



realtimepublishers.comtm

Tips and Tricks
Guidetm To

Secure Content
Appliances

McAfee[®]
Proven Security[™]

Dan Sullivan

Note to Reader: This book presents tips and tricks for four topics related to secure content appliances and their role in enterprise security. For ease of use, the questions and their solutions are divided into topics, and each question is numbered based on the topic, including

- Topic 1: Business Justification for Secure Content Appliances
- Topic 2: Policies and Procedures for Secure Content Management
- Topic 3: System Architecture and Secure Content Management
- Topic 4: Secure Content Appliance Performance

Topic 1: Business Justification for Secure Content Appliances1

Q 1.5: What are best practices for educating users about spyware, spam, and phishing?1

Preventing Spyware Infections1

How to Reduce Spam.....3

Phishing Facts Every Email User Should Know4

Topic 2: Policies and Procedures for Secure Content Management.....5

Q 2.4: How can administrators use quarantine and deferred mail management to secure content?5

Quarantining Content.....6

Deferred Email Management.....8

Q 2.5: Some spam passes through the filters; how can the filtering be improved?8

Identifying Spam with General Rules.....9

Erroneous Categorizing11

Additional Filtering Mechanisms11

Staying Up to Date.....12

When All Else Fails12

Topic 3: System Architecture and Secure Content Management13

Q 3.5: How do appliances stay up to date on the latest threats?.....13

Tracking Updates13

Updating Antivirus Applications14

Updating the Anti-Spam Application14

Topic 4: Secure Content Appliance Performance.....15

Q 4.4: How can an organization minimize spam?15

Educate Users.....15

Do Not Contribute to the Problem.....16

Q 4.5: How can an organization implement better access controls to Internet content?16

Copyright Statement

© 2006 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Topic 1: Business Justification for Secure Content Appliances

Q 1.5: What are best practices for educating users about spyware, spam, and phishing?

A: The first step in educating users about spyware, spam, and phishing is to explain the nature of the problem and the consequences of unwanted emails and programs.

Preventing Spyware Infections

In addition to using spyware blocking and removal tools, there are several steps users can take to reduce the chances of a spyware infection. These include:

- Properly configuring your browser—For Internet Explorer (IE), proper configuration includes disabling the Enable Install On Demand options (see Figure 1.6 for an example).

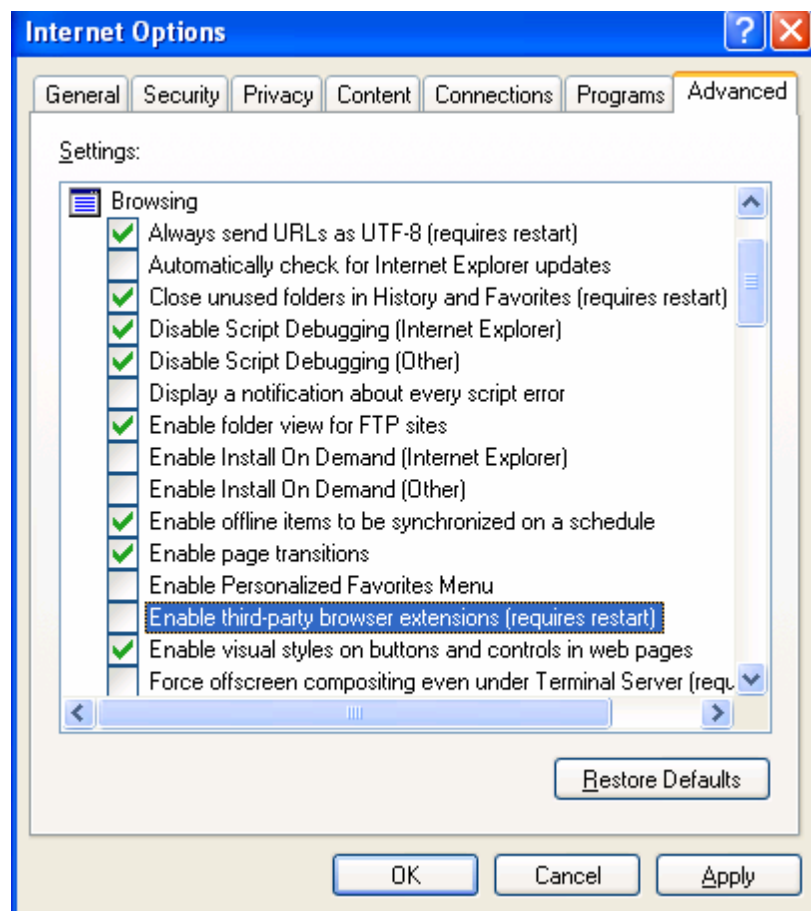


Figure 1.6: Configuring browser security settings is one step to reducing the chances of a spyware infection.

