Content Security

By Govind Rammurthy – MD and CEO – MicroWorld Technologies Inc.

Content Security refers to monitoring Internet access and e-mail activity in your network. This white paper provides information about Content Security, its need and recommends features that good Content Security software should have.

Contents

What is Content Security

Content Security broadly involves setting Security Policies that govern Internet use in your home or organization. You, as the system administrator or parent, set guidelines for productive and safe use of the Internet. This also involves control over e-mails and attachments sent or received by your employees or child.

Need for Content Security

The Internet access you have provided in the office costs money. You wish to see it used as a productive tool and increase business. It also provides the best way to appear busy. Employees can open multiple pages, a few of them related to legitimate work, while the others cater to their 'personal' interests. It takes a single mouse click or Alt+Tab to navigate between pages, when a supervisor appears.

This section provides details of how Internet access can be abused.

Statistics of Internet abuse

Consider the following facts:

- **33%** employees surf with no specific objective; men are twice as likely to do this as women. (www.emarketer.com)
- **70%** Internet porn hits occur between the hours of 9am and 5pm, during office hours. (Businessweek.com)
- 30% to **40%** of employees' Internet activity is not business related and costs employers millions of dollars in lost productivity. (IDC research)
- Men are **20 times** more likely to view and download pornography. (www.emarketer.com)
- **1 in 5** men and 1 in 8 women admitted to using their work computers as the primary lifeline to access sexually explicit materials online. (MSNBC).

Estimating net abuse costs

The following equations allows you to estimate how much misuse of Internet costs you:

Number of employees with Web access:	= A
Average hourly cost per employee including overheads	= B ($)
Average time spent in non business net use/day	= C (Hours)
Average time spent on personal e-mail+ Chat/day	= D (Hours)
Working hours/day	= 8

Cost to your organization for non business activity (E) = {B * 8/C * D} * A

In the above example: If A= 50; B = $ 40; C and D = 2 Hours,

Then, non-business net costs/day = $ 4000.

Assuming average worked days for an employee as 240,

Annual non-business surfing costs = $ 960,000

If your company cannot take this drain, then read on.

Impact of net misuse

Impact of net misuse can occur in the following ways:

Productivity Loss: Time lost when employees use the net to peruse personal e-mails, search for jobs, access porn sites, use the IRC chat for personal chat. They are indulging in unofficial activities for which you pay.

Bandwidth Loss: Downloads of images, music, movie files, etc. consume massive bandwidth. This only slows down legitimate net use. You pay for the bandwidth.

Security: Net access is double sided. When you open a website, it also has access to your PC. If your network does not have the requisite security, then it falls a prey to virus, Trojans, hacking, theft of confidential data, etc. Your employees can send confidential information, willfully or otherwise.

Adverse PR: There have been numerous news reports of employees being fired for accessing inappropriate material. The offenders may have paid for their crime but your company will carry a stigma and the news gives rise to speculations about how much of such activity remains unearthed.

Moral Degradation: Constant exposure to obscenity, hate, violence, etc. from the Internet, can morally corrupt good personnel. After all, nothing can beat Sex.

Numbers Game: If a handful of your employees are caught with porn, you can do something. What if 80 % of the male staff indulges in this habit? Do you fire everyone? You may even find your crack programmer (whom you have lured in with a high salary) and the project leader, prone to watch porn. Moreover, if they take it up as a challenge, they may even crack your security systems.

Copyright infringement: Can happen willfully or unintentionally. An employee downloads and uses a software program, a graphic image or a proprietary document thinking that, because it's on the Web, it is free. Copyrights extend to the web media also.

Legal: When your employees visit porn sites, access sexually explicit material, post hate mails, they are committing an offense. Your company is liable for legal action. Employees using the Internet must remember that:

- If an employee downloads objectionable materials and shows it to another employee (maybe a female colleague), your company could be liable for sexual harassment damages.
- IT managers face prosecution if their corporate networks are used to carry illegal material from the Internet. The law for online transport of information is the same as offline. (Computer Weekly)

- E-mails are acceptable as evidence in courts. So if an employee sends e-mail, with good intentions, claiming to offer services or products, which your organization cannot provide, your company can be liable for breach of promise lawsuits.

There are many other legal issues and enumerating all of them are not in the scope of this white paper.

