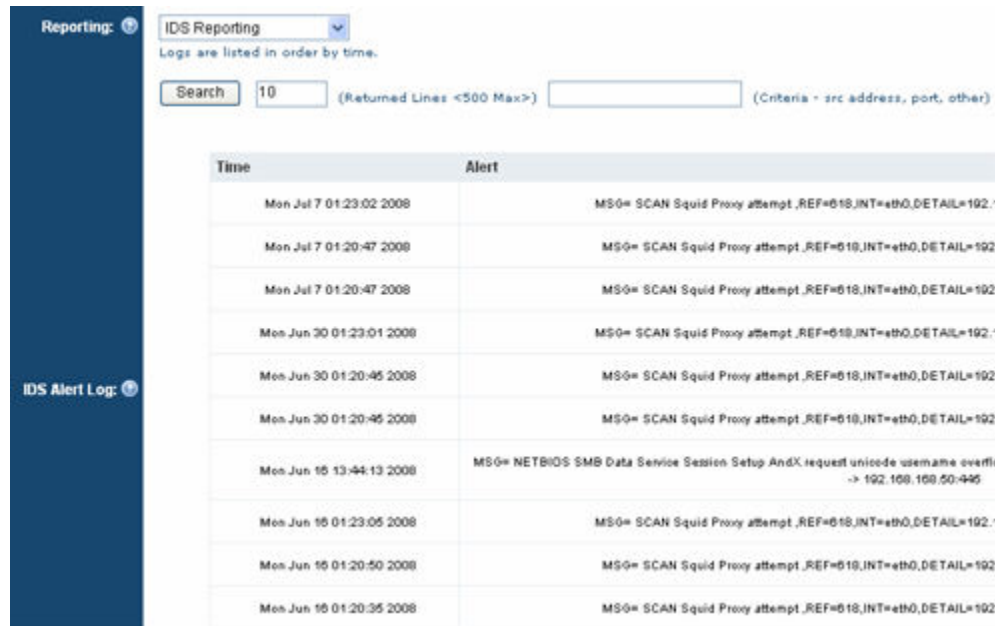
### Shaping Policy Statistics

When using our policy based shaping module to create individual shaping policies for end-users and/or network nodes, a set of statistics is generated for each policy. These statistics are updated every five minutes and are provided in both a standard and graphical output.

Additionally, total monthly usage, peak usage and usage during the past hour / day and week are also stored for easy reference. Full statistics are also downloadable via a comma delimited CSV file.

## IDS Reporting

This report can be used to see the latest intrusion detection vulnerabilities found by the built-in IDS technology from SourceFire. Further this report is searchable so that one can look for logs for specific devices or signature types.

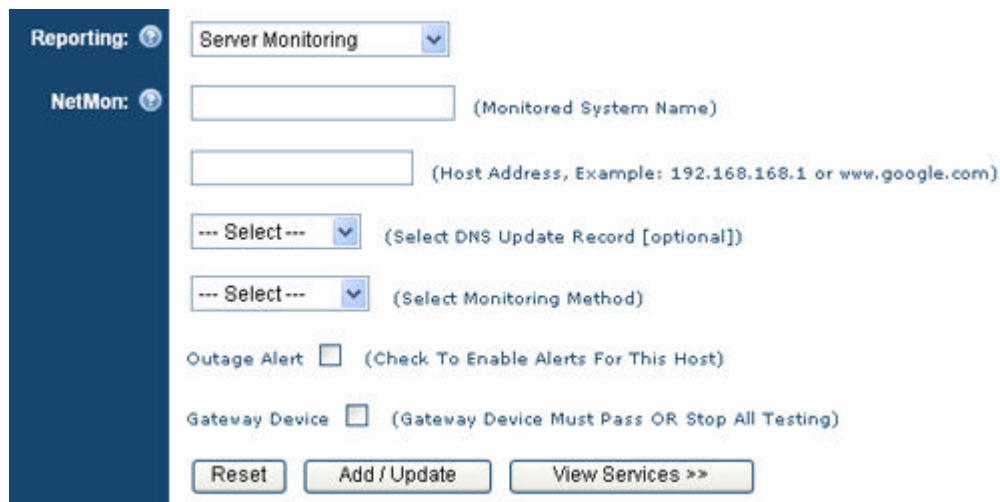


The screenshot shows the 'IDS Reporting' interface. On the left is a dark blue sidebar with 'Reporting: ?' and 'IDS Alert Log: ?'. The main area has a dropdown menu set to 'IDS Reporting' and a note 'Logs are listed in order by time.'. Below this is a search bar with '10' entered and '(Returned Lines <500 Max>)' next to it. A table of alerts follows, with columns for 'Time' and 'Alert'. The alerts are listed in descending order of time, with the most recent at the top.