For more information about controlling IE security, see “Working with Internet Explorer 6 Security Settings” at <http://www.microsoft.com/windows/ie/using/howto/security/settings.msp>.

Mozilla Firefox, another popular browser, has fewer known vulnerabilities than IE and is thus a good option for security-conscious users. As with IE, Firefox users can disable the automatic installation of software, as Figure 1.7 shows.

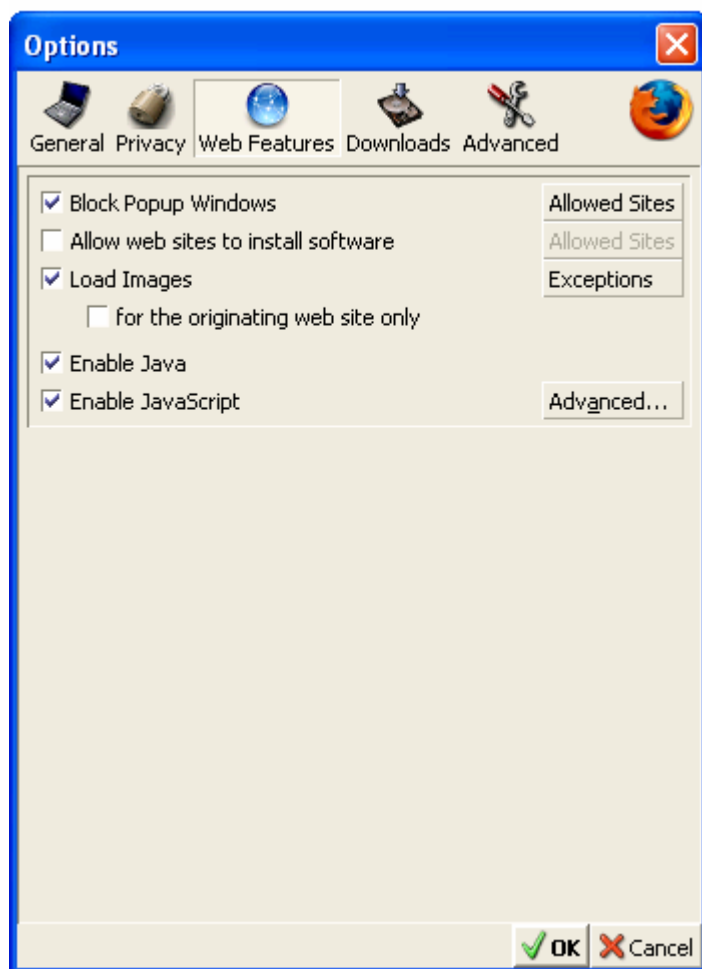


Figure 1.7: Firefox allows users to disable the automatic installation of software.

If the “Allow web sites to install software” option is selected, users can specify which sites are allowed to install software (see Figure 1.8).

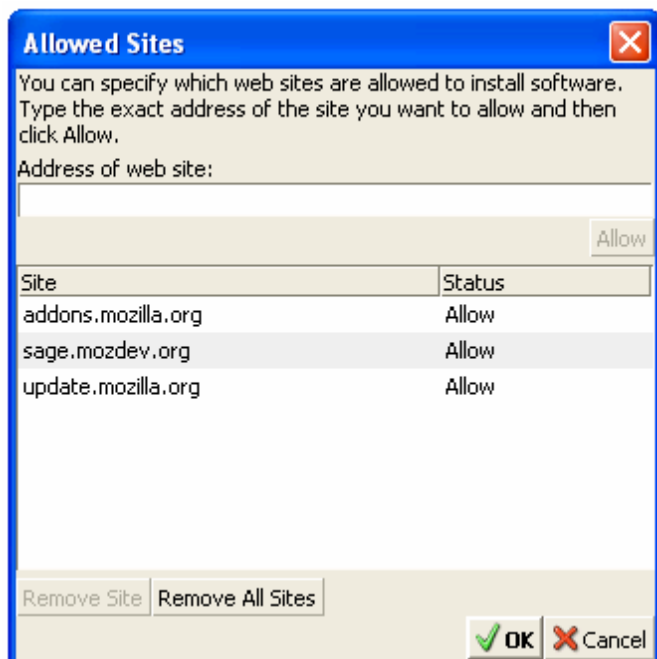


Figure 1.8: Firefox allows users to list trusted sites for the purpose of automatically installing software.