For more information visit http://www.info-law.com/guide.html

Recommended Features of Content Security Software

The Content Security software should broadly address the following issues:

- Control access to websites
- Control e-mail activity
- Control remote file modification
- Block Spammer's e-mail ID and issue warnings and notifications

If your organization is large, then you need to assign **uniform global security policies** that govern all machines in your network.

Recommended features of good Content Security software are given below:

Control access to Websites

The software should allow you to selectively block and allow websites on your network. The following issues need to be addressed:

1) Restricted words: Software should allow you to specify restricted words and phrases like: porn, xxx, etc. and add them to the restricted words list. Access to any URL or page, that has these words, should automatically be blocked.

The software should also be intelligent enough, not to block or flag educational or medical sites. Many Content Security software's, currently available in the market, have this crippling problem.

2) List of banned sites: Software should allow you to add URLs of banned sites. Access to these sites is immediately blocked. Some notorious sites like www.hustler.com, www.playboy.com, etc. do not change their names. Such known sites need to be blocked outright.

3) Banned IP: Websites can be accessed by entering the IP (Internet Protocol) number. The software should be able to translate the IP number to its website name and block access if it contains restricted words or is on the banned list.

For e.g. www.sex-circus.com can be accessed through its IP, http://198.63.10.71 when you use other Content Security software. Software's like eScan are intelligent enough to translate the IP to its URL and block it.

4) Filter Category: The software should allow you to create category of filters for block and allow site. Sites related to the category can be listed there. For e.g. Pornography Category will have sites related to porn and all sites for this category are blocked. It should be possible to add or remove sites from block and allow category with a mouse click.

5) Log Files: The software should auto create a log of sites visited, blocked sites and reason why it was blocked.

Figure 1, shows a screen shot of eScan, the top selling Anti-Virus and Content Security software that has this feature of adding restricted words.

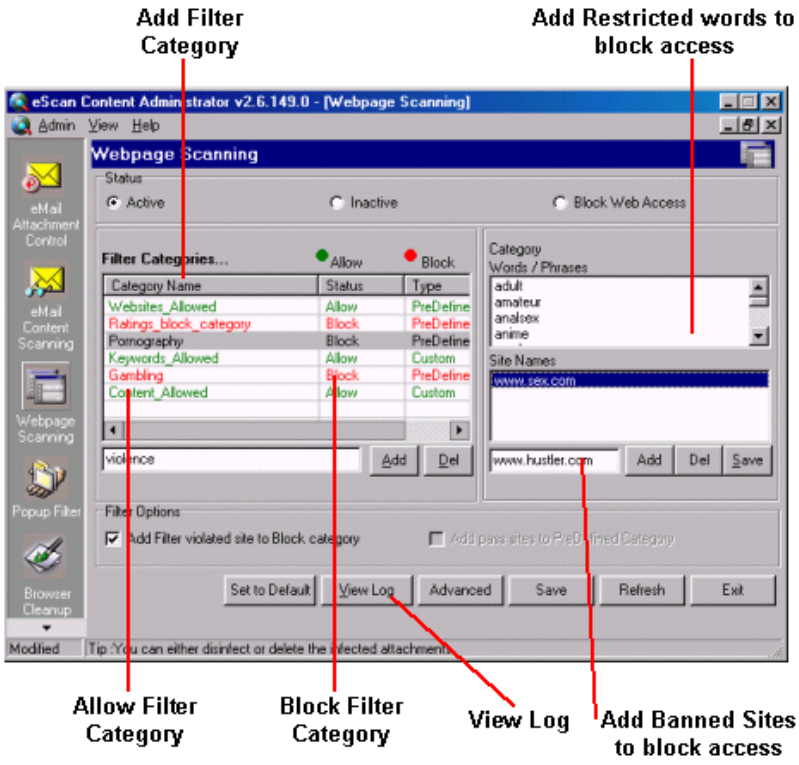


Figure 1 Block access to banned sites

ADVANCED CONTENT MATCHING OPTIONS

The software should allow you to set advanced content matching options that search for restricted words in different parts of the web page, set number of times a restricted word occurs in a page before it is blocked, allow you to block page elements like images, applications, movie files, etc.

1) Content Matching: After a list of restricted words is made, the software should automatically, search for such words in the accessed site. But content matching feature should be intelligent enough to differentiate between a porn site and a medical site that gives anatomical reference of a human body.

