Global Information Assurance Certification Paper

What about Content Scanners?

Kenneth F. Kobylanski

December 2001

Table of Contents

This document will detail the issues involved regarding content access, acceptable network use and the importance of having a well-defined security policy. This paper will also demonstrate how integral content scanners can be to safeguarding networks and enterprise integrity.

I. What are the issues?

A. Why would you use content scanners?

Email and the Internet have brought a host of new threats and issues to network and business security. These threats and issues may and usually do include:

- Vulnerability to virus infection and malicious code
- Transmission of confidential information
- Legal liability exposure through defamation and offensive or pornographic material
- Spam, relay attempts and denial of service attacks
- Loss of privacy through unsecured email
- Reduced network speed through non-business bandwidth utilization
- Lost productivity from personal use of email and the web

B. Confidentiality Breaches

Accidental or deliberate, confidentiality breaches are an increasing threat to organizations and can have a devastating effect on customer and market confidence. Replying to all recipients of a message without checking the list for non-company employees may lead to an unintentional leak of confidential information. On the other hand, the premeditated distribution of a customer database may be a calculated act of sabotage.

A 1999 CSI/FBI Computer Crime and Security Survey found that 90% of respondents detected computer security breaches within the last year, with 26% of these reported as theft of proprietary information. 74% acknowledged financial losses due to security breaches, with 42% able to quantify their losses totaling over $265m.

In a PC Week Survey in 1999, up to 31% of respondents admitted to intentionally or accidentally sending confidential information outside the organization[1].

C. Damage to Reputation

Actions by disgruntled employees, information sent unintentionally, legal cases brought about by employees, or spam and spoof attacks can all lead to adverse publicity for an organization.

The long-term consequence of any threat like this is the overall damage to the reputation of the organization. The resulting negative publicity could damage company reputation, reduce consumer confidence and even cause share prices to collapse.

With a comprehensive content security solution in place, an organization is better able to protect itself against these threats.

In December 2000, Norton Rose, a prominent and distinguished law firm, had their reputation tarnished as the originator of the "Claire Swire" e-mail, a sexually explicit e-mail that circulated to over 10 million people around the globe.

In January 1999, Michael R. Overly, a disgruntled customer sent spoofed e-mails to employees at Samsung Electronics, USA, accusing them of hacking and other crimes. The e-mails appeared as though Samsung's attorney had sent them, causing employees to panic[2].

D. Legal liability

With the growth of Internet usage, the issue of legal liability manifested itself first in the USA, and subsequently across the rest of the world. Cases involving e-mail misuse and sexual or racial harassment via e-mail have resulted in legal liability lawsuits with multi-million dollar penalties.

Traditionally, employers have been responsible and liable for the actions of their employees in the workplace. However, if an organization can demonstrate a 'duty of care' to reduce unacceptable employee activity, then it could minimize its potential for liability.

January 2000, Human Rights (USA) / Computer Weekly
Nissan Motor Company. Two employees at Nissan who were fired for sending sexually explicit e-mail messages subsequently sued for unfair dismissal, claiming violation of privacy. However, Nissan won the lawsuit because it had an e-mail policy in place that prohibited the use of company owned computer systems for non-company business.

January 1999, Human Rights (USA)
Distribution firm BG paid out a $161,000 libel settlement to rival Transco, after a BG senior manager sent a defamatory e-mail to Transco staff, wrongly suggesting that Exoteric Gas Solutions (created by BG) had misused confidential information from Transco[3].

E. Lost Productivity

It is all too easy for employees to utilize e-mail and the Web during work hours, for non-work related activities. In a recent study by the American Management Association, 64% of employees have access to e-mail and 48% to the web.

In March 1999, the CSI/FBI Computer Crime and Security Survey reported that 97% of responding organizations had experienced employee abuse of the Internet, with IDC, estimating that the cost in lost productivity incurred by an employer with 1,000 employees could be as much as $96,000 per year.

According to eMarketer.com, 32.6% of workers have no specific objective when they surf the Internet[4].

F. Degradation in Service

This can take many forms, but the typical cause is a Spam attack - unsolicited or junk e-mail. It takes up valuable bandwidth and server space and wastes e-mail recipient's time. Excessive spam attacks can lead to a Denial of Service, where the server crashes due to the volume, size and intensity of the messages being sent.

