

Migrating from MIMESweeper for Web software to the Clearswift Web Appliance

Technical Bulletin

INTRODUCTION

The Clearswift Web Appliance shares the same powerful content engine as the MIMESweeper for Web software, but being an appliance is packaged a little differently. This technical bulletin examines some of those differences and highlights areas of the appliance that improve on the capabilities available with the web software so that these can be considered when planning for the migration.

For example, one obvious difference is that the appliance comes with hardware – but that is completely flexible – because ‘appliance’ in this instance includes ‘virtual appliance’ and you can install the ISO image on your own approved IBM, HP and Dell hardware or within a virtual VMware ESX environment.

MIMESweeper for Web software has been a great solution since it was first launched more than 10 years ago however, but today Clearswift Web Appliance offers an easier to manage and more complete solution with:

- Full integrated Anti-Virus, URL filtering, Anti-Spyware and Content filtering components
- Anti-Spyware includes ‘call-home’ protection with full infection reporting
- PCI & PII templates for accurate Credit Card and NI (UK) and SI (USA) number
- Improved security through the scanning of HTTPS traffic for malware AND data leakage
- Automated security protection updating and downloading of patches and upgrades
- Highly scalable and resilient with no single point of failure through peer appliance deployment
- Simpler to manage, easier to use web UI – saving both time and money
- Scheduled reporting – to reduce repetitive administration
- One screen System Health monitoring and, SNMP + e-mail system management alerting
- Comprehensive change control procedures with configuration roll-back of policy changes
- Comprehensive fully supported solution with all components from a single vendor
- Time-based policy for improved policy productivity controls (1.3 Feb 2009)
- Time-based reporting to monitor and police user activity and browsing trends (1.3 Feb 2009)

THE IMPORTANT DIFFERENCES

Web Policy Routes: The biggest difference between these two solutions is that the web appliance uses a ‘flat’ policy structure, like a traditional firewall, while the software uses a hierarchal policy structure.

This means that the appliance policy is much easier to use and understand (see figure 1) but very complex policies could be more time consuming to implement but with the advantage that once implemented the policy is far easier to modify via the graphical user interface plus you can print the policy for future reference.

Each route on the web appliance defines the source (user or user group) the destination (web site or categories of site) and the type of content allowed. Figure 1 shows that access to some categories of site are blocked for everyone, Gambling, Hacking, Hate etc. whereas access to other categories of

site such as 'Shopping' are allowed, but only at certain times of day as denoted by the clock symbol, and only if certain rules are not broken. In the case of the 'Shopping' route there are 6 content rules defined that prevent viruses, spyware, suspicious script and encrypted data from being downloaded and confidential office documents from being uploaded.