- Browse trusted sites—File sharing sites, such as music “sharing” sites, are likely spots for picking up spyware and other malware.
- Keep your browser and operating systems (OSs) up to date with patches.
- Use a firewall—Doing so can help prevent spyware from transmitting information from your computer.

How to Reduce Spam

It’s safe to assume spam will always be with us. Although spam filtering can be quite successful, reaching into the 90+ percent success rates for blocking spam, it’s better to never receive spam in the first place. The following list highlights options for minimizing the amount of spam you receive:


- Do not add your email address to newsletters, opt-in offers, or other lists without understanding how your email address will be used. Reputable businesses and organizations publish and adhere to privacy policies. Make sure you understand an organization’s privacy policy before giving them your address.
- Do not post your email on newsgroups or Web-based message boards. These sites are culled by spammers for email addresses.
- Do not respond to spam. A reputable mass emailer may take you off a list as requested but don’t assume you are working with a reputable business if you don’t know them.
- Use a disposable email address when you must give an email address. If this disposable address begins to attract too much spam, drop the address.

Phishing attacks are a more troubling type of spam that warrant their own set of guidelines.

Phishing Facts Every Email User Should Know

Email users should understand the following about phishing attacks:

- Phishing is a form of social engineering, otherwise known as a con. The phisher gains the confidence of their target and then elicits useful information.
- Phishers gain confidence of victims by *appearing* to be a trusted and legitimate entity, such as a bank or other business. It is relatively easy to steal logos and even entire Web pages from Web sites, so users should not be fooled by the well-known logo or look and feel of their bank.
- Rather than judge an email by appearance, examine the content closely. For example, is your bank emailing you that they need to verify your account number, Social Security number, or online banking password? If so, the message is most likely a phishing scam. When in doubt, ask yourself, has the bank ever called or sent postal mail with these questions? Chances are they haven't. Banks and businesses have other ways to verify their records.
- Beware of emails with upsetting or exciting messages. Phishers count on emotion to overtake rational assessment. If something serious has occurred with your personal finances, would a business email you about it? Not likely. When credit card companies suspect fraud, they call the home phone number of the card holder.
- If you do decide to follow a link in an email, always type the URL into the browser. Doing so will help avoid any tricks used to exploit vulnerabilities in browsers. It will also make it more likely you will catch a minor difference in a legitimate Web address that links to a bogus site.
- Watch for promises of prizes, get-rich-quick schemes, and similar appeals to greed coupled with a request for personal information. (Spam sometimes makes similar promises but requires the recipient to purchase something in return).
- Spammers blanket thousands of email addresses, pretending to be EBay, Pay Pal, banks, and other institutions. Don't be surprised if you receive a phishing email from a business with which you have an account; phishers count on getting at least some customers from those businesses.
- Do not put personal or financial information in an email or Web site in response to an email. When in doubt, contact the business either by phone or through the business's Web site (by typing in the Web address or getting it from a search engine; don't use the URL in the email).

 For more information to educate users about phishing scams, see the Anti-Phishing Working Group's "Consumer Advice: How to Avoid Phishing Scams" at http://www.antiphishing.org/consumer_recs.html, the United States Federal Trade Commission's "How Not to Get Hooked by a Phishing Scam" at <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>, and the United States Department of Justice's "Special Report on Phishing" available at http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf.

As with other security threats, phishing is a process of evolving threats and countermeasures. As email users become more educated about the nature and consequences of phishing, phishers have to hone their appeals. The latest evolution of phishing has earned the name “spear-phishing” because it uses low volumes but highly targeted phishing emails. This method makes these types of attacks more difficult to detect by businesses and more likely to fool the intended victim.

📖 See Computer World’s “Training Needed to Halt Spear-Phishing Attacks” at <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,104087,00.html?source=x584> for more information about spear-phishing, including the results of a test conducted by the State of New York on email users at five state agencies.

Topic 2: Policies and Procedures for Secure Content Management

Q 2.4: How can administrators use quarantine and deferred mail management to secure content?

A: When there is a problem with a message or a document, how can it be addressed? There are several options:

- Delete the message or document
- If the problem is a threat, such as a virus infection, clean the message or document and send it on
- If the message cannot be cleaned, store the message for further review
- If the content of the transmission contains banned words or phrases, store the message for further review
- If the message cannot be delivered, store it for future delivery attempts

The first option works well with known spam or messages that are sent containing banned language. The second option is used to allow messages through after the threat has been eliminated and there is no concern for harm to network resources. The remaining options all require the ability to isolate and store content before acting on them further. A secure content appliance should do so by providing quarantine areas and deferred mail storage as Figure 2.4 shows.