According to a Gartner Group study of 13,000 e-mail users, 90 percent receive spam at least once a week, and almost 50 percent get spammed six or more times per week, whether at work or at home.

Degradation in service can also be caused by users sending and receiving e-mails with large attachments, or by downloading large files from the web, such as MP3 music files or photographs. According to the Ferris Messaging Survey in December 1999, messages are usually between 40KB and 100KB but are set to double. Also messaging bandwidth requirements are expected to be three to five times higher than that of today.

Based on a statistic by Marshal Software, a single employee earning 37,440 dollars per year and spending just six minutes per day on personal email will cost an organization $468 in lost productivity. If the company had 5000 employees, the total bill would be $2,340,000. If an employee earning 50,000 dollars per year surfs the web for one hour per day, it will cost his/her employer 6.5k per year[5].

The following statistics relate to the above list of security threats often incurred at any one site, based on a survey done by research firm NFO:

- 50 percent of employees frequently surf the World Wide Web for personal reasons at work.
- One in eight men and one in nine woman surf to sites with sexual content from the office[6].

As you can see, email and web surfing can cost a significant sum of money for a short amount of time that is spent per day. I am sure that these numbers are not as realistic as an employer might want to believe of actual time spent on non-business related emailing and web surfing.

II. Solving the Issues

A. Security Policy

Implementation of a security policy is based upon policies, standards, guidelines and procedures. They are the details which state what practices will be allowed on an organization's network resources. A security policy is most often written and updated by information assurance individuals and managers. These policies are often the legal liability that all rules are followed and acceptable practices on a network are complied with. The user acknowledging they will comply usually signs these policies. The common practice is to have each user re-comply with the security policy yearly. These policies are enforced by use of tools such as content scanners. Based on the rules and policies in an organization, content scanners will be chosen for their functionality and configured accordingly.

B. Content security A Definition

Content Security allows organizations to analyze, protect and manage the content in e-mail and web communications over the Internet and Intranets. Managing the flow into, out of, and around the organizations, content security helps protect network and business integrity[7].

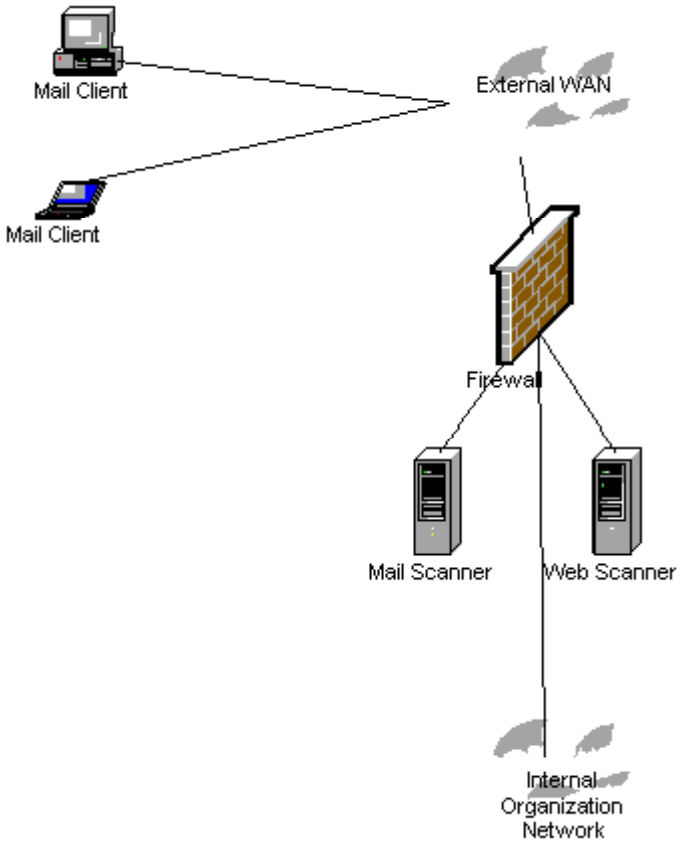

Figure 1 Content scanner placement within a networks DMZ

C. Functionality

The functionality of a content scanner is to monitor inbound and outbound traffic for content that is prohibited by a security policy or damaging to network resources.

