



LUCIDVIEW ENHANCED GUARDIAN AND COMMAND CENTRE FEATURE SET

Confidentiality Notification

All data contained in this document, all of its schedules, and attachments shall be deemed confidential and proprietary to LucidView (Pty) Ltd, and shall not be disclosed by any recipient, in any manner, to any party, without the prior written consent from LucidView (Pty) Ltd.

Copyright Notification

All rights reserved. No part of this document may be used, reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the copyright owners.

Copyright © LucidView (Pty) Ltd 2005-2015

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.

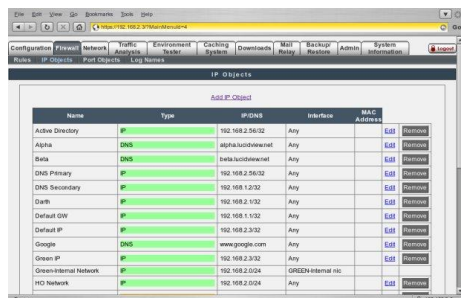
The Guardian's core features can further be extended by adding plug-in modules. These modules seamlessly integrate with the existing features of the Guardian, providing added functionality when it is needed, allowing the Guardian to scale as new features become available on the network.

The Command Centre is a separate device that provides for central management of two or more LucidView Guardians within an organization. It is used to manage all the LucidView Guardians from a single site and to take proactive measures over the entire network when an incident is picked up by one of the Guardians. When a particular LucidView Guardian detects a source of errant data, e. g. a virus attack, it will both act to limit its impact and send a message to the Command Centre. The Command Centre will respond by triggering the other LucidView Guardians to take the same action and prevent the attack from spreading.

The Command Centre is also used for the technical upkeep of all the Guardians. It provides for central backup and restore of all the Guardians, loading of data into replacement devices, distribution of software fixes and enhancements, configuring of remote Guardians and a master archive for extensive trend analysis and audit trails.

2. LUCIDVIEW ENHANCED GUARDIAN FEATURE SET

i. User Interface and Access Control

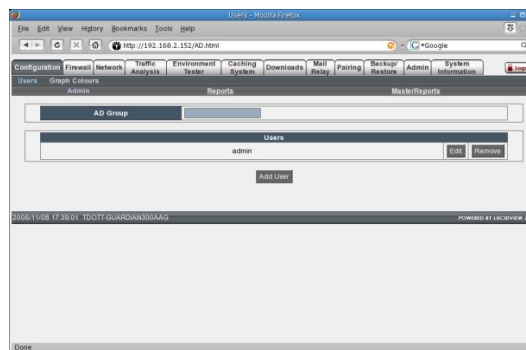


| Name | Type | IP/DNS | Interface | MAC Address | Actions |
|------------------------|------|---------------------|--------------------|-------------|-------------|
| Active Directory | IP | 192.168.2.56/32 | Any | | Edit Remove |
| Alpha | DNS | alpha.lucidview.net | Any | | Edit Remove |
| Beta | DNS | beta.lucidview.net | Any | | Edit Remove |
| DNS Primary | IP | 192.168.2.56/32 | Any | | Edit Remove |
| DNS Secondary | IP | 192.168.2.56/32 | Any | | Edit Remove |
| Darth | IP | 192.168.2.1/32 | Any | | Edit Remove |
| Default GW | IP | 192.168.1.1/32 | Any | | Edit Remove |
| Default IP | IP | 192.168.2.3/32 | Any | | Edit Remove |
| Google | DNS | www.google.com | Any | | Edit Remove |
| Green IP | IP | 192.168.2.3/32 | Any | | Edit Remove |
| Green-Internal Network | IP | 192.168.2.0/24 | GREEN-internal-net | | Edit Remove |
| HD Network | IP | 192.168.2.0/24 | Any | | Edit Remove |

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.

II. Access Control via Active Directory Groups

The Enhanced Guardian allows administrators to allow access control to be derived from Active Directory groups. This slots in with the existing Active Directory administration structures, allowing WAN and LAN administrators access to the correct level of configurability on all the Guardians on the network. This allows for an easily applicable central management policy.

