



CLEARSWIFT

MIMEsweeper™

e-policy products for email and web

CS MIMEsweeper™ for Web 5.0

A powerful and comprehensive Web filtering solution that allows in-depth management and control of Internet access - not just URL blocking

The value of Web access to businesses is undeniable. From gathering news and information, to communicating with partners and customers, to streamlining business transactions, organizations aren't looking back when it comes to leveraging the medium. As a result, desktop access to the Web has become standard functionality across organizations, both large and small. But for IT managers and other decision makers, the business benefits are tempered by an array of threats to an organization's IT infrastructure, data, intellectual property, productivity and reputation.

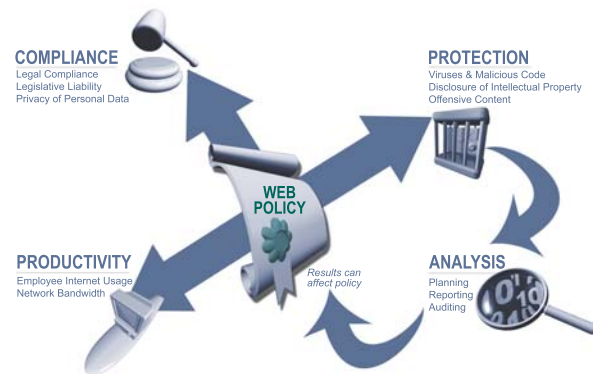
CS MIMEsweeper™ for Web is a content filtering solution that protects organizations from virtually every kind of Web-related threat, giving IT managers the ability to implement a comprehensive policy for Web transmissions and employee access - including an extensive set of security options not offered by URL blockers and anti-virus tools alone.

CS MIMEsweeper™ for Web is the most cost effective, feature-rich, scalable Web filtering product available, offering comprehensive protection to thousands of users.

Not just URL blocking

URL blocking is an important first step in protection against Web-related threats. However, today companies want much more than URL blocking. With new Web sites being created every day, no database of undesirable URLs is ever completely up to date.

A Web policy is not exclusively concerned with blocking access to the Web. It's about allowing access to appropriate sites, whilst ensuring that security is maintained during access and that the Web e-policy continues to be enforced. Organizations need to analyze the content of Web pages and decide, in real-time, whether or not to allow access based upon the content found. Just as organizations can filter email according to content as well as addressee, organizations can now filter Web traffic according to content and not just URL addresses.



Why choose CS MIMEsweeper™ for Web?

- Offers in-depth content filtering capabilities - not just URL blocking
- 300% increase in performance - up to 4GB cache
- 4 fold increase in scalability - up to 4 load-balanced servers in one array
- Based on the market leading content filtering technology, CS MIMEsweeper™
- Protects against loss of sensitive material through Web-based email systems e.g. Hotmail accounts and bulletin boards
- Filters undesirable file types
- Provides detailed usage reports & analysis with built-in graphical tools
- Enables organizations to define policies right down to the individual user level
- Blocks access to inappropriate Web sites based on their content, URL or URL category

Policy-based Web filtering

In addition to protecting themselves from these content security threats, organizations are coming under increasing pressure to ensure their networks are being used responsibly. Using corporate networks for non-business related pursuits can have a major impact on network performance, and is making organizations liable to major lawsuits. To avoid these risks, organizations need to establish Web usage policies, communicate them to their employees and use Web content filtering tools to enforce the policy.

CS MIMEsweeper™ for Web enables organizations to take control of the Web content flowing into and out of the enterprise - custom-fitting the policy to their own business environment and employee needs. For example, it may be acceptable (from a policy point of view) to use Web email accounts (such as Hotmail or Yahoo! Mail) during working hours, but unacceptable to send spreadsheets (e.g. price book, accounting information) or receive executable files using these accounts.

Why choose Clearswift?

Clearswift is the world's number one provider of software for managing and securing electronic communications. With a growing user-base of more than 14,000 customers, 16 million users around the world depend on Clearswift for protection and peace of mind.

NEW FEATURES

For this release of CS MIMESweeper™ for Web, Clearswift have primarily focused on improved performance, scalability and manageability. This in turn has reduced the total costs of deploying, scaling and administering the solution.

Increased Scalability

A four fold increase in scalability has been achieved with the ability to now run an array of up to 4 servers in a load-balanced configuration. This is achieved by using a routing protocol that shares requests between servers whilst ensuring that where a request has already been cached it is delivered from the right server's cache. CS MIMESweeper™ for Web makes it very easy for organizations to increase the total number of users, without having to rely on costly third party load-balancing software.

Increased Performance

Each Server in the array can serve approximately 2000 users enforcing a comprehensive Web policy consisting of AV, lexical analysis, file blocking, and URL filtering. This represents a 300% increase in performance per server over CS WEBSweeper 4.1. As might be expected, performance per server is dependant on the Web policy, thus with a less comprehensive Web policy of just URL blocking the performance would increase dramatically, albeit with reduced security.

