



LUCIDVIEW GUARDIAN

1 Overview

The LucidView Guardian is a highly integrated network diagnostic and bandwidth management tool that features unique solutions to problems facing virtually every medium to large scale network today. It features a central management point where network traffic can be monitored and fine-grained prioritization can be applied.

Sophisticated trend analysis can easily be performed over long periods of time to provide critical planning information, like how much bandwidth is still available or how a new server or service would impact the current bandwidth usage. In the short term, since the Guardian monitors the network in real time, network anomalies can be traced as soon as they occur. This is particularly useful for detecting and managing zero-day attacks and tracing network faults.

The Guardian can prioritize different network services right down to an expression matching the URL. This allows the flexibility to map business rules directly to network priority: media files that are business related receive a higher priority than files that are not. Traffic priority or firewall rules can also be done according to the geographical location of the host IP address. This is ideal for cases where local and international traffic needs to be handled differently.

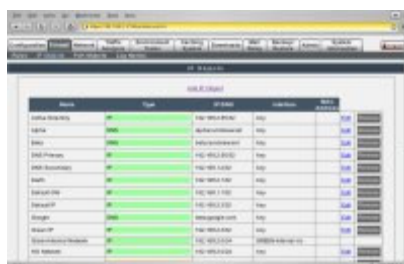
The Guardian can also become part of the normal end-user experience of the casual user of the network. It provides transparent, secure, Kerberized authentication with an Active Directory, linking user credentials to network traffic with no added host software or configuration needed. Each user is able to view their web browsing statistics, network bandwidth usage, cache efficiency, estimated time spent using the Internet and many other variables via the interface. In companies where the management structure has been mapped in the Active Directory a feature is also available allowing managers to view the statistics of their subordinates.

In order to allow bandwidth to be redistributed even into off-peak hours, the Guardian features a highly configurable transparent download manager. It integrates into the end-user interface and improves cache efficiency by recognizing downloads as potentially identical even when downloaded from different web sites. This becomes a communal resource where large updates or commonly used applications only need to be downloaded once to become available for the whole network. It seamlessly integrates with the cache, so even automated applications like Windows Update do not need to re-download updates if it is locally available.

The Guardian features a mail relay with sophisticated logging capability. Errors in the mail setup can easily be traced and problem email servers can be identified. Detailed reports can give a breakdown of all the email traffic passing through the relay with several useful summaries added.

2 Feature Breakdown

2.1 User Interface and Access Control



The Guardian's graphical user interface is available over a secure HTTPS connection and functions with any modern web browser. It features customizable levels of access control and the creation of multiple administrator and reporting capable accounts. Access can easily be restricted to the local network or granted for remote administration.

2.2 Gateway Capabilities

The Guardian is capable of functioning in a fully transparent bridge-like configuration, integrating with an existing firewall or router. It can also function as an explicit gateway, routing between three network interfaces, allowing for the creation of a DMZ. The Guardian also integrates into the DNS and NTP services on the network.

2.3 Host/Network and Service Labeling



The Guardian allows the association of descriptive labels to hosts, networks and services on the network. This allows the configuration screens to be human readable and makes much more pertinent information available to the viewer at a single glance. The labels are easily interchangeable: the same rule may apply to a single host, a network, a group of hosts or even a geographical location.

Some of the types of labels the Guardian supports are:

- Host IP,
- network range,

- DNS name,
- geographical location,
- MAC address,
- network port or port range,
- associated network interface and
- groups containing elements of the above.

Integrated Firewall/Routing Solution

The Guardian has a full enterprise-level firewall capable of an almost infinite level of customization. The networking stack uses the descriptive labels to determine the route a packet should take on the network, and performs any modifications specified. Packets can easily be accepted, denied, NATed, prioritized or masqueraded, depending on the firewall rule set up.

Here is number of examples:

- International traffic can be given priority over local traffic.
- Active Directory replication bandwidth can be reserved.
- Peer-to-peer traffic can be de-prioritized.
- Business-critical URLs can be given priority.
- Services like video conferencing and VOIP can be assured quality of service.