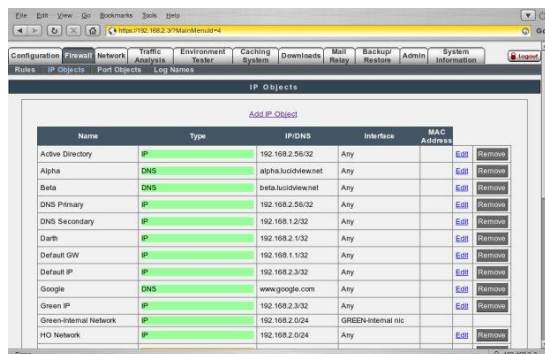


Administratively, since full audit capabilities are available on all Guardians, full accountability can always be provided for any change in the configuration.

III. 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.

IV. 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,
- Type-of-service tags, and
- groups containing elements of the above.

V. Integrated Firewall 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

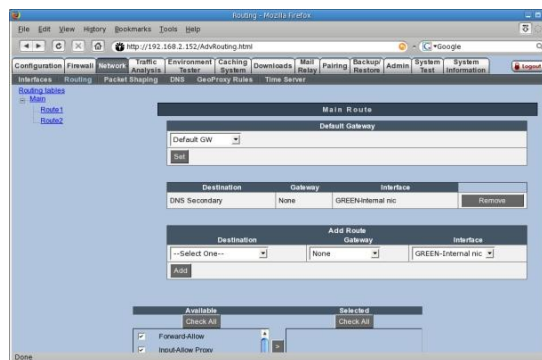
should take on the network, and performs any modifications specified. Packets can easily be accepted, denied, NATed, prioritized or masqueraded, depending on the firewall rule set up. Here are a number of examples:

- 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.

VI. Advanced Routing

The Enhanced Guardian has the ability to handle multiple routing tables and intelligently decide which route a connection should take. Routing tables can be dynamically assigned based on firewall matching rules.

A specific example would be if all mail traffic were to be redirected to a specific gateway on a separate link. The Enhanced Guardian would be able to route all mail transparently to the new gateway, irrespective of the host it originated from. Web browsing traffic from the same host would be routed over a different gateway. This gives the flexibility of installing transparent traffic scanning devices and intrusion detection services on potentially dangerous traffic, while allowing critical traffic to bypass the slow process of being scanned and verified.



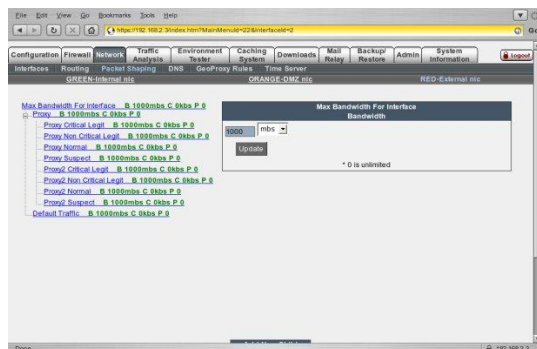
VII. VPN

The Enhanced Guardian implements a full routed VPN solution between other Guardians. This allows for secure communications over the WAN, encrypting all the traffic, yet retaining the ability to shape within the encrypted stream.

The Enhanced Guardian also supports compressing the data before it is encrypted. Depending on the type of traffic carried over the WAN, this can result in substantial gains in bandwidth efficiency.

Additionally, the Enhanced Guardian can easily apply rules as to what kind of traffic should be encrypted and what should not, allowing remote sites that use the Internet to provide the infrastructure for the VPN to determine the optimum route for the traffic they generate: Sensitive traffic to the remote sites travel over the encrypted VPN, while direct Internet traffic remains unencrypted.

VIII. 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.

Streams can be assigned by any firewall rule that can classify traffic: this means MAC-based rules, geographical rules and application-based rules can all be manipulated. Furthermore, the Guardian can manipulate traffic within a protocol. This is highly useful to create rules that allow certain types of files high priority and flag others as suspicious behavior. This extends to sophisticated matching rules that can be applied to the URL of the web site visited, scanning for strings that are flagged high or low priority.

The Enhanced Guardian supports asymmetric shaping: inbound and outbound traffic can be shaped according to different policies.

The Guardian supports three parameters per stream: priority, reservation and maximum allocation.