Mail content scanners can be configured to monitor and scan all mail messages. They are scanned for the following: malicious code, enforce file size limitations, prohibited words or phrases, recipients, dangerous file types, viruses, and Spam[8]. All of these elements are important aspects of mail content security as stated by the above examples.

Malicious code is active code, often set inside a trusted program that has the intent to infect or damage data and/or network resources. Some content scanners combat malicious code by using what is referred to as a sand-boxing technique. This technique allows the code in question to execute in a contained environment while all function and system calls are monitored for suspicious behavior. If malicious activity is detected, the scanner can be configured to send the program to a quarantine server, delete the program, or if possible remove any offending code. The most commonly preferred action for this scenario would be to quarantine the code for further analysis and identification.

Content scanners examine header information for some of its scanning. Recipients are reviewed and if there is a policy defining that mail is not to be sent or received from an individual or an entire domain, content scanners can be configured to deny delivery and potentially further process the offending mail.

File size limitations are based on attachments in a mail message. The attachment information is contained in the header and therefore can be configured to limit the size of mail messages as to not deplete network resources. Some content scanners can also scan the actual attachment for its size, thus checking for any inconsistencies between declared and actual size of the mail message.

Prohibited words and phrases can be entered into multiple dictionaries. Each of these dictionaries can have different actions associated with them. These words can be by themselves or part of larger words. Scanners look at and into the headers, body and any attachments for this content.

The reviewing of file types is an important aspect to the security of mail and web security. Scanners have the ability to look at the file characteristics to determine actual file type. This is an important aspect of scanning because replacing the file extension or adding multiple extensions has become a common way to hide malicious files. Identification by file characteristics will also identify any unknown file types or extensions that could lead to new previously undefined threats. Experience has shown that without checking the characteristics of an attachment you are not efficiently or effectively scanning for threats. Not all content scanners block by characteristics. In one such case, executable attachments were identified by the application / octet-stream mime type. This was not only a weak and insecure technique for type identification, but it also misidentified other file types that were generically identified by their sending clients as application/ octet-stream.

Scanning for viruses is not a primary function of

content scanners. However, they can be configured to work in conjunction with anti-virus software. Many times viruses are caught during the malicious code scanning.

Spam is an email denial of service attack that consists of flooding an email server to a point that it can no longer handle the traffic and shuts itself down. This attack is useful in getting malicious messages thru a server without notice. Content scanners can be configured to allow a maximum number of mail messages to be sent in a specific amount of time. This function eliminates the threat of spam email.

Mail scanners can be configured to do various actions with a message that has violated site policy. Depending on the type of violation, a message can have multiple actions taken. These include being quarantined locally for administrative reviews, sent to a dedicated quarantine server, have any offending attachments stripped off before delivery, or flatly dropped from the network. Additionally, all messages generate a log trail reflecting their violation or delivery status. This can help administrators locate problem areas. With mail content scanning included in a network, confidentiality breaches, damage to reputation, legal liability, lost productivity and degradation may be avoided.