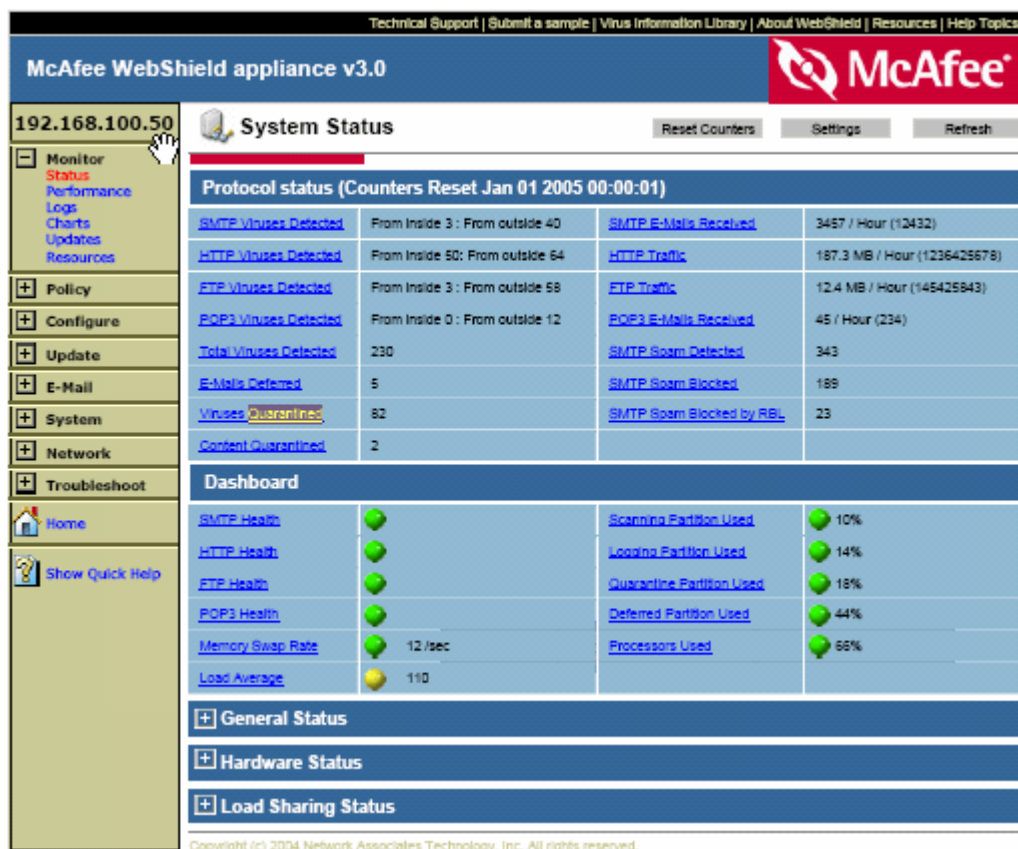


Figure 2.4: At any time, a systems administrator can find the number of quarantined and deferred messages stored in the appliance.

Quarantining Content

Quarantining content isolates a threat to a storage area on the appliance so that the threat cannot harm network resources. A message should be quarantined if one of two things occurs:

- The message is infected with a virus that cannot be removed and the governing policy dictates that, as a secondary action, the message must be quarantined
- The message is categorized as spam

Isolating Virus-Infected Messages

Once quarantined, administrators should review the messages and take appropriate action (see Figure 2.5).

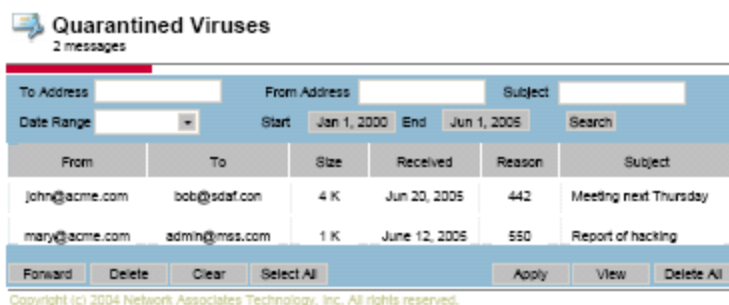



Figure 2.5: Quarantined viruses are kept in a secure area on the appliance until they are acted upon by the administrator.


Administrators have several options for dealing with these isolated messages. The messages can be viewed, deleted, or forwarded.