A. 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.

B. 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.

C. Maximum Allocation

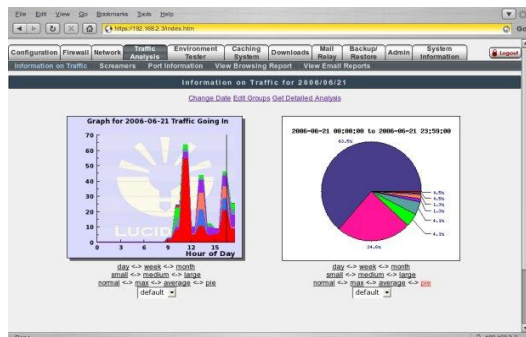
A stream may be limited to a maximum bandwidth allocation. This is often useful to debug network applications by simulation a smaller connection. It's also useful to curb errant network

applications where prioritization is inadequate and to manage denial of service attacks.

IX. Service Labels for MPLS and Intelligent Routers

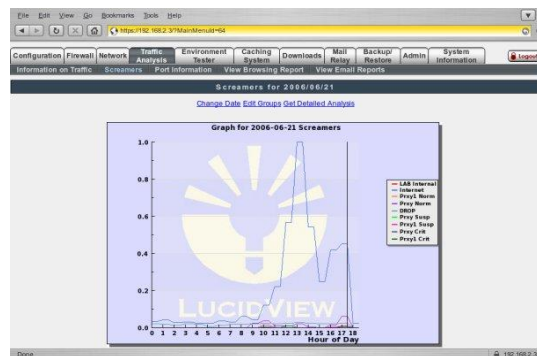
The Enhanced Guardian allows the attachment of QoS labels to every marked stream: this allows seamless integration with MPLS class-based routing, or any other QoS compliant routers and allows for non-critical traffic to be redirected to a lower cost class. This can improve network service delivery while at the same time minimizing costs.

X. 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 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.

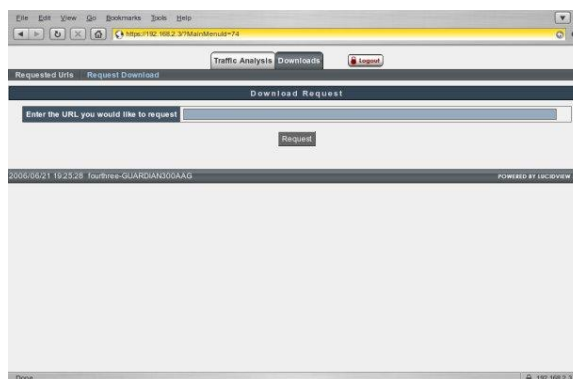
XI. Web Proxy

The screenshot shows the Mikrotik WinBox interface with the Firewall Rule configuration page. The configuration is as follows:

- Configuration:** Firewall Rule
- Chain:** input
- Outgoing Interface:** eth0
- Action:** drop
- Log:** checked
- Rule Name:** rule1
- Chain:** input
- Outgoing Interface:** eth0
- Action:** drop
- Log:** checked
- Rule Name:** rule1

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.



The Guardian has the functionality of running as a transparent caching service. It can be integrated with an existing proxy, replace an existing proxy, or transparently redirect all outgoing web browsing traffic to the internal cache to be managed by itself.

The Enhanced Guardian's proxy is capable of redirecting to different proxies or web servers based on the destination URL. For organizations with a hybrid Intranet/Internet presence, this feature allows the Enhanced Guardian to forward the requests and access the content in a more optimal manner. Combined with the Enhanced Proxy Features in the next section, this allows the Enhanced Guardian to act as an access controller for the Intranet.

XII. Enhanced Proxy Features

The Enhanced Guardian can apply rules to users based on their Active Directory profiles. This can include different shaping profiles and block lists. This is very useful for organizations where users have different tiers of access.

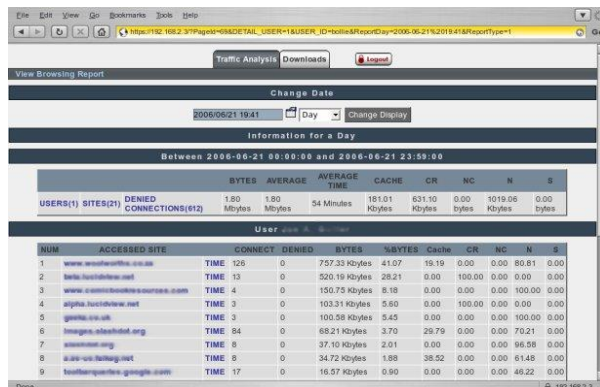
XIII. Reverse Proxy

The Guardian is fully capable of acting as a “reverse proxy” or “website accelerator”. In this mode, the Guardian proxies for a web site, or multiple web sites, providing the following services:

- Load balancing,
- Caching,
- Compression and
- SSL offloading.