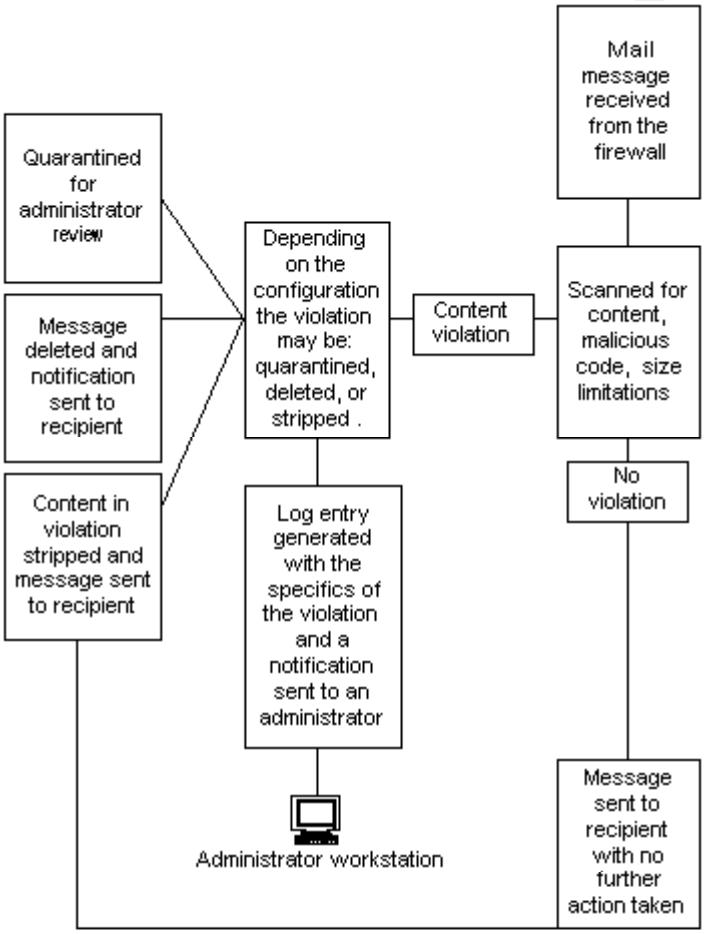

Figure 2 Data flow thru a content scanner

Web content scanner functionality is much the same as that of mail scanners. They can be configured to block web sites based on both DNS (Domain Name Service) names, such as www.blockedsitename.com and/or its corresponding IP address. Web content scanners will block the download of unauthorized software based on site configurable rules. Commonly content scanner

developers will have pre-made lists, selectable by category. This aids administrators by providing a baseline for their site policies. Contained in these lists are web sites that vendor research teams have determined to be inappropriate due to various circumstances. These lists most often contain web addresses containing unacceptable materials such as pornography, racism, sex, violence, and illegal drugs.
Having the option to review and block web sites would have had a great effect on the examples above. Many of the issues could have been avoided, thus protecting the organization and the network.

When evaluating content scanners, there are many considerations. Determining which features are necessary for your organization is difficult. After thorough testing and evaluation, if security is your primary goal, here are some considerations often overlooked but nonetheless vital to securing a network from mail vulnerabilities:

-Selectable case sensitivity. Often-found are the use of acronyms and uppercase letters, which may slip through a content scanner if configured incorrectly. For example (TS), this is a government acronym for top secret. Without case sensitivity as an option this may cause a configuration mishap. Of the tested products: MailSweeper, Mail Marshal and Mail Gear. Mail Gear does not offer this capability. To configure Mail Gear each word would have to be entered into the dictionary twice, or have a separate dictionary for uppercase and lowercase.

-Quarantining of messages based on content, attachments type, size or content and source and/or destination address. This is crucial for an administrator to analyze the messages content, view its source and possibly makes recommendations to disallow mail from the source. Quarantining also allows the administrator to decide if a message was blocked mistakenly, and allows him/her to re-examine the current policy.

-Message modification. Stripping of arbitrary determined file types with delivery and logging. This option strips the content in violation automatically and sends the remaining content of the message to its recipient. At this point a log entry is made to track the violation. Unlike quarantining, you are unable to analyze the message. The ability to remove an attachment depends on the scanner’s ability to identify the attachment type.

-Attachment Identification or recognition by file characteristics. Support for creation of custom defined file types for use in all mail processing rules by defining file characteristics common to that type. Identifying characteristics makes for a more secure environment. It has been seen that executable files can be passed without detection by simply changing its name. If a content scanner can view these files' characteristics, it is less likely that a false message would be passed. MailSweeper and MailMarshal both have this ability.

-Routing information removal. Internal masking of IP addresses is essential when securing enterprise networks. When a mail message is sent through a network, IP headers are attached to the message for routing purposes. These headers often contain the fully qualified domain name and IP address of each mail server, content scanner and firewall that is in its path. Some content scanners have the ability to remove this information or to mask it with false information configured by the administrator. MailSweeper and Mail Marshal give you this option. Sendmail is an example of a mail exchanger along with a plug in that can remove routing information. An example of this has been provided below.

```
Received: from firewall.box.com ([192.20.0.41])
      by www.sending.box.com (8.10.2+Sun/8.10.2) with SMTP id g0BK6oU02634
      for <receiver@root.com>; Sat, 12 Jan 2002 01:06:50 +0500 (GMT)
Received: from mailexchange.box.com by firewall.box.com
          via smtpd (for www.sending.box.com [148.41.0.253]) with SMTP; 11
Jan 2002 11:55:29 UT
Received: (private information removed)
Received: (private information removed)
Subject: test
Date: Fri, 11 Jan 2002 15:05:12 -0500
Message-ID: <960174C7BC037F418E2118BCE44AF95E239E@box.com>
X-Scanned-By: MIMEDefang 2.1 (www dot roaringpenguin dot com slash
mimedefang)
```

Having the ability to remove this information reduces the risk of sharing internal IP address space, thus making it more difficult for a hacker or attacker to violate your network.