Words occurring in the following areas of the web page should be detected and denied access to:

- Site Name
- HTML Tags
- Page Title
- Page text or body
- Page description and keywords

2) Threshold Level setting bar: Restricted words like babe, sex, etc. can be found in legitimate sites. In Figure 1, you created a list of restricted words. In a website, if any three words from the list appear as a combination, more times than set as the threshold value, the site is blocked. The Threshold level bar allows you set the threshold value number.

Figure 2, shows a screen shot of eScan, the top selling Anti-Virus and Content Security software that has features of Advanced Control.

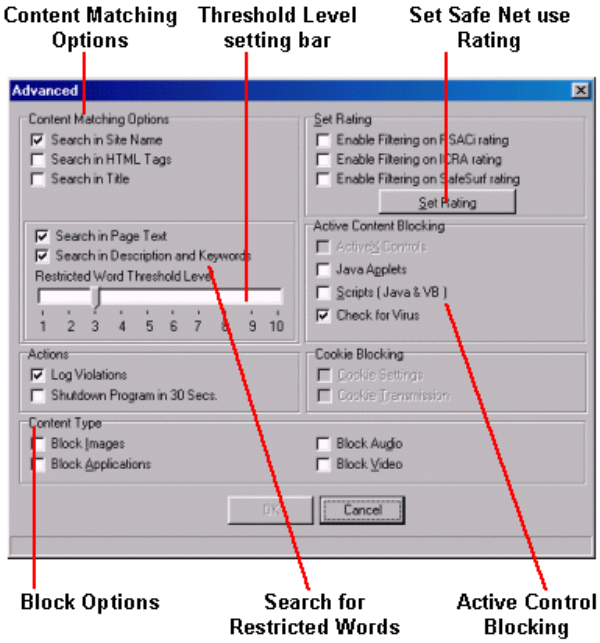


Figure 2 Content Control Options

3) Block Options: The software should allow you to choose options for blocking a website as given below:

- **Block Images**: Images on web pages are not displayed.
- **Block Applications**: Block applications like .exe files that can be run on your machine.
- **Block Audio**: Audio or sound files on websites are not played.
- **Block Video**: Movies on web sites are not allowed to run.

4) Active Control Blocking: Some web sites embed objects like Applets and Scripts, in your browser when you access their WebPages. The software should allow you to bar this action.

5) Safe Net Use Rating: For safe net surfing, organizations like RSCAi, ICRA, SafeSurf, etc., rate sites based on the language, Nudity, Sex and Violence. Your employees should access only sites rated as per your requirements, by these organizations.

The software should allow you to choose a rating agency and further fine tune access options for Language, Nudity, Sex and Violence.

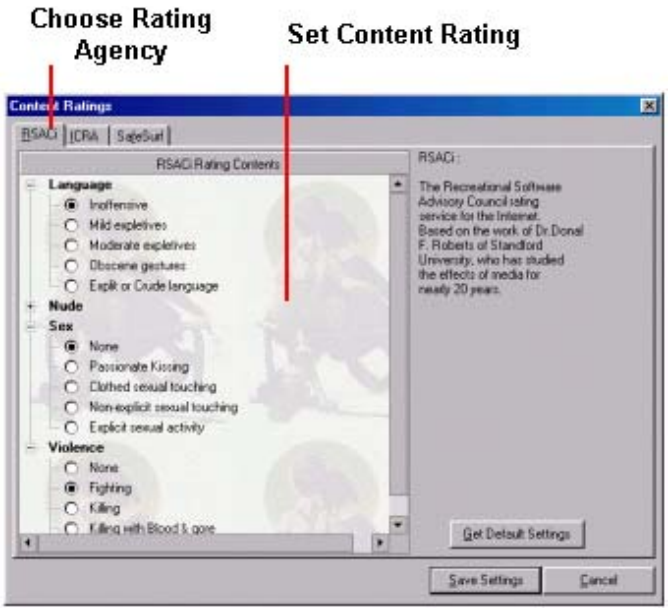


Figure 3 Set Content Rating

Good Content Security software should be effective against Spam. Refer to the **white paper on Spam** for more details.