2.4 Bandwidth Manipulation



The Guardian categorizes network traffic into different streams to facilitate bandwidth manipulation. These streams can be as course-grained as a range of IP addresses and network ports, or as fine grained as web traffic transferring a file with a specific extension. The Guardian allocates available bandwidth to a stream based on rules supplied for those streams. The Guardian supports three parameters per stream: priority, reservation and maximum allocation.

2.4.1 Reservation

The Guardian can reserve a specified amount of bandwidth for use by a specific stream. If that stream is not currently active, or requires less bandwidth than the reservation, the difference goes to the unallocated pool, to be divided up based on the priority of the streams. With this option, even a low priority stream can still be assured of a minimum quality of service.

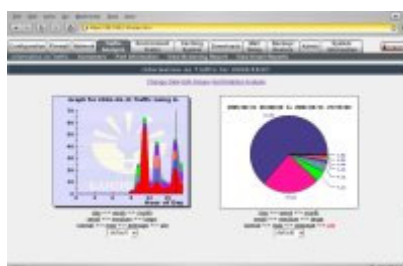
2.4.2 Priority

If excess bandwidth is still available after all the streams have had their minimum reservation met, bandwidth is allocated to streams according to priority. This means that bursting traffic can be allocated a relatively high priority and, if bandwidth is available, preempt lower priority traffic.

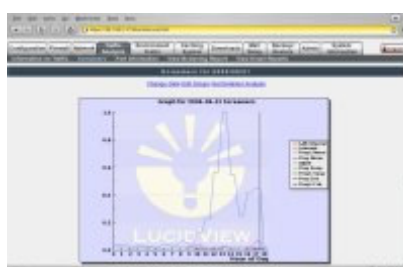
2.4.3 Maximum Allocation

A stream may be limited to a maximum bandwidth allocation. This is often useful to debug network applications by simulation a smaller connection. It's also useful to curb errant network applications where prioritization is inadequate and to manage denial of service attacks.

2.5 Network Traffic Analysis



The Guardian offers a customizable real-time view of all the traffic flowing through it. Streams marked in the firewall module are automatically available to be plotted. Graphs can be switched to average mode, to illuminate trends and compare traffic states.



The Guardian also supports a unique feature to separate noisy traffic from regular traffic. Certain classes of traffic (like port scans and network worms) do not necessarily utilize a lot of bandwidth, but open up a large amount of remote connections. Monitoring the bandwidth would not suffice to spot this class of traffic on the network. Normal hosts that perform these tasks are certain types of network monitors, routers NATing or masquerading and large-volume email servers. The Guardian detects these automatically and adds them to another graph. This is highly useful to quickly spot errant peer-to-peer hosts, classes of viruses and probable attacks on the network.



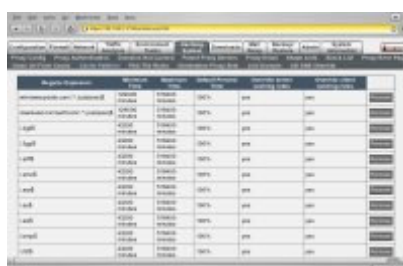
The Guardian maintains a large detailed history of the traffic patterns that it has observed. While the graphing mode provides quick and easy access to the most common traffic analysis, the entire history is also available to be queried using an analysis tool. Simple queries like: "How much bandwidth does the mail server use?" can easily be performed over a user-specified period. More advanced queries can even be exported to a CSV file to be imported in a spreadsheet. Every parameter on a stream can be extracted this way. Combined with a full history kept for as long as two months and graphs available for six months, this gives the network administrator an incredible tool to monitor the network with over time.



The Guardian also provides a range of tools to pro-actively monitor the network. These do not require any special client-side software. A service like HTTP can also be monitored and the performance over time can be graphed quite conveniently. Specific network routes can be monitored for delays and this helps pinpoint network faults in real time. This provides the network administrator with an important daily view of the network delays, not necessarily associated with bandwidth throughput, but none the less critical for applications like VOIP.

2.6 Web Proxy

The Guardian can integrate with an Active Directory to provide single sign-on authentication for end-users. This utilizes highly secure kerberized authentication that comes default with any Active Directory client, linking each user with their specific web traffic. Serving as a web proxy and cache, it allows business rules to be directly mapped to network bandwidth management policies. Business critical web sites and files can easily be given priority, yet non-critical traffic can still utilize the full bandwidth pipe if it is available.