The above examples were taken from a vendor survey that was distributed in response to the security needs of a recent project. Below is the actual file with responses. Putting this document together was crucial to choosing the best vendor product to satisfy the needs of a client.

	Vendor		
Content Scanning	Mail Gear	Mail Sweeper	Mail Marshall
Content Scanning			
1. Scanning for single words in message body, headers, and attachments?	Yes	Yes	Yes
2. Scanning for phrases in message body, headers, and attachments?	No	Yes	Yes
3. Support selectable case sensitivity? Global? Word or phrase wide?	No	Yes/Yes/Yes	Yes
4. Support conditional statements (ex. NEAR, NOT, AND,..)? Which? Combinations?	No	Yes/All/Yes	Yes/All/Yes
5. Support for non-alpha-numeric characters in search strings? Which are/are not supported?	Yes	Yes/All	Yes/All
6. Scanning of all known email formats (ex. BinHex, Base64, uuencode, ..) ?	No	All SMTP	Yes
7. Recognition of encryption formats?	No	Yes	Yes
8. Support for command line switches to call secondary scanners (custom scripts, virus scanners, …)?	No	Yes	Yes
9. Support for integrated modules to do additional scanning (virus, custom dlls, …)?	No	Yes	Yes
10. Support for customer selectable site for scanner upgrades (ex private server instead of vendor site)?	No	No	Yes
11. Ability to call command line programs or integrated modules on certain parts of a mail message (body, headers, individual attachments, all attachments, attachments of certain types)?	No	Attachments	Yes
	Mail Gear	Mail Sweeper	Mail Marshall
Violation Handling			
12. Quarantining of messages based on content? Attachments? Source and destination address? Source and destination domain?	Yes	Yes	Yes
13. Immediate dropping of messages based on content discovered?	Yes	Yes	Yes
14. Support for different actions based on content found (ex. multiple quarantine areas, drop some while quarantining others,..)?	Yes	Yes	Yes
15. Ability for administrator to have message delivered or dropped after review in quarantine areas?	Yes	Yes	Yes
16. Ability for administrator to arbitrarily modify quarantined message before delivery (ex. remove text, add text, manually delete unwanted attachments, …)?	No	No Only before quarantined / Cannot be done manually	Yes
17. Ability to enforce policies on attachment size? Number of attachments	Yes/Unlimited	Yes/Unlimited	Yes/Unlimited
	Mail Gear	Mail Sweeper	Mail Marshall
Message Modification			
18. Stripping of arbitrary customer determined file types with delivery and logging?	No	Yes	Yes
19. Support for explicit allow/ implicit strip list of attachment types for stripping?	No	Yes	Yes

20. Support for explicit strip/ implicit allow list of attachment types for stripping?	No	Yes	Yes
21. Support for notification message addition on modified messages?	No	Yes	Yes
22. Stripping of only some attachments in a message while leaving others intact?	No	Yes	Yes
23. Support for automatic word or phrase replacement in message body? In message headers? In attachments?	No	No	No
	Mail Gear	Mail Sweeper	Mail Marshall
Attachment Identification			
24. Attachment decompression and scanning with all known compression methods? How many levels of decompression? Mixed compressors (ex. a zipped, rared, tarball embedded in a document)?	No	Yes/ up to 50 levels /All	Yes / 20 / Yes
25. Ability to recognize when more decompression beyond customer set threshold is needed?	No	No	Yes
26. Ability to take customizable action when attachment in not decompressable within set threshold?	No	No	Yes
27. Attachment recognition by file characteristics?	No	Yes	Yes
28. Support for creation of custom defined file types for use in all mail processing rules by defining file characteristics common to that type?	No	Yes	No Beyond 160 Types Identified
29. Creation of custom defined file types for use in all mail processing rules by declared file extension?	No	Yes	Yes
30. Support for quarantining and/or stripping files of undetermined type (unknown type characteristics, type characteristics don't match extension, unknown extension, encrypted)?	No	Yes	Yes
	Mail Gear	Mail Sweeper	Mail Marshall
General			
31. Is this product already approved for Department of the Navy use? Any military use?	Yes	Yes	Yes
32. In what countries was this product developed?	US	UK	New Zealand
33. Is this product ghostable (Symantec Ghost, ghost of one box installed on another with identical hardware design)?	Yes	Yes	Yes
34. What OS's does this product require/support?	NT/2000	All Microsoft	All Microsoft
35. What OS patches does this product require?	SP6a	SP5 or above NT	SP6a / SP1
36. What hardware does this product support (ex intel, sparc, mac,…)?	Intel	Intel	Intel
37. Any minimum hardware requirements (ex hardware dongle, known hardware issues)?	None	PII 400 / 128MB	None
38. What mail protocols does this product support (ex SMTP, MSExchange,…)	SMTP	SMTP	SMTP
Mail Server			
39. Support for customization of mail server greeting message (ex. "Generic mail server ready to receive.")?	No	Yes	Yes