 Unless the message is being sent to an antivirus vendor as a sample for analysis, use forwarding with care. The message will still be infected.

Quarantining a virus-infected message keeps the malware from reaching the desktop. Although the desktop is likely protected by local antivirus software, it is better to keep the virus from reaching its destination. The desktop, for example, may not have the latest antivirus signature files or scanning engine. Some malware is now designed to disable desktop antivirus programs. Another technique changes the local host file so that automatic updates programs cannot reach vendor's sites to download updates. Quarantining at the appliance is another example of layered protection that compensates for vulnerabilities and threats to individual components of the security system.

Isolating Spam

Identifying spam is not an exact science. Some messages that may appear to be spam are legitimate emails and vice versa.

 Question 2.5 explores how spam filtering depends upon rules that score messages as to the likelihood of them being spam.

Some spam is easily identified and systems administrators can be confident that it is actually spam. Borderline cases are more problematic. Administrators do not want to raise the threshold too much on what is considered spam or else spam that should be blocked will make it to recipients' inboxes. At the same time, email administrators do not want to delete a legitimate email that is mistakenly categorized as spam. Quarantining provides a middle ground. Messages that are considered spam can be stored in the email quarantine area until they are reviewed by the administrator and dispatched accordingly.

Deferred Email Management

Information security is often described as providing CIA: confidentiality, integrity, and availability. Deferred email management contributes to integrity and availability by providing the ability to defer the delivery of messages if there is a problem relaying a message. Ideally, a high-level dashboard display, as Figure 2.6 shows, will include the status of deferred messages.

Protocol status (Counters Reset Jan 01 2005 00:00:01)			
SMTP Viruses Detected	From inside 3 : From outside 40	SMTP E-Mails Received	3457 / Hour (12432)
HTTP Viruses Detected	From inside 50: From outside 64	HTTP Traffic	187.3 MB / Hour (1236425678)
FTP Viruses Detected	From inside 3 : From outside 58	FTP Traffic	12.4 MB / Hour (1454258431)
POP3 Viruses Detected	From inside 0 : From outside 12	POP3 E-Mails Received	45 / Hour (234)
Total Viruses Detected	230	SMTP Spam Detected	343
E-Mails Deferred	5	SMTP Spam Blocked	189
Viruses Quarantined	82	SMTP Spam Blocked by RBL	23
Content Quarantined	2		

Figure 2.6: A secure content appliance interface should provide summary information about the number of quarantined and deferred items.

Controlling Content Distribution

Quarantining is also used with content filtering to ensure that controlled content—such as proprietary information, personal documents, and other confidential material—is not sent outside the organization inappropriately. Like spam, the suspect content may be stored on the appliance and held for review by the application administrator.

Quarantining and deferring are two common methods for creating middle grounds. In the case of quarantining, infected messages, borderline spam, and suspect content can be held and reviewed before letting it pass or deleting it completely. In the case of deferred email, messages can be stored and forwarded at a later time rather than discarding a message after initial attempts fail.

Q 2.5: Some spam passes through the filters; how can the filtering be improved?

A: Spam filters depend upon rules that are designed to identify messages that are truly spam without mistakenly categorizing legitimate email as spam. These rules are created by examining large numbers of spam messages to identify characteristics common to spam. Typically, these rules take into account phrases commonly found in spam and their location within the structure of an email.

Identifying Spam with General Rules

Spam messages will, of course, vary, but there are common characteristics that anti-spam designers can use to identify the most obvious spam:

- Promises of easily earned money
- Free or discounted items
- Apparent messages from a customer service department
- Surveys
- Fear-inducing messages, such as claims that the reader's PC is unprotected

Marketers have long known that short, well-phrased pitches can get a user's attention. Spammers use the same principal, and, fortunately for the rest of us, this is the Achilles heel of spam. Table 2.1 lists several phrases that are good indicators of spam along with scores, or weights, indicating the relative confidence that this phrase indicates a piece of spam.

Spam Indicator	Score
Get paid for your opinion	2.0
On sale	1.0
Limited time	0.8
Unbelievable prices	0.8
From: Antivirus Administrator	1.2
Dear Friend	1.8
Congratulations you are a winner	2.0

Table 2.1: Example spam phrases and scores of the likelihood that they are spam.

Scores are essential to measuring the likelihood of spam. All of the phrases listed in Table 2.1 can be used in legitimate emails. However, if enough of them are used, even if they only weakly indicate spam (for example, through the use of "limited time"), there is a good chance the message is actually spam. Similarly, if only two or three phrases are used but are strongly correlated with spam (for example, "Get paid for your opinion"), chances are good that the message is spam.