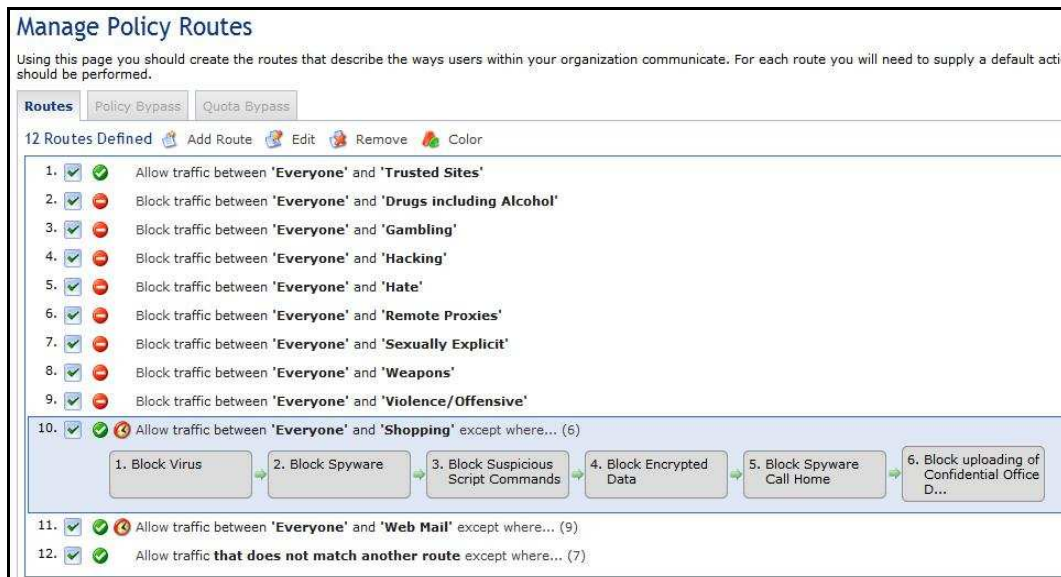


Figure 1 – Web policy routes and Content Rules

Authentication: Both products integrate with LDAP/AD for authentication and in addition to NTLM the web appliance supports Kerberos. Typically customers authenticate using NTLM or Kerberos because this method is transparent to the user and does not require them to enter a user name and password when accessing the Internet.

Policy: The web appliance is able to create policy rules based on the user authenticated or via the user's machine IP address. It is also possible to configure a hybrid policy using both authenticated users and IP addresses. This is in contrast to MIMESweeper for Web software which only supports Authenticated users or IP address.

Databases: There is no requirement for external SQL licenses – the web appliance comes with its own auditing database on board.

Management: The web appliance has more management features than the web software.

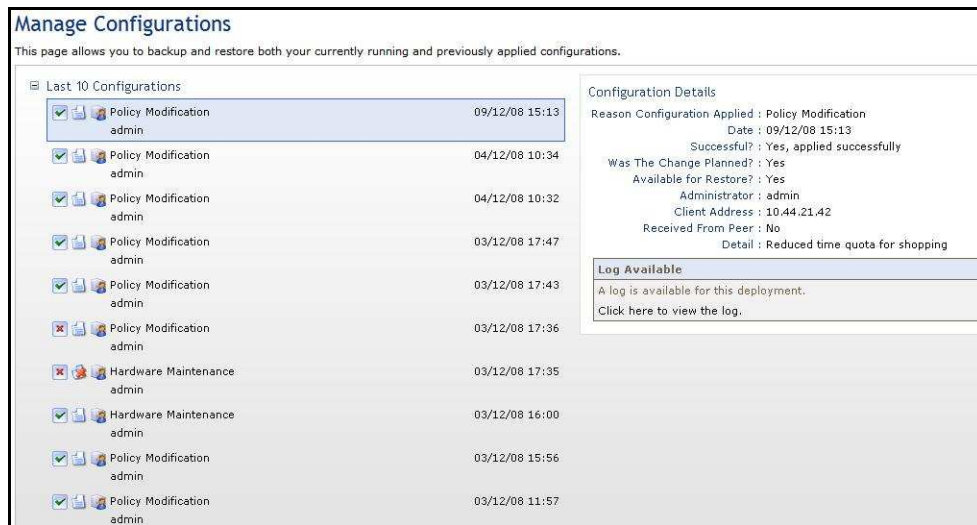


Figure 2: Managing configurations

For example, each policy change is logged against the administrator who applied the change (Figure 2). The last 30 changes are archived and available for re-use. Policy is optionally pushed to another eight web appliances at the same time, if needed. Policy changes are also applied at any time without disconnecting any users who are currently browsing.

A full suite of logs and alarms are available making it easy to install an appliance in a 'lights out' data centre. The appliance will let you know if there is any problem (figure 3).