40. Support for customization of declared hostname in SMTP transfer (ex. “helo hidethis.privatedomain.com”)?	No	No	Yes
41. Ability to prioritize mail delivery/scanning priority based on customer definable criteria (src/dst user, existence of attachments, size of message, size of attachments)?	No	No	No
42. Support for IP based mail delivery table with mail scanning (ex. mail from server 1.1.1.1 gets relayed to server 2.2.2.2)?	No	No / Routing only to destination hosts	No
43. Support for port based mail delivery table with mail scanning (ex. mail received on port 25 gets relayed to 1.1.1.1, mail received on port 26 gets relayed to 2.2.2.2)?	No	No	No
44. Support for domain based mail delivery table with mail scanning (ex. mail to domain.com gets relayed to 1.1.1.1, mail to domain2.com get relayed to 2.2.2.2)?	Yes	Yes	Yes
45. Ability to optionally not append and/or strip existing mail routing information on customer definable mail (ex. strip all mail routing information on outgoing mail)?	No	Ability on Rcv only/ MailSweeper adds its own	Yes
46. Support for separate mail processing rules for incoming and outgoing mail?	Yes	Yes	Yes
47. Support for destination and/or source address rewriting (ex. mail to joe@domain.com is rewritten to joe@ domain.com, all users at public.com get rewritten to private.com)?	No	Yes	Yes
48. Acceptance of non-authoritative DNS replies when making DNS queries?	Yes	Yes	Yes
	Mail Gear	Mail Sweeper	Mail Marshall
Logging			
49. Ability to log to multiple logs (ex. quarantined log, sent log, received log, quarantined for bad attachment log)?	Yes	Sent and received will be logged to the same log file / quarantined will be logged to the report DB if enabled	Yes text based no SQL
50. Ability to export logs via syslog? Oracle hooks? Anything?	No	No	Yes
51. Ability to prioritize all log entries (ex. disallowed attachment=2, disallowed content=4)?	No	No	Yes
52. Flexibility with creating new logs (ex. every 10/30/60/120 minutes, size based)?	No	No	Yes
53. Ability to log when configuration changes occur?	Yes	Manually	No
54. Ability to log what configuration changes occur?	No	No	No
	Mail Gear	Mail Sweeper	Mail Marshall
Management			
55. Local management? How?	Yes / Web	Yes/ MMC	Yes / MMC