Increased Cache Size

CS MIMESweeper™ for Web is a full caching security Web proxy server. For this release the cache has been increased in size from 500MB to 4GB, precluding the need for a 3rd party caching product, and improving network performance by delivering more responses directly from the cache.

Improved Manageability

The Web policy can now be managed across all servers in an array as if they were a single entity, making the overall management of a consistent Web policy far easier.

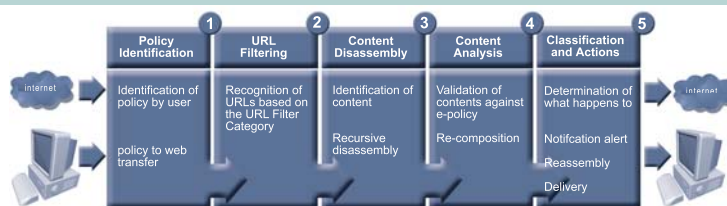
In addition, CS MIMESweeper™ for Web's management interface has many similarities with the CS MAILsweeper™ for SMTP interface. This overlap in the policy configuration and management aspects maximizes the potential for skills transfer, with minimal training, where both solutions have been deployed alongside each other.

Other New Functionality

- Support for French and German operating systems
- The URL database now provides both domain and page based categorization - i.e. www.bbc.co.uk/sports is categorized as sports, whereas www.bbc.co.uk/ is categorized as arts and entertainment
- SMTP email alerter
- Support for Symantec AV tool
- IP addresses in User Lists for policy selection
- Web-based reporting
- Support for client-to-Web server NTLM authentication
- Customizable proxy error pages
- Standard format transaction log
- Intelligent script analysis
- Configurable proxy timeouts
- Configurable list of HTTPS ports
- A configurable maximum download size
- Improved streaming media detection

FIVE STAGES OF WEB PAGE ANALYSIS

CS MIMESweeper™ for Web acts as a caching http proxy server, scanning Web traffic entering and leaving an organization for content security threats. It checks the user identity and the page being browsed and then applies the appropriate content security policy. If the URL has not been blocked by the URL Filter, CS MIMESweeper™ for Web disassembles the contents of the page or any downloads/uploads and validates this against the policy, before allowing it to pass, cleaning it of any threat or blocking it. You can choose to utilize the administrator notification facility to inform of the detection and potential breach against the e-policy.



STAGE 1: POLICY IDENTIFICATION

Recognition of policy rules as defined by user

- User authentication: when a user initiates a transmission, CS MIMESweeper™ for Web determines user Internet access privilege by looking at LDAP user list, NT user list or Text file user list (user defined), or even client IP addresses.
- Application of security operation: checks the individual Web usage policies in place, by looking at the policy scenarios set-up, including the time-of-day policies.
- Bi-directional policy application: allows or denies downloads and uploads (e.g. Web-based email) based on the usage policy.

STAGE 2: URL FILTERING

Recognition of URLs based on the URL Filter Category

- URL identification: compares the URL against the extensive URL database of more than 5.6 million URLs to determine if the URL has been included into one of the 40 pre-defined categories.
- Policy check: determines whether or not the user requesting this page is allowed access to that particular category of sites.
- Policy enforcement: if the user is not allowed access then the page is blocked and no more processing takes place. If the user is allowed access then the processing of the actual contents of the Web transfer continues from step 3 below.

STAGE 3: CONTENT DISASSEMBLY

Recursive disassembly of objects to identify original content

- Content identification: identifies the contents in HTTP and browser FTP traffic.
- Format recognition: recognizes and manages the key formats used in Web transfers.
 - Compression/encoding formats - TNEF, UUE, TAR, PGP, LZH, RPM, ARJ, (including self-extracting ARJ), GZIP, RAR, CMP, ZIP (multiple variants), BINHEX & CAB, MIME, HTTP & binary
 - Document formats: MS Office (CDA), RTF, HTML and PDF
 - Executable formats: Windows, DOS, Java byte
 - Image formats: JPEG, DXF, DWG, PSP, DNG, PIC, TIFF, PCX, FIL, BMP & GIF

- Sound formats: MIDI, AIF, VOL, AU, WAV and MP3
- Video formats: RM, MPEG, GM and AVI

- Content recognition: identifies the type of content by looking at the file architecture, rather than just the file extension.
- File blocking: stops files by name and can be used in association with wildcards.
- Pattern matching: enables file types to be specified by their binary sequence, giving administrators the flexibility to specify and block any file type.