Time	Alert
Mon Jul 7 01:23:02 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192.
Mon Jul 7 01:20:47 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192
Mon Jul 7 01:20:47 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192
Mon Jun 30 01:23:01 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192.
Mon Jun 30 01:20:46 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192
Mon Jun 30 01:20:46 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192
Mon Jun 16 13:44:13 2008	MSG= NETBIOS SMB Data Service Session Setup AndX request unicode username overfl -> 192.168.168.50:445
Mon Jun 16 01:23:05 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192.
Mon Jun 16 01:20:50 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192
Mon Jun 16 01:20:35 2008	MSG= SCAN Squid Proxy attempt ,REF=618,INT=eth0,DETAIL=192

## Server Monitoring

This feature provides the ability to monitor internal and external servers to determine their availability. This is an add-on feature as it does not tie into the actual routing table at this time. Server monitoring can be accomplished via either ICMP or HTTP testing.



The screenshot shows the 'Server Monitoring' configuration interface. On the left is a dark blue sidebar with 'Reporting: ?' and 'NetMon: ?'. The main area has a dropdown menu set to 'Server Monitoring'. Below this are several input fields and checkboxes: 'Monitored System Name', 'Host Address, Example: 192.168.168.1 or www.google.com', '--- Select --- (Select DNS Update Record [optional])', '--- Select --- (Select Monitoring Method)', 'Outage Alert  (Check To Enable Alerts For This Host)', and 'Gateway Device  (Gateway Device Must Pass OR Stop All Testing)'. At the bottom are three buttons: 'Reset', 'Add / Update', and 'View Services >>'.

Steps for settings up server monitoring:

Step 1) Enter a server name.

Step 2) Select the test type (ICMP/HTTP) and enter the appropriate address to test.

Step 3) Enable alerting and make sure to add an Outage email alert (if required).

## Server Reporting

Within 5 minutes the new server will be tested for accessibility. Once active an alert will be sent whenever an outage is detected. The graph below provides the last outage time and the ICMP statistics if available.

Select	Name	Status	UP/DOWN	Alerts On	Last Outage	ICMP Data (read trip)				Host	Type	GW
						Latency	MIN	AVG	MAX			
<input type="radio"/>	Google		UP		0:11:08,2008-06-20	83.336	83	83	84	www.google.com	WEB	
<input type="radio"/>	TEAR		UP		22:30:35,2008-05-07	0.006	0	0	0	192.168.100.100	ICMP	Yes

## System Logging

The appliance provides a fully functional system logging utility to allow network administrators examine configuration changes, system alerts, or even all new connection attempts. Outage alerts, route changes, and firewall updates are all logged to this utility.

## Syslog Server

All logged information can be sent to an external syslog server by entering its IP address in the field provided.

NOTE: All logs are dated using the current system time.

**Reporting:**

**Syslog Server:**  .  .  .  (Server To Send Syslog Messages)

**Syslog Options:**

- Enable  Disable (Check To Include Firewall Logs)
- Enable  Disable (Check To Include WAN Data)
- Enable  Disable (Check To Include Application Usage Reporting)
- Enable  Disable (Check To Include SLA/Server Alerts)
- Enable  Disable (Check To Include System Stats)
- Enable  Disable (Check To Log ALL New Sessions - Firewall must be enabled)

**WARNING:** The log all new sessions option can generate large volumes of traffic.

**System Logs:**

```
Edge EDGE-0090FB048C4A 01:11-07/08/08 Email Alert Executive Support Report My home lab - Tue Jul 8 01:10:15 PDT 2008
Edge EDGE-0090FB048C4A 01:11-07/07/08 Email Alert Executive Support Report My home lab - Mon Jul 7 01:10:17 PDT 2008
Edge EDGE-0090FB048C4A 01:11-07/06/08 Email Alert Executive Support Report My home lab - Sun Jul 6 01:10:14 PDT 2008
Edge EDGE-0090FB048C4A 01:11-07/05/08 Email Alert Executive Support Report My home lab - Sat Jul 5 01:10:16 PDT 2008
Edge EDGE-0090FB048C4A 01:11-07/04/08 Email Alert Executive Support Report My home lab - Fri Jul 4 01:10:15 PDT 2008
```