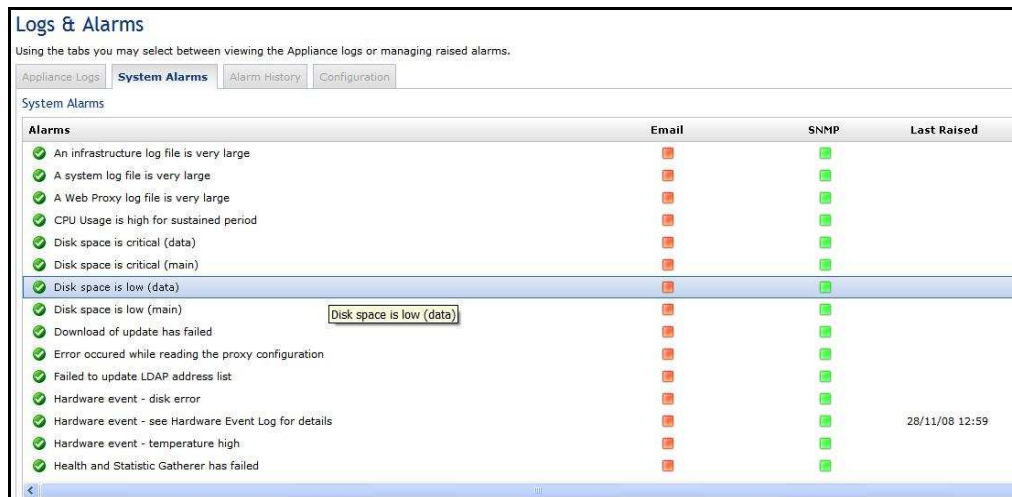


Figure 3: SNMP and e-mail alerting

The Clearswift Web Appliance also provides a System Health view (figure 4) which visually presents all the key information about web traffic throughput, threats, systems and service performance making it easy for an administrator to monitor the key parameters through a single screen view.

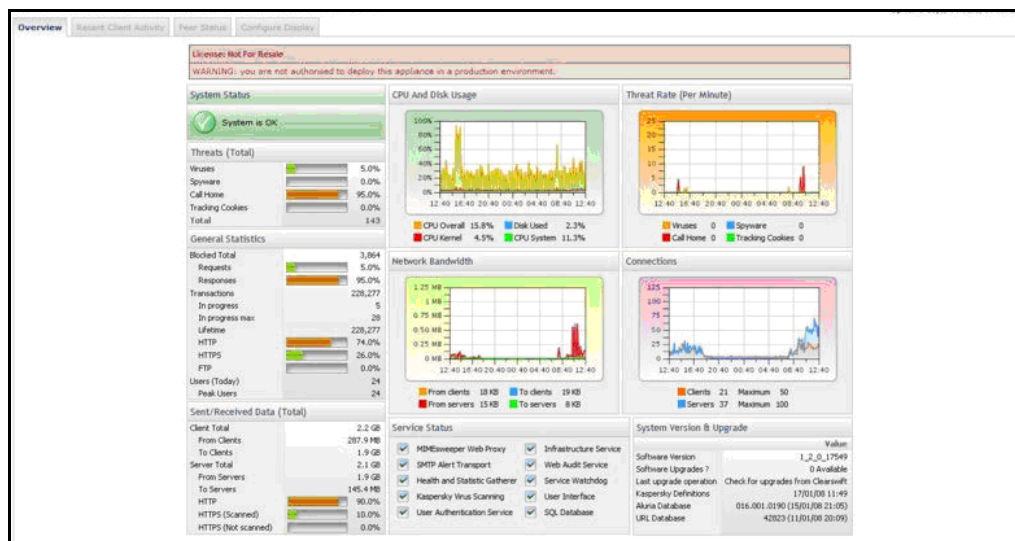


Figure 4: System Health

Integration of AV and URL Filter: The web appliance comes as standard with Kaspersky Anti-Virus on board. With our web software you need to purchase and install your own Anti-Virus product – which although allowing greater choice does mean an extra integration point to manage (ensuring engine versions are compatible etc.) and cost

The web appliance also includes Clearswift's premium URL filter, again built-in as standard and fully integrated, allowing for the policy to be defined based on the category of the site being accessed. This allows different levels of analysis to be performed based on the type of site e.g. extra scanning of data transferred to webmail sites to ensure uploaded documents are fully checked for confidential information and blocked if found.

Spyware: As Spyware is the most prevalent form of malware, the web appliance includes a dedicated anti-spyware engine CounterSpy™ from Sunbelt Software (in addition to the capabilities of Kaspersky to detect spyware). This engine ensures that spyware is not downloaded by your users. In addition, if the user takes a laptop out of the office and that laptop becomes infected with spyware when connected to an unprotected network, it will ensure that the spyware “call homes” are stopped and that you are notified of the machines/users infected through reports (figure 5) that can be set to run automatically throughout the day and delivered via e-mail.