Control e-mail

E-mails have become one of the prime sources for Internet Abuse. Offensive mails can be sent and received from your network. This section of the white paper addresses various issues regarding e-mail abuse like Spam and Attachments.

RESTRICTED PHRASE CHECKING FOR SPAM MAILS

Spam mails are unsolicited junk mail. These have an enticing subject line like: deal of a lifetime; free your debts, etc. The words may occur in the body, header, and HTML tags of the e-mail.

- The software should have a **block list** of such words and phrases. Any mail with the words as the subject, should be automatically deleted or quarantined.
- You should be able to add or delete words and phrases to the block list.
- The software should detect such phrases in e-mail body and HTML tags.
- The software should allow you to enable or disable this feature.

Figure 4 shows a screen with Restricted Phrase Checking feature, from eScan, the top selling Anti-Virus and Content Security software.

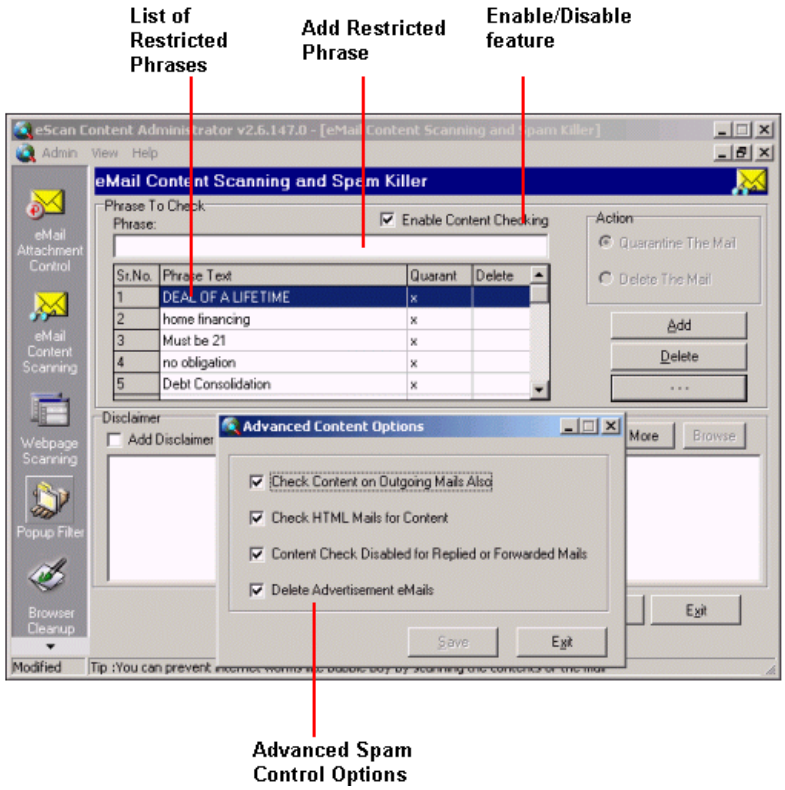


Figure 4 Restricted Phrase Checking

BLOCK SPAMMER

Another way to beat a Spam is to refuse entry to e-mail IDs that are known Spammers. Software with the following features effectively combats Spam.

- Add e-mail ID of known Spammer to the **block list**. Any mails received from an ID, included in the list are automatically deleted, without being downloaded into your server.
- If required, the software should remove an e-mail ID from the block list and allow mails from it.
- Software should allow a notification to be sent to the intended recipient and system administrator. The notification should provide details of: who the mail came from and who it is for, subject, reason why the mail was deleted, etc.

Figure 5 shows a screen with Block Spammer ID, from eScan, the top selling Anti-Virus and Content Security software.