Source	Destination	Protocol	Bytes	Packets	Connections	Time	Rate
192.168.1.1	192.168.1.2	HTTP	1024	10	1	0.1s	102400
192.168.1.1	192.168.1.3	HTTPS	2048	20	2	0.2s	204800
192.168.1.1	192.168.1.4	FTP	512	5	1	0.05s	51200
192.168.1.1	192.168.1.5	SMTP	1536	15	1	0.15s	153600
192.168.1.1	192.168.1.6	POP3	768	7	1	0.07s	76800
192.168.1.1	192.168.1.7	IMAP	1280	12	1	0.12s	128000
192.168.1.1	192.168.1.8	SSH	256	2	1	0.02s	25600
192.168.1.1	192.168.1.9	TELNET	128	1	1	0.01s	12800
192.168.1.1	192.168.1.10	SMTP	1536	15	1	0.15s	153600

The caching system is highly configurable, allowing the network administrator to choose how long objects can be in the cache. Objects can be deleted from the cache and both client and server-side commands can be superceded by the caching system. Web sites can be forced not to cache, in order to accommodate web sites designed without caching in mind. Block lists can

be used to disallow users certain sites. The caching server can also join an existing caching hierarchy.



The Guardian features an integrated download manager that compares the file that is being attempted to be downloaded with files that have previously been downloaded. This allows a user the opportunity to download a file in the local download cache rather than directly from the Internet, even if it uses a different URL or web site. The download manager can be activated for a specific site, or a broad range of URLs, file types and files larger than a certain size. Overrides can be specified for applications that automatically update themselves from the Internet. The users can also view files that other users have downloaded, along with their descriptions and dates the file was requested. This encourages a local archive of often-downloaded utilities that are valuable to users, and might have escaped the notice of an administrator. A user also has the opportunity to schedule the download as high-priority rather than low priority against their name: This allows business critical documents and applications to preempt normal traffic without the intervention of an administrator.

2.7 Web Browsing Traffic Analysis

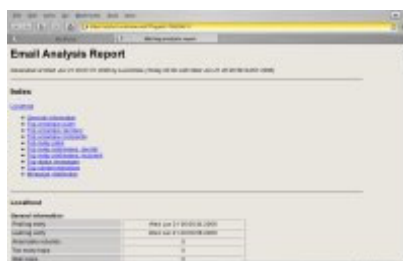


The Guardian keeps detailed logs regarding the web browsing of all the users on the network. This information is available in a user-friendly query mechanism. Parameters like the URL, user name, estimated time spent on the Internet, number of connections made and caching statistics can be viewed in summary or for a specific URL, user name or time. It's easy to pick out the top traffic generating sites and users. It's also easy to determine what sites need to be cached in order to maximize the bandwidth efficiency.

The Guardian allows each user to view their own browsing statistics. This is an invaluable tool in many cases to catch spyware, adware and other unauthorized web traffic. The Guardian can also use management structures incorporated in the Active Directory to allow managers to view the browsing habits of their subordinates. This can be extended several levels deep, and allows managers to identify frequently used project web sites that are prime candidates for caching.

The Guardian can also send regular email reports based on web browsing statistics to managers and users alike. This can inform users what rank they are and how they compare to the rest of the company with regards to Internet usage. The email template can be customized with varying degrees of information or news.

2.8 Mail Relay



The Guardian features an integrated mail relay. This is coupled with a reporting facility that allows a network administrator to spot problem emails being relayed. Email can also be managed like any other stream by the bandwidth management tools.

2.9 Diagnostics and Self-monitoring

The Guardian features a number of diagnostic utilities to test the network environment. Test emails can be generated, the Active Directory can be queried and routes can be traced, among others.

The Guardian continuously monitors its own hardware using on-board sensors. This extends to disk health monitoring, multiple internal temperature sensors and CPU utilization. The Guardian has built-in redundancy, so a hardware failure would not result in loss of data. It also features strong cryptographic security so that in the event of theft, no possible security compromising information can be retrieved off the device.