The screenshot shows the MIMesweeper Web Appliance interface. The main heading is 'Machines Making Requests to Spyware Sites'. Below this, there are filters for 'Peers' (set to 'This Peer only') and 'Date Range' (set to 'This Year'). An 'Export to:' dropdown is set to 'PDF' with a 'Go' button. The main content is a table with the following data:

Last Requested	Machine	Domain Requested	Calls Made
04-Dec-2008 11:14:27	10.44.21.42	http://www.888.com	5
01-Dec-2008 15:04:39	10.44.21.42	http://s28.sitemeter.com	1
01-Dec-2008 14:58:32	10.44.21.42	http://s32.sitemeter.com	1
27-Nov-2008 17:18:41	10.44.21.42	http://www.alexa.com	3
25-Nov-2008 08:15:09	192.168.201.5	http://s28.sitemeter.com	1
20-Nov-2008 17:44:54	10.44.18.190	http://beacon.securestudies.com	2
19-Nov-2008 14:41:01	10.44.17.107	http://www.888.com	3
19-Nov-2008 12:31:09	10.44.22.210	http://www.888.com	20

At the bottom of the report, it states 'Time to execute report: 175 ms'.

Figure 5: Machines infected with spyware report

TECH FAQ

Reporting: The web appliance comes with a comprehensive set of default reports, which are easily customized with different filter parameters. All reports can be saved and scheduled for automatic delivery via e-mail where regular HR/Management reporting is required.

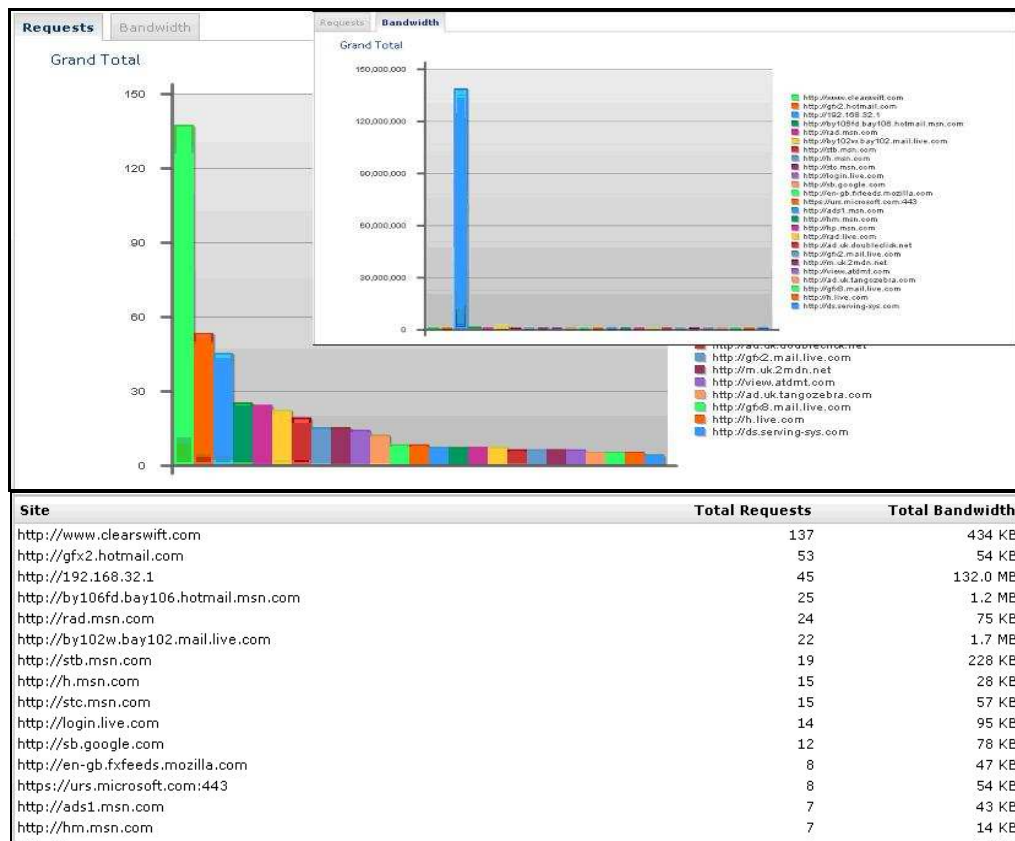


Figure 6: Web Appliance Reports

The MIMESweeper for Web software has a similar suite of reports but does not provide the automatic scheduling and delivery of reports.