XIV. Web Browsing Traffic Analysis

The Guardian keeps detailed logs regarding the web browsing of all the users on the network.



The screenshot shows the 'View Browsing Report' interface. It includes a 'Change Date' section set to '2006/06/21 19:41' and a 'Change Display' button. Below this is a summary table for the day of 2006-06-21 00:00:00 and 2006-06-21 23:59:00. The summary table has columns: BYTES, AVERAGE, AVERAGE, CACHE, CR, NC, N, S. The values are: 1.80 Mbytes, 1.80 Mbytes, 54 Minutes, 181.01 Kbytes, 631.10 Kbytes, 0.00 bytes, 1019.06 Kbytes, 0.00 bytes.

Below the summary table is a detailed table titled 'User and A. S. log'. It has columns: NUM, ACCESSSED SITE, TIME, CONNECT, DENIED, BYTES, AVERAGE, CACHE, CR, NC, N, S. The data rows show various sites accessed, including www.meridian.com, www.lucidview.com, www.comcast.com, alpha.lucidview.net, google.co.uk, images.google.com, www.meridian.org, www.meridian.org, and www.meridian.org.

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

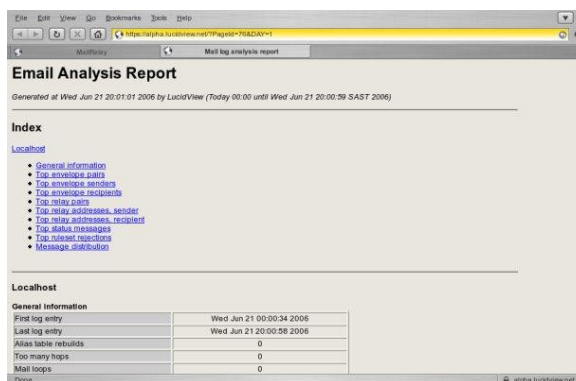
can be extended several levels deep, and allows managers to identify frequently used project web sites that are prime candidates for caching.

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.

XV. 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.

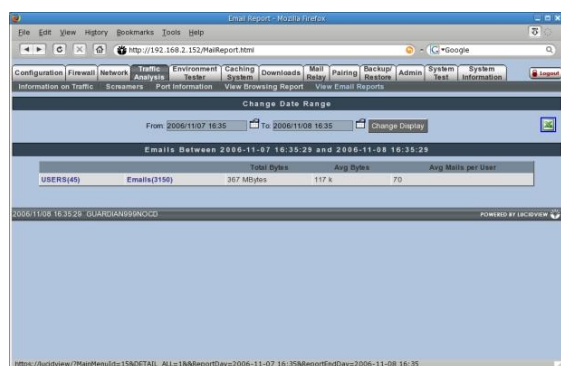
The reports generated by the mail relay show detailed statistics on who the “top talkers” are, both in user terms and domains, or email server terms. These reports point out who the top



senders and receivers are, how many messages they have transferred and the average size of the emails.

The Guardian also supports the use of an industry-standard spam block list that will reject a large percentage of unsolicited email before it is received.

XVI. Advanced Mail Relay Reporting and Abuse Management



The same flexibility and reporting that the Core Guardian provides for web browsing, the Enhanced Guardian applies the mail relay. This opens up a whole new avenue of abuse management, email prioritization and network monitoring. Emails with

large attachments can be made visible to managers, high-priority email domains can be established and malicious emails can be rejected before it reaches the mail server.

The Enhanced Guardian can provide weekly or monthly email reports detailing the email use of all the employees in the company. Optionally, managers can receive reports on statistics for their subordinates, leading to the curbing of email abuse.

It can easily be identified when email is used as a file transfer system. This is inefficient: no proper records are kept, file resuming is not available and it clogs up bandwidth that can be better used for other purposes.

Resource-based billing can easily be implemented: user that subscribe to high-volume mailing lists that have no business-related use can be pinpointed and dealt with.

Very important statistical information can be gleaned from email usage: a virtual map can be generated detailing the most important communication links to and from your organization.