STAGE 4: CONTENT ANALYSIS

Analysis of objects according to policy and data type

- Virus scanning: compatible with all leading virus scanners, and supports multiple concurrent virus scanners.
- Content cleaning: identifies and re-composes infected content.
- Access control: controls access to Web pages by PICS, URL and advanced text analysis of Web pages and files (e.g. for the control of pornographic or unsuitable Web pages).
- User Access: limits user access to certain Web pages according to specified times of the day.
- Content validation: validates content by file type, file name or file size.
- Detection of Java, JavaScript/VBscript and ActiveX
- Content control: controls cookies (i.e. ignore, remove or block), HTML automatic mailtos and hidden forms and cyberwoozles (data siphoning).

STAGE 5: CLASSIFICATION AND ACTIONS

- Classification and disposal of content: classifies and disposes of content according to Web usage policy in place.
- Allocation of actions: e.g. page blocked, file blocked, threat removed before page delivered, upload blocked.
- Notification to Users: CS MIMESweeper™ for Web features a configurable text message or HTML page informs users when a page is blocked.
- Notification to administrators and other appropriate parties: CS MIMESweeper™ for Web can be configured to send SNMP alerts, email alerts to administrators and other appropriate parties.

E-POLICY BASED CONTENT SECURITY

Web usage policies are applied based on a combination of user profile, URL being accessed and content of the page being viewed. For example, it may be an organization's policy that no-one other than the IT department has legitimate reasons for downloading executable files - which can only be downloaded from company approved sites - or that all users can access sports or news sites, but only outside of normal working hours. CS MIMESweeper™ for Web enables policies such as these to be easily implemented, putting organizations in control of Web usage in the workplace.

E-policy based content security is about establishing a written policy, educating all employees within the organization on what is or is not acceptable use of the Internet, and enforcing Web usage policies consistently and uniformly, using CS MIMESweeper™ for Web.

Improve business and network productivity by defining an e-policy and letting your employees know the boundaries of what is or is not acceptable use of the Web. Broadcast to your employees the fact that you are a responsible organization by providing feedback on the progress of large downloads and reasons for blocking a page. This feedback is provided to the user via HTML pages, and can be customized and refined by the system administrator to reflect the company's image and include details of deployed Web usage policy. If required, CS MIMESweeper™ for Web can also be configured to inform the administrator with an email alert.

CS MIMESweeper™ for Web URL Filter Category

The URL Filter Category is an optional plug-in that provides easy access to an extensive database of over 5.6 million URLs. The URLs have been organized into 40 clearly defined categories that contain more than 900 million Web page references, covering 65 languages.

An acceptable Web usage policy may be created by selecting the categories that are deemed inappropriate. The URL Filter is then used to restrict access to all the sites contained within the selected categories. Different categories may be applied to different groups or individuals within the organization, allowing granular filtering to be implemented as required.

The URL Filter Category is used to restrict access to all sites contained in the categories selected. The URL database provides both domain and page based categorization - i.e. www.bbc.co.uk/sports is categorized as sports, whereas www.bbc.co.uk/ is categorized as arts and entertainment.

Easy to implement, the URL Filter is the first step in filtering site access and applying the Web usage policy. CS MIMESweeper™ for Web provides additional in-depth content analysis and continued protection and is the obvious choice for companies wishing to control Internet access.

Automatic updates of the URL Filter database can be scheduled. These updates are obtained via the Internet on a daily basis, thus removing the necessity to update and maintain the URL database manually.

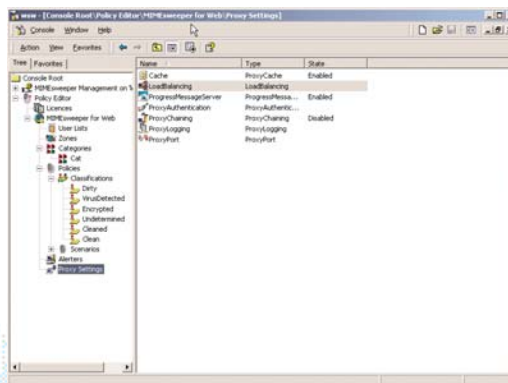
CS MIMESweeper™ for Web Policy Manager

CS MIMESweeper™ for Web enables organizations to implement, enforce and maintain a Web usage policy within a clearly defined framework. This means that different policies can be applied to different users within an organization.

The product provides an easy to use 'Policy Editor' user interface.