The filtering rules add the score associated with each matching spam phrase to find the total score for a message. If the score exceeds a threshold, the message is considered spam.

To illustrate how this works, consider two example emails. The first is a legitimate message in response to a sales call.

Dear Frank,

Thanks for taking the time to meet with me yesterday about our new line of office furniture ***on sale*** through the end of the month. I'm sure you'll agree that some of our specials are at ***unbelievable prices*** but we are only offering these to select customers and for a ***limited time***.

I've attached a formal proposal for your review. Please feel free to contact me with any questions; otherwise I will call you Friday to follow up.

Regards,
Mary Jones
Acme Office Furniture

This message has three phrases commonly found in spam (indicated by bold italics). The total score is calculated as:

On Sale	1.0
Unbelievable prices	0.8
Limited time	<u>0.8</u>
	2.6

Assuming a threshold of 4 (a low tolerance for spam), this message is not considered spam and would pass through the filter. The following example is a fictional but representative spam:

Dear Friend,

Congratulations you are a winner! For a ***limited time***, you can claim your prize from Grand Award Sweepstakes! Just click the link below, provide us with your name and address and the bank account number where you would like the funds deposited.

Again, congratulations,
Yours truly,
Grand Award Sweepstakes Prize Committee

This message also has three phrases commonly found in spam (indicated by bold italics). The total score for this message is:

Dear Friend	1.8
Congratulations you are a winner	2.0
Limited time	<u>0.8</u>
	4.6

As the total is greater than the 4.0 threshold, this message would be correctly categorized as spam.

This technique generally works well because it's fast (there is no complex analysis, just string matching and simple arithmetic), and with well-crafted rules, correctly categorizes most spam. However, occasionally, things do not work as planned.

Erroneous Categorizing

Spam filter rules are not perfect. They apply rules derived from examining large samples of spam and non-spam messages. Using statistical methods, rule designers can generalize rules from large samples to find the best indicators of spam. As with the use of statistical methods in other applications, there is a margin of error. These errors come in two forms: false positives and false negatives.

False Positives

A false positive mistake categorizes a legitimate email as a piece of spam. This mistake occurs when phrases commonly found in spam are used in the email. If false positives are occurring at an unacceptable rate, the threshold for classifying a message as spam may be raised. Doing so will cause fewer messages to fall into the spam category and reduce the chances of a false positive because the message has some, but not many, characteristics in common with spam. For example, the first sample message would have been categorized as spam if a lower threshold, such as 2.5, had been set. Although lowering the threshold decreases the chance of false positives, it increases the chances of a false negative.

False Negatives

False negatives are mistakes that allow spam to pass through as legitimate email. In the ideal spammer world, spammers would be able to maximize their use of marketing phrases that catch readers attention while still “flying under the radar” of the anti-spam filters. As spammers learn the phrases that cause their messages to be filtered, they will vary the content of the message to avoid trigger matches with spam rules. If they can avoid triggering enough rules, their message scores will fall below the threshold and the spam will make its way to the recipient. Such messages are false negatives.

Clearly, there is not a definitive set of rules that will correctly identify all spam while avoiding false positives. Even if you could compile an ideal set of rules for all known spam, it would not necessarily work as well for new spam created by spammers with those very rules in mind. Filtering spam is a cat-and-mouse game. Spammers are constantly trying to avoid detection and will continuously vary their content.

Additional Filtering Mechanisms

Besides filtering rules, spam can be controlled through the use of white lists and black lists. A white list contains email addresses and domains trusted not to send spam. Business partners, clients, patients, government agencies, public companies, and other organizations that do business with a company may be added to the white list. Any messages that are sent from those addresses are not subject to filtering by spam rules.

The white list is useful for two reasons. First, as the messages are not scanned for spam phrases, the anti-spam application can operate more efficiently. This benefit is especially useful when a small number of domains send a large proportion of all email to a business or organization.

Black lists contain a list of addresses and domains of known spammers. Any message from an address on the black list is categorized as spam and not allowed through. Black lists complement filtering rules based on content phrases. Rather than crafting rules to cover all the spam that may come from known spammers, the black list effectively shuts down traffic from those addresses.

Staying Up to Date

It is also important to stay up to date on spam filtering rules and the anti-spam engine. Anti-spam designers build new rule sets to address the changing patterns of spam as they emerge. Appliance administrators can use the Update | Anti-Spam option in the appliance to download and install the latest rules and anti-spam engine (the application that executes the rules).