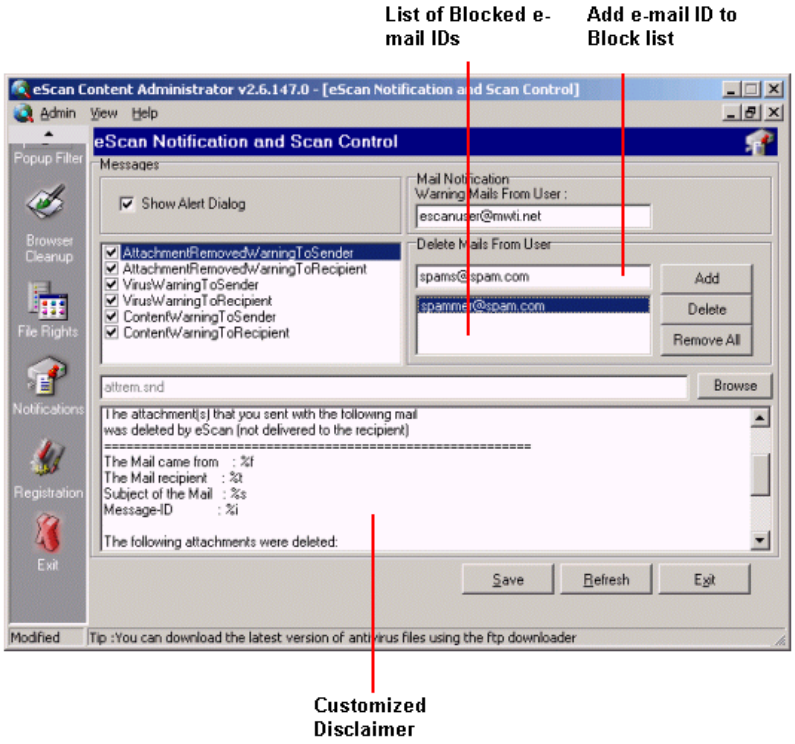


Figure 5 Add e-mail ID to Block List

E-MAIL ATTACHMENT CONTROL

E-mails are an invaluable tool to send and receive information. But they provide a very easy way to send out company confidential information in the form of attachments. While e-mail themselves can carry only information, e-mail attachments are the real sources to leak valuable company information. The following features need to be present:

Block Attachment: The software should allow system administrators to block specific attachments types of specific types (for e.g. .doc, .exe, etc.) from being sent or received. This puts an end to important documents like source codes, sales figures, annual accounts, etc. from being e-mailed.

Auto Compress Attachments Software should automatically compress, outgoing and incoming attachments. This saves valuable bandwidth. There also has to be an option that allows you to exempt specific attachment types from auto compression.

Options for Attachments Auto Compress: Advanced options for auto compress should allow you to:

- Select **minimum size** of attachments, above which it should be auto compressed.
- Select minimum **compression %** below which attachments should not be compressed

- Select the compression **level** that best suits your need: Best Speed and Best Compression.