The benefits

- Implement rules through 'Policy Scenarios' - which can be a single or a range of security operations, such as detecting or blocking file types, advanced text analysis of document content, detecting or removing viruses etc
- Apply policy to each object passed through CS MIMESweeper™ for Web based on users and destination
- Dynamically update user lists from LDAP directories which ensure that the desired security policies are applied to users
- Define and apply organizational, departmental and user specific policies easily and consistently through a hierarchical structure
- Amend policies on lower organizational levels to meet the business needs for individuals or groups
- Generate reports on traffic, threats and CS MIMESweeper™ for Web operations, including URL blocking
- Comprehensive auditing and reporting functions with standard graphical reports provide detailed information, such as sites most visited and threats detected



TECHNICAL REQUIREMENTS

Hardware

- Pentium III 1000 MHz (dual processor recommended)
- 1024 Mb RAM
- 500Mb disc space (plus up to 4Gb for the cache)

Software

- Microsoft Windows 2000 (Server or Advanced Server) with Service Pack 3
- TCP/IP network protocol
- Internet Explorer 6.0 (SPI)

For reporting

- Windows 2000 Server with Service Pack 3
- SQL 2000 (or MSDSE 2000 as supplied on our CD) with Service Pack 3
- Microsoft IIS v.5

PROTECTION

With a security toolkit consisting of firewalls, anti-virus software and URL blocking alone, companies remain vulnerable to many threats. CS MIMESweeper™ for Web works in tandem with firewall and anti-virus solutions to provide a comprehensive security solution that guards against breaches of confidentiality and other threats, such as damage to reputation, lost productivity, pornography, theft of data, legal liability, degradation in service and data corruption.

Loss of Confidential Information

- Theft of Data
- Unintentional or intentional circulation of confidential information outside the organization (i.e. Web mail such as Hotmail or Yahoo! mail)

Legal Exposure

- Copyright infringements
- Damage to reputation
- Legal liability brought on by misuse of the Web

Threats

- Loss or corruption of data
- Virus infiltration
- Malicious code
- Denial of service (DOS) attack
- Unpack attacks
- Network degradation and downtime
- Data siphoning and corruption by stripping

COMPLIANCE

CS MIMESweeper™ for Web provides bi-directional content analysis of uploads and downloads. For most organizations, the information leaving the organization is of critical importance, especially where confidentiality must be maintained for regulatory or legal reasons. An organization's email policy provides part of the solution, but Web mail must also be included in the organization's overall e-policy to provide complete protection and compliance.

PRODUCTIVITY

CS MIMESweeper™ for Web helps address productivity issues by ensuring browsing activity within company time is business related, rather than of a personal nature. There is no doubt that the Internet is a vast and important resource for gathering competitive and business related information. However, with unrestricted access to the Web, it is all too easy for employees to be inadvertently distracted from their business focus (e.g. shopping, finance, chat, personal Web email, hobby and general interest sites etc.). CS MIMESweeper™ for Web includes functionality to address these productivity issues by providing multiple methods for recognizing the type of site (i.e. Games, Sports, Travel etc.) being accessed. This can then be used to enforce the Web usage policy according to the sites' applicability to an individual's business activity. Sites that are not business related can be blocked, or restricted access may be granted based on the time of day.



- Blocks access to inappropriate sites based on their content, purpose or URL
- Manages undesirable file types, such as MP3s, AVIs, MPEGs and executables
- Prevents or restricts information sent or received via Web mail
- Audits and reports on individual or group Web traffic and warns the offenders
- Blocks oversized files that cause degradation in network service
- Reports, monitors and sends alerts on Web usage activity

ANALYSIS

CS MIMESweeper™ for Web allows organizations to understand networks and user behaviors, as it relates to compliance, protection and productivity.



Utilize CS MIMESweeper™ for Web's powerful reporting tools to map trends, make informed decisions and smart investments:

- Detailed and informative graphical reporting
- Capacity planning for improved efficiency and cost reduction
- Real time statistics on current Web users
- Comprehensive auditing and reporting to identify inappropriate activity



CLEARSWIFT™

Managing and securing
electronic communications

EUROPE

United Kingdom
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire, RG7 4SA
UNITED KINGDOM
Tel: +44 (0) 11 8903 8903
Fax: +44 (0) 11 8903 9000

Germany
Amsinckstrasse 67
20097 Hamburg
GERMANY
Tel: +49 40 23 999 0
Fax: +49 40 23 999 100

France
54-56 Avenue Hoche
75008, Paris
FRANCE
Tel: +33 1 56 60 58 00
Fax: +33 1 56 60 56 00

AMERICA

US West Coast
15500 SE 30th Place
Suite 200
Bellevue
Washington, 98007
UNITED STATES
Tel: +1 425 460 6000
Fax: +1 425 460 6185

US East Coast
1050 Winter Street
Suite 1000
Waltham
Massachusetts, 02451
UNITED STATES
Tel: +1 781 839 7321
Fax: +1 781 522 7488

ASIA PACIFIC/JAPAN

Australia
Ground Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA
Tel: +61 2 9424 1200
Fax: +61 2 9424 1201

Japan
Eisho Takanawadai Bldg 6F
2-11-8,
Minato-ku Shiroganedai
Tokyo-to, 108-0071
JAPAN
Tel: +81 (3) 5423 8171
Fax: +81 (3) 5423 1274

www.clearswift.com