When All Else Fails

There may be times when the up-to-date spam filters, black and white lists, and threshold adjustments are not effectively blocking spam. When that occurs, contact your vendor and submit samples of the spam that is slipping through. Anti-spam designers will then be able to study the spam and develop appropriate countermeasures.

Where to Send Spam Examples?

Most anti-spam vendors accept examples of spam that are not blocked by their products. The following list provides some of the most popular vendors along with instructions for submitting spam:

- McAfee customers can send examples of spam to customer+false-positive@clicknet.com and customer+missed-spam@clicknet.com
- TrendMicro users can send their examples to spam@support.trendmicro.com
- Symantec users can send spam examples by following the instructions posted at http://service1.symantec.com/SUPPORT/ent-brightmailkb.nsf/0588786bcfa7fb9888256f72007c8a4b/5d0964f0afa6403f88256f93008006cb?OpenDocument&src=bar_sch_nam&seg=sb

Finally, when there is a sudden outbreak of a particular type of spam, vendors may develop specialized rules, known as extra rules in the technical documentation, to combat the outbreak.

To summarize, the following steps should be followed to improve the spam detection rate of a secure content appliance:

- Update anti-spam filtering rules
- Update the anti-spam engine
- Adjust spam score threshold
- Add entries to the black list and white list
- Submit samples of missed spam to your anti-spam vendor
- Download extra, specialized rules as needed

Following the first two steps will help to ensure the appliance is configured to filter the latest and broadest range of spam. Adjusting thresholds and configuring black and white lists can fine tune the appliance's performance. In special circumstances, submitting a sample of missed spam and downloading specialized rules may be the correct course of action.

Topic 3: System Architecture and Secure Content Management

Q 3.5: How do appliances stay up to date on the latest threats?

A: Vendors typically provide frequent updates for secure content appliances. Virus developers and spammers change their techniques and content to avoid detection, but vendors keep abreast of these changes and update both signature files (virus definition and spam definition files) and the scanning engines that use those signature files. Fortunately, keeping the appliance up to date on the latest threats is a relatively simple matter because the appliance automates virtually all of the work.

Tracking Updates

The option Monitor | Updates tool allows administrators to set the schedule for updating both signature files and scanning engines.



Figure 3.10: The automatic update facility allows for separate scheduling of signature file (rules) and scanner (engine) updates.

The option Monitor | Updates displays information about the status of antivirus and anti-spam automatically scheduled updates. The display includes

- Names of scheduled updates
- Current status of each scheduled update
- Date and time of last update

Antivirus and anti-spam updates are configured separately.

Updating Antivirus Applications


Antivirus applications should be updated at least once per week but more frequently is preferable. Most antivirus designers and developers are regularly updating virus definition files to counter emerging threats. Although the application uses heuristic, or “rule of thumb,” filters to catch a class of viruses as well as virus-specific rules to detect specific viruses, it is best to keep the virus definition files up to date to ensure new threats are consistently detected. When a virus spreads suddenly or can inflict significant damage, antivirus vendors will create extra definition files and release them as soon as possible to combat the spread of the virus.

In addition to keeping the virus definition file up to date, the appliance keeps the antivirus engine up to date. The engine is the program that reads the virus definition file and uses those definitions to identify viruses and clean infected files. The engine is updated to detect new types of viruses that do not have the same characteristics as older viruses. In general, the engine is updated every few months.

Update files can be downloaded to the appliance from three sources:

- An authorized vendor FTP site
- A proxy on the local area network (LAN), if the appliance is not configured to access external FTP sites directly
- A server within the network that has already downloaded the files

To keep up to date, use the Monitor | Status | General Information or the Monitor | Updates option to determine the current revision level of the antivirus engine and virus definition file.

 Virus definition files and antivirus engine updates are available at <ftp://ftp.nai.com/virusdefs/4.x/>.

Updating the Anti-Spam Application

Like the antivirus application, the anti-spam components of a secure content appliance are updated frequently by vendors. Both spam definition files and the anti-spam engine are kept up to date to counter changes in spamming practices.

New anti-spam definition files will contain rules to identify spam that may have slipped past earlier filters. In addition, extra rules are created for sudden widespread instances of spam that are otherwise not caught by existing filters. By keeping up to date on the latest virus and spam threats, secure content appliances are able to deploy appropriate countermeasures as new threats emerge.

Topic 4: Secure Content Appliance Performance

Q 4.4: How can an organization minimize spam?