The 1.3 Web appliance release (available in February 2009) will include time based reports that will highlight - the time a user spends browsing; the users that access the web for the most amount of time; and which types of site are the most popular and may be the biggest risk to employee productivity.

SSL/HTTPS Decryption: On average 10 to 20% of an organisation's web traffic will be encrypted HTTPS traffic. The web appliance provides full decryption and scanning of HTTPS traffic for malware and other content violations. This is available as a pre-integrated cost option on the web appliance. Clearswift do not offer HTTPS scanning for the MIMESweeper for Web software.

This HTTPS option ensures you are able to protect your users browsing experience (and audit it) even if the website they are browsing is encrypted. Many Web 2.0 services are encrypted now, including webmail accounts, so scanning HTTPS traffic is increasingly important.

With the Clearswift Web Appliance HTTPS option all traffic is decrypted although you are able to selectively disable for selected sites or routes, for example for Internet banking sessions so they are not decrypted. Even when it is fully operational a user's privacy is maintained through the privacy settings that are in place. Additional security is also provided by the certificate checks made by this module and the ability to set policy based upon the certificate information received by your users.

PCI & PII Detection Templates: The web appliance is able to detect credit card numbers. This discovery process is LUHN algorithm validated – so that only valid credit card numbers are detected and not just any string of 16 digits. You define whether your users are able to enter credit card details into non secure websites, or whether you apply weightings. So for example, exchanging one credit card number is allowed, but not two, five, ten etc. You are also able to ensure that your users aren't uploading credit card numbers to webmail accounts, even if these numbers are included in a MS Office doc or PDF. These features are essential in helping organizations comply with PCI standards.

For the USA and UK there are also PII (Personally Identifiable Information) templates that validate National Insurance numbers (UK) and Social Security numbers (USA). We aim to add more of these checks for other countries and regions.

Peer Appliances: If you deploy more than one Clearswift Web Appliance, for resilience or increased user scalability, then they are able to be peered together into a web appliance peer group. This means that any policy changes made on one web appliance are automatically and immediately pushed out and updated on all other peered web appliances. Up to 9 web appliances may co-exist in a single peer group and policy changes are all made without disconnecting users.

Common Policy Console: Additionally, up to 9 Clearswift Email Appliances are able to be peered into a web appliance peer group. Doing this automatically transforms the Policy Center of every peered e-mail and web appliance into a common policy console view, able to apply policy to both e-mail and web appliances from one place. This makes it very straightforward to administer both protocols and share common policy elements easily and consistently – for example a reference list containing internal confidential information is easily utilized by both types of appliances. Common rules may also be applied across both protocols– and for instance a Threat Report may be run across both protocols. As before all policy changes are automatically pushed to all peered web and e-mail appliances.

And, as the interface used in both appliances is almost identical – very little skills uplift is needed for an administrator to learn how to use a web or an e-mail appliance once they are familiar with one.

WEB APPLIANCE VERSION 1.3 (FEBRUARY 2009)

The next release of the web appliance will be available in February 2009 and the two main enhancements are (1) time-based reporting and (2) time-quota policy. Time based reporting was touched upon earlier and the following provides an overview of the new powerful time-quota policy controls.

Time Quota Policy Time quota policy provides organisations with the flexibility of allowing users the benefit of personal internet browsing (shopping, webmail, social networking, gaming etc.) whilst ensuring this benefit is not abused. This is achieved by monitoring the browsing activity of all users and keeping the 'non-business' related browsing within reasonable time limits, and within defined periods of the day i.e. 1 hour during a 2 hour lunch period.

Each web policy route is able to have its own unique time quota defined and shown below (Figure 7).

The green area defines when access to this route (Shopping Sites) is allowed with no time restrictions i.e. before 7am and after 6pm. In this example the intention would be to allow unlimited access to Shopping Sites outside the normal working hours for those that either arrive early, or stay late.