56. Remote management? How?	Yes / Web	Only services , quarantine areas and reporting via the MMC	Yes/MMC
57. Encrypted remote management? How?	No	No	
58. Support for multiple mail scanners per management console? How many?	Yes	Yes	Yes / MMC
59. Support for various management levels (ex. read-only, logs only, certain quarantine areas only, full management and configuration)?	Yes	Yes	Yes
60. Remote management requirements (OS, hardware, patches/services packs, ports, network resources)?	Microsoft	NT4 SP5/ with MMCI.2 // W2k MMCI.2 ports 20200 and 135	All Microsoft
61. What are the management security measures (ex access lists, passwords)?	NT Authentication	NT Authentication	NT Authentication
62. Support for real-time viewing of logs through management console? Queues? Refresh rate?	Yes	Real-time via SQL7	Yes
63. Support for customizable notification actions (ex. email, pager, pop up on remote console, remote beep)?	Yes	Yes	Yes
64. Support for different notification actions based on violation?	Yes	Yes	Yes
65. Ability to lock out local management and only allow remote management?	No	Yes/ not for configuration	Yes
66. What type of management session conflict resolution (ex. two full access session at the same time)?	None	None	None
67. Ability to change remote management ports?	Yes	Yes	Yes
68. Ability to import and export configuration from/to other scanners?	No	Yes	Yes
	Mail Gear	Mail Sweeper	Mail Marshall
Mobile Code			
69. Support for identification of mobile code types when attached or embedded (ex. ActiveX, Java, JavaScript, VB Script,..)?	No	Yes	Yes
70. Type of mobile code recognition (ex. keyword, file extensions,…)?	Keyword / file ext	Both	Both
71. Support for stripping mobile code and delivering mail?	No	Yes	Yes Attachments only
72. Support for message quarantining after mobile code discovery?	No	Yes	Yes
73. Support for mobile code sand boxing?	No	No	No
74. Support for making exceptions in mobile code rules based customizable criteria (source/destination address, domain, mobile code type)?	No	Yes	Yes
	Mail Gear	Mail Sweeper	Mail Marshall
Load Handling			
75. Tested messages/minute or Mb/s?	Not available	Not available	See Test Paper
76. Independent tests? Who provided test cases?	Not available	Not available	No

77. What was the test environment (ex. OS, hardware, patches, network,…)?	Not available	Not available	See Test Paper
78. Were the results independently published?	Not available	Not available	No
79. What software was used for testing?	Not available	Not available	See Test Paper
80. Maximum sustained testing length (duration and load)?	Not available	Not available	See Test Paper
81. Support for clustering?	Not available	No	Yes
82. Support for mail separation based on processing needed (ex. all messages with attachments go to box1 for intensive examination, all other messages go through box2 for faster processing)?	Not available	Not available	No
83. Estimated performance on a Dell 2450 (2 1-Ghz P3's, 2Gig RAM, 2 18Gig SCSI Raid 0) with W2K?	Not available	Not available	26 Sec
84. Estimated hardware requirements for 50,000 average email users with 1 MB max allowable attachment? 5 MB? 10 MB? With 100,000 users? 250,000 users? 500,000 users?			
	Mail Gear	Mail Sweeper	Mail Marshall
Licensing			
85. Pricing scheme (ex per user, per scanner)?	Per Scanner	Per User	Per User
86. Support for enterprise keying (ex. no internet access or phone calls needed to get machine specific keys)?	Yes	License Specific	Yes

The deployment of content scanners within a network is not a one-time task. Policy changes and reviewing updates to the content lists is an ever-evolving mission. Through due diligence, an administrator and information assurance security professional can increase the security, availability and heighten the awareness of e-mail and web use.

Conclusion

The problems related to web and e-mail use have brought to light the various scenarios that have been reported based on the threat to organizations through email and web browsing. The need for solid acceptable-use policies and the tools needed to enforce them have been identified and explained.
Content scanning should be added to the security checklist of every network administrator whose job depends on information assurance.

IV. References

[1] "Content Security: Confidentiality Breaches." URL: http://www.mimesweeper.com/products/contentsecurity/confidentiality.asp (10 Jan 2002).

[2] "Content Security: Damage to Reputation." URL: http://www.mimesweeper.com/products/contentsecurity/reputation.asp (10 Jan 2002).

[3] "Content Security: Legal Liability." URL: http://www.mimesweeper.com/products/contentsecurity/legal.asp (10 Jan 2002).

[4] "Content Security: Legal Liability." URL: http://www.mimesweeper.com/products/contentsecurity/productivity.asp (10 Jan 2002).

[5] Berg, Al. "Pulling the Plug on Surfing and Spam." Information Security April 2000 57-67

[6] "Content Security: Degradation in Service." URL: http://www.mimesweeper.com/products/contentsecurity/service.asp (10 Jan 2002).

[7] "At the forefront of content security." URL: http://www.mimesweeper.com/products/contentsecurity/default.asp (10 Jan 2002).

[8] "Policy-Based Information Protection and Data Integrity." URL: http://www.mimesweeper.com/download/collateral/pdfs/idcreport.pdf (10 Jan 2002).