A: Spam will not be eliminated in the foreseeable future, but there are several measures organizations can take to minimize spam:

- Educate users
- Filter content to prevent spam from entering the network
- Prevent inadvertent relaying of spam
- Prevent Trojan horse programs from distributing spam through your computers

These measures use a combination of human and technical countermeasures to decrease the likelihood of spam.

Educate Users

Getting a spam message in front of a reader is a key goal of spammers; it is also a critical point for actions that can affect the level of spam this person receives. If spam does make it to a user's inbox, the user should flag the message as spam or junk mail if their email client has a built-in filter. In addition, the user should *not*

- Reply to the message
- Unsubscribe to the message
- Buy anything solicited by the email
- Click on a link embedded in the email


These actions will inform the spammers they have found an active email address. In the case of clicking on a link, making a purchase, or even just loading an HTML-based email, which sends back tracking information, these actions can improve the effectiveness of spam. The cost of spamming is so low (especially when the spammers use computers and bandwidth belonging to someone else) that even a small number of responses can make the whole spamming operation worth their efforts.

In addition to properly handling spam, users should provide their email addresses only to trusted parties. When signing up for online services, users should read the privacy agreement and understand for what purposes their email addresses will be utilized and whether their addresses will be sold to a third party. Do not post a personal email address online. Also, do not forward email from an unknown sender; doing so may lead to another user replying to the original spam, purchasing something from the spammer, or otherwise contributing to the success of the spam operation.

Do Not Contribute to the Problem

Also, organizations should make sure they are not contributing to the problem. First, ensure that email servers do not provide for third-party relay. This service is provided by email servers that allow external users to send messages through the server without checking that the sender is a legitimate user. This feature of email servers allows spammers to use the resources of other organizations to send their junk email. To help minimize spam and reduce the threat of impacting the efficiency and productiveness of your own servers, configure email servers to prevent third-party relay.

The secure content appliances have to act as relay agents, so it is important to configure the appliances to relay only locally originating mail. Adding at least one entry to the local domains list on the appliance will enable anti-relaying functions and protect against spammers appropriating your mail services. This entry should be added when the appliance is installed. An open relay can easily be discovered on the Internet, often in a matter of just several hours.

 If you are not sure whether third-party relay is enabled on your email servers, test for it using the mail relay testing service from the Network Abuse Clearinghouse. The service is available at <http://www.abuse.net/relay.html>.

Do Not Become a Zombie

Zombies are computers that have been compromised to the point where an attacker can control the functions of the computer. A number of well-known blended threats (malware that includes multiple pieces of malicious code, such as a virus, worm, Trojan horse, keylogger, and video frame grabber) include code to gain some control over the infected computer. Once in place, the malware opens a communication channel with a chat room or private server where it finds additional instructions, updated code, or new code to execute on the compromised machine. Networks of these zombie computers may be used by spammers to conduct their mass mailings.

To prevent this type of breach, use layered defenses, including desktop antivirus software, network and personal firewalls, and content filtering on the network. A secure content appliance provides effective countermeasures to several different types of threats and provides a first line of defense to keep servers, desktops, and other network devices from becoming unwitting participants in a spammer's efforts.

Q 4.5: How can an organization implement better access controls to Internet content?

A: Controlling access to the Internet content is a challenge. Browsers are ubiquitous, there are many sites accessible to users, and the number and nature of sites are changing constantly. Rather than defining access controls on all objects, as is commonly done with operating systems (OSs) and applications, systems administrators are better able to manage Internet content by applying filters as the content is accessed. This method changes the typical access control model of "User A is allowed to perform operations 1, 2, and 3 on file X" to "Users are not allowed to download content from the following sites..."

Content filtering is the process of blocking access to sites listed in a library of banned sites. These libraries, known as black lists, categorize URLs into groups such as entertainment, gambling, shopping, sports, and so on. Effective blacklists can range in size from hundreds of thousands to millions of URLs. As Web content changes constantly, URL blacklists should be updated frequently. At the same time administrators are blocking known banned sites, they may also know of specific sites that should not be accessed from business systems. Blacklists are used to block all content sites regardless of the content. Similarly, white lists are used to ensure that sites with legitimate use in business operations, such as business partners' Web sites, professional references, and general information sites, are always accessible.

As network scanning appliances are typically placed just inside the firewall, they are ideally positioned to scan content as a form of Internet access control. An additional benefit of an appliance-based approach to Internet access control is that antivirus and anti-spam services are available as well. If a user manages to access an untrusted site, such as a peer-to-peer file-sharing network used for downloading shareware, for example, and downloads an infected file, the antivirus scanner will be able to stop the virus before it can infect local devices.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.