The orange area defines a period of time between 11am and 2pm where access to this route (Shopping Sites) is restricted to a maximum of 60 minutes browsing within a 4 hour period. For this example, users are can use their lunch hour quota at sometime within this four hour period.

Finally, on Saturday the office closes early at 5pm rather than 6pm. To account for this earlier finish time the unrestricted period defined by the green area starts an hour earlier and the lunch period

defined by the blue area only allows for 30 minutes of lunchtime browsing within the four hour lunch period.

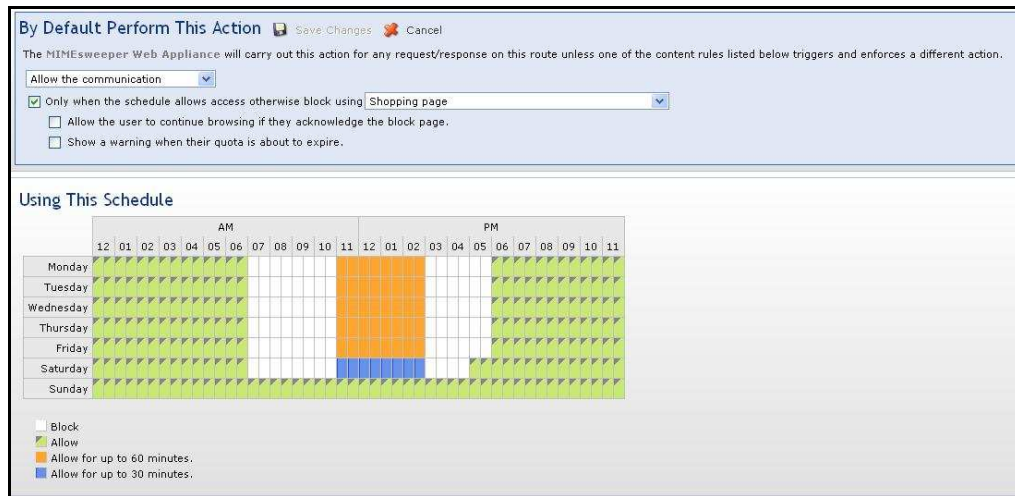


Figure 7– Web policy route schedule

In addition to the time policy controls shown above each route is able to have one or both of the following two options enabled (Figure 9).

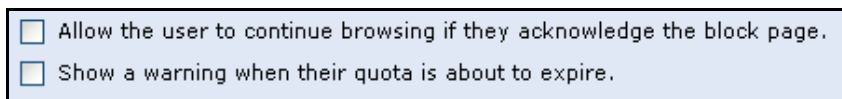


Figure 9 – Additional time quota options, override and expiry warning

The first of these will allow the employee to override the block page that is displayed when their time limit has been reached, but if they do override then it will be audited and the 2nd option will warn the user that their quota is about to expire within # minutes.

CONCLUSION

MIMESweeper for Web software was first launched more than 10 years ago in 1997 when the Internet was barely transactional and definitely not the essential collaborative medium it is today. The Clearswift Web Appliance is a complete solution for today’s Web 2.0 user interactions while offering a far easier to manage and lower total cost of ownership solution that includes:

- Full integrated Anti-Virus, URL filtering, Anti-Spyware and Content filtering components
- Anti-Spyware includes ‘call-home’ protection with full infection reporting
- PCI & PII templates for accurate Credit Card and NI (UK) and SI (USA) number
- Improved security through the scanning of HTTPS traffic for malware AND data leakage
- Automated security protection updating and downloading of patches and upgrades
- Highly scalable and resilient with no single point of failure through peer appliance deployment
- Simpler to manage, easier to use web UI – saving both time and money
- Scheduled reporting – to reduce repetitive administration
- One screen System Health monitoring and, SNMP + e-mail system management alerting
- Comprehensive change control procedures with configuration roll-back of policy changes
- Comprehensive fully supported solution with all components from a single vendor
- Time-based policy for improved policy productivity controls (1.3 Feb 2009)
- Time-based reporting to monitor and police user activity and browsing trends (1.3 Feb 2009)

- End -