XVII. Integrated Configuration Audit Trail

For maximum accountability, the Guardian implements an extensive involatile audit trail. This allows an administrator to see what configuration changes has been applied, at what time, and by which user account. This information is securely archived and not erasable or modifiable, not even by the administrator with the highest privileges. Usage reports can be generated and activity can be monitored.

XVII. High Availability

The Enhanced Guardian has the option to work in a high-availability scenario. If downtime needs to be minimized, pairing the Enhanced Guardian allows the option for multiple fail- safe routes, ensuring maximum availability of critical services.

The Enhanced Guardian supports the active/passive high-availability solution: Two devices are connected with a heartbeat monitor, and if the primary link fails, the secondary device takes over. This allows for full redundancy on a critical network.

A special “Guardian HA” is available for use in this specific case. This model Guardian can only be used in an active/passive HA configuration, but otherwise supports the entire Enhanced Guardian feature set.

XIX. 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, memory usage, 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.

XX. Database Service Monitor

The Guardian allows the generation of specialized SQL queries to monitor a database server.

XXI. Alerts

The Enhanced Guardian allows the generation of specific alerts based on a programmable rule set. These alerts are fully customizable and can be delivered via email.

This type of alert system, coupled with the Guardian's data analysis facilities is an invaluable tool to spot worms, virus outbreaks and network scanners when they happen. Hackers running vulnerability scanners also trigger certain rules, allowing you to respond quickly to any potential problem on your network.

Alerts are fully configurable to monitor vital WAN applications. If the application uses more or less bandwidth than usual, an alert could be issued.

3. LUCIDVIEW GUARDIAN HA FEATURE SET

I. High Availability

A special "Guardian HA" is available for use in High Availability scenarios. This model Guardian can only be used in an active/passive HA configuration, but otherwise supports the entire Enhanced Guardian feature set.

II. Enhanced HA Cluster for Multiple Sites

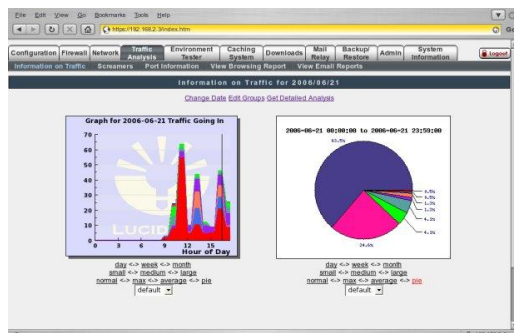
This unique addition to the LucidView product line offers unrivaled centralized management for organizations with a number of remote offices. This Enhanced High Availability solution allows for the management of the WAN traffic of up to 16 sites with unsurpassed availability.

Acceleration of key business applications, emails and VOIP is performed by eliminating the effects of abuse and introducing caching and prioritisation where it matters. The solution is able to manage at least 64 Mbps per site simultaneously for a combined throughput of up to 1 Gbps.

In addition to this the cluster, has a powerful reporting engine to accurately report usage and trends of the various sites, in a human readable form. See the features and specification documentation of the LucidView Enhanced Guardian in HA mode for more details.

4. LUCIDVIEW COMMAND CENTRE FEATURE SET

I. Centralized Collation and Analysis



The LucidView Command Centre collates data for analysis from paired Guardians. This gives an overhead view of the entire WAN, providing the ability to compare usage between branches and allowing for trend analysis and expansion planning.

All the information that is available on the Guardians paired to the Command Centre is available locally on it.

This makes it easy to cross-reference a specific application's network usage over the entire WAN. Monitoring the health of an important business application across multiple LANs is a very simple exercise, and this proves an invaluable resource when planning expansion.

II. Centralized Status Reporting

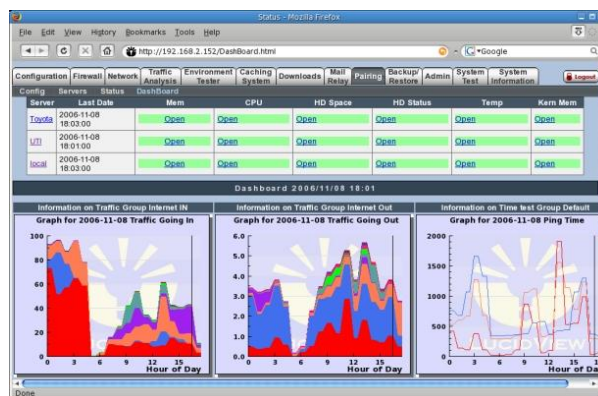
The LucidView Command Centre offers a centralized platform to view the status of all the remote Guardians on the network. Service levels and device health can be monitored at a single point.