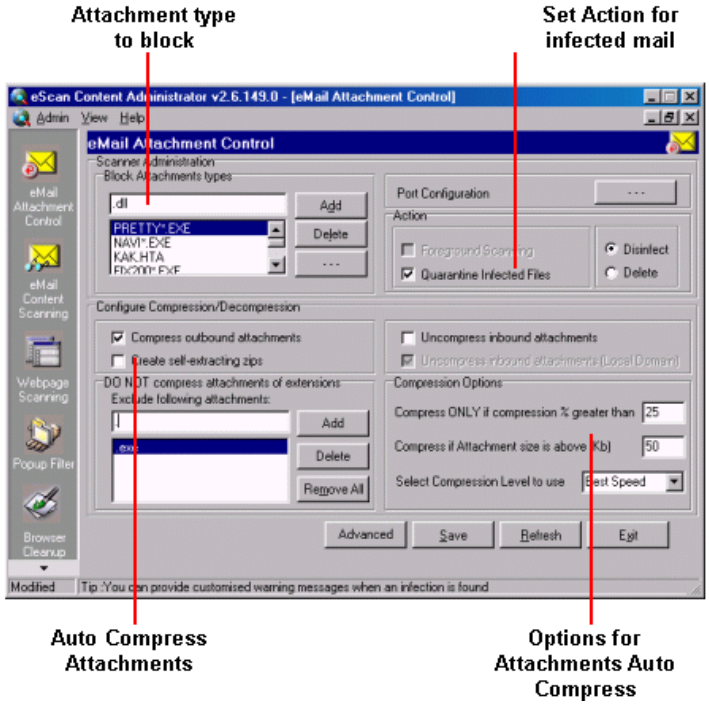


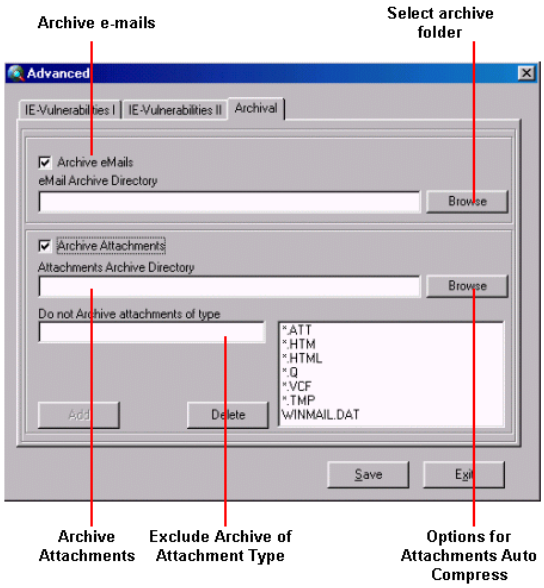
Figure 6 Attachment Auto Block

Figure 6 shows a screen with features to block and auto compress attachments, from eScan, the top selling Anti-Virus and Content Security software.

ARCHIVE E-MAILS

Software should allow system administrators to save into an archive folder, e-mails and attachments, sent or received by users in the network. The saved e-mails can then be browsed to see if the contents violate your security policy. At the same time, you should be able to exclude specific attachment types from being archived.

Figure 7 shows a screen with e-mail archiving features, from eScan, the top selling Anti-Virus and Content Security software.



Control Remote File Modification

The network has important files that should not be modified by other users in the network. Certain types of viruses like FunLove, Kleiz, etc. spread by modifying or creating specific file types like .exe, etc. The software should allow system administrators to specify file types that cannot be modified or created by remote users.

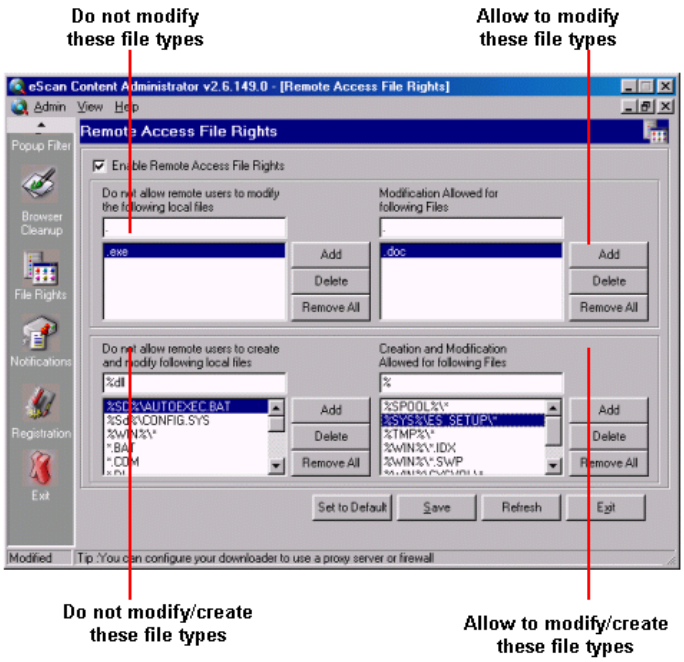


Figure 8 Assign Remote File Rights

Figure 8 shows a screen with features to assign remote file rights, from eScan, the top selling Anti-Virus and Content Security software.

Important Note

Remember the following -

- Your **personnel** are the most valuable **assets**.
- Your main goal is to ensure that your **business thrives**.
- You main goal must be to ensure that offenses are **not** committed and not to carry out a witch-hunt to purge your organization of offenders and make an example of them.

At the beginning, **notify** all the employees that you are setting up a security system and that all Internet traffic from individual machines and individual e-mails are under surveillance. This radically brings down the probable offenses by a huge percentage.

After all, when you see a traffic cop, you try to observe all the traffic rules, instinctively and instantaneously.

Further Reading

The following white papers provide information about related topics:

White paper on **Spam**, White on **Parental Control**

About the Author

Govind Rammurthy is a hard core 'techie' with keen business acumen. He founded MicroWorld Technologies Inc. in 1995 and has been in the forefront of the fight against Viruses and other threats. He leads the team of programmers and QA who have developed world-class product suites: **eScan** and **MailScan**. These products offer the greatest control in the areas of Anti-Virus and Content-Security.

To find out how MicroWorld can help you, visit http://www.mwti.net/