The Command Centre provides the ideal method of tracking a zero-day attack on the network and is able to issue alerts on hacking attempts.

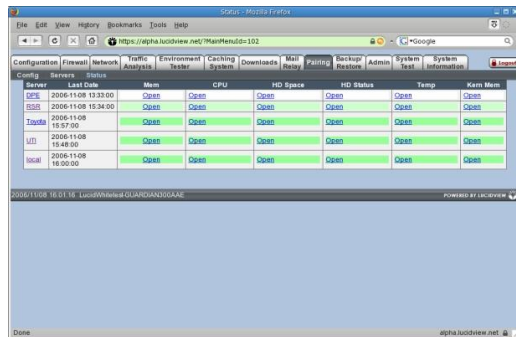
III. Dashboard

The Dashboard provides the ability to view the entire WAN at a glance, and spot problem points and possible problems immediately from a network operations centre.

This output can be specially formatted for a continuous large-screen display. This allows a network operations centre to display a real-time view of the network on a wall screen.



IV. Centralized Administration



The LucidView Command Centre offers a single point of remote administration for all the Guardians paired to it. Managing the configurations of the remote Guardians can be done in a secure and centralized fashion. These are typical administration tasks that the Command Centre make effortless:

- Deploying new Guardians,
- rolling back configurations,
- applying new policies, and
- verifying remote configurations.

V. Centralized Policy Management

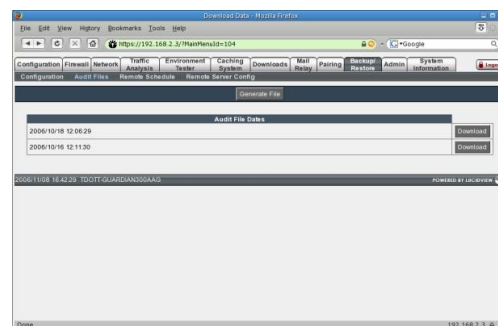
The Command Centre can enforce policies on the Guardians it manages. This provides a powerful QPM solution and includes firewall policies.

The entire LucidView product suite is designed for centralized management. Centrally, one can easily manage infections that are impacting network performance by enforcing blocking rules. A central shaping policy can be shared, as well as any criteria required to implement it remotely.

VI. Remote Configuration Archiving

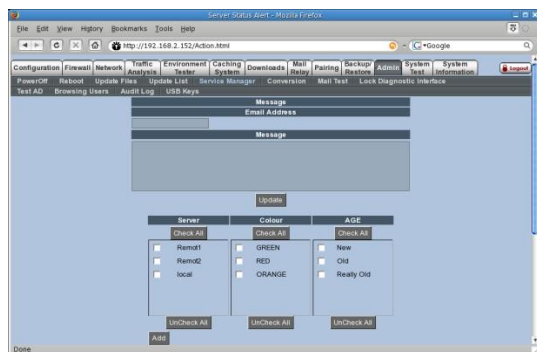
The LucidView Command Centre automatically archives any associated Guardian's configuration if and when it changes. This provides easy remote roll-back functionality whenever it is needed.

The Command Centre also aggregates the remote Guardian audit trails. This allows central report-generation of all WAN administration tasks



that impact the network. Detailed analysis can be done of the impact of every single configuration change on the whole WAN.

VII. Alerts



The Command Centre allows the generation of specific alerts based on a programmable rule set. These alerts are fully customizable and can be delivered via SMS, email and SNMP traps.

This type of alert system, coupled with the Guardian's data analysis facilities is an invaluable tool to spot worms, virus outbreaks and network scanners when they happen. Hackers running vulnerability scanners

also trigger certain rules, allowing you to respond quickly to any potential problem on your network.

Alerts are fully configurable to monitor vital WAN applications. If the application uses more or less bandwidth than usual, an alert could be issued.

VIII. Consolidated view

On the Command Centre a consolidated view is available for all Guardians paired with the Command Centre. This allows data from multiple Guardians to be displayed simultaneously on one figure on the Command Centre interface for easy comparison and monitoring purposes.