

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

Q1.3: What is the ROI for secure content appliances?1

ROI and Related Calculations.....1

Calculating ROI on Secure Content Devices.....2

Topic 2: Policies and Procedures for Secure Content Management.....6

Q2.2: How can a systems administrator monitor the effectiveness of current settings?6

Establishing a Baseline6

Reporting on Appliance Performance.....7

Monitoring Tasks11

Topic 3: System Architecture and Secure Content Management12

Q3.2: Why are desktop antivirus software and personal firewalls still needed?12

Layered Security12

Securing Mobile Devices15

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

Q4.2: How can an organization protect against spyware?.....15

Keeping Spyware Out.....16

Copyright Statement

© 2005 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 Content Central. To download other eBooks on this topic, please visit [http://www.realtimepublishers.com/contentcentral/.](http://www.realtimepublishers.com/contentcentral/)]

Topic 1: Business Justification for Secure Content Appliances

Q1.3: What is the ROI for secure content appliances?

A: The Return on Investment (ROI) for a secure content appliance is based on a range of factors, including:

- Losing productivity of employees who have to deal with spam in their email accounts
- Additional hardware and software licensing costs to maintain adequate resources to process high volumes of email, including spam
- Losing staff time to eradicating and repairing damage caused by malware infections
- Avoiding fines for failure to comply with regulations
- Avoiding lost intellectual property when proprietary documents are transferred out the of the organization

Clearly, some factors are easily quantified, such as the amount of storage that is taken up with spam. Others, such as lost employee productivity, can at least be roughly estimated. However, some of the largest factors, such as regulatory fines and lost intellectual property are difficult to assess. Nonetheless, organizations can perform some basic ROI analysis on secure content appliances.

ROI and Related Calculations

ROI is one of a number of capital expenditure analysis calculations. Depending upon your needs, one or more of these calculations may be used to determine whether deploying a secure content device makes financial sense. The most commonly used calculations are:

- Present value—Present value is a calculation that takes into account the value of money over time. For example, if a company saves \$10,000 in 1 year from an investment in IT infrastructure, and one can reasonably expect to earn 6 percent if that savings were invested (that percentage is known as the discount rate), then the present value of \$10,000 a year from now is $\$10,000/1.06$ (1 plus the discount rate), or approximately \$9434.
- Net present value—The net present value is similar to present value but takes into account initial costs.
- Payback period—The payback period is the time period in which the total savings from an investment equals the amount of the investment. For example, a \$25,000 investment that saves \$10,000 per year has a payback period of 2.5 years.

- ROI—ROI takes into account both the net present value of money and the net benefits realized by the investment. Net benefits are defined as:

Savings + Increased Revenue - Recurring Costs

Without going into the details of why the calculation is defined as it is, here is the basic formula for calculating ROI over a 3-year period:

$$\frac{[\text{Net Benefit for Year 1} / (1 + \text{Discount Rate})] + \text{Net Benefit for Year 2} / (1 + \text{Discount Rate})^2 + \text{Net Benefit for Year 3} / (1 + \text{Discount Rate})^3]}{\text{Initial Costs}}$$

- Internal rate of return—The internal rate of return (IRR) calculation is the most complex of the group listed here. IRR is often used to compare the benefits of different projects and choose among them. As IRR is expressed as a percentage, it is easy to compare projects of different financial and time scales. IRR calculates the discount rate at which the present value of the net benefit of an investment equals zero. (Microsoft's XIRR function and Star Office and Open Office's IRR function can be used to calculate IRR.)

 For more information about IRR, see and "Internal Rate of Return Revisited" at http://members.tripod.com/~Ray_Martin/DCF/nr7aa003.html.

Calculating ROI on Secure Content Devices

To assess the investment value of a secure content device, you need to include in calculations the costs of spam, viruses, phishing attacks, lost productivity that result from non-business-related Web activity, violations of regulations, and loss of intellectual property. The last two items are difficult to estimate. The following example will ignore those values, as they are very environment dependent—thus, the results of the calculations may underestimate the true value of the investment.

The Cost of Spam

First, let's examine the cost of spam. There are basically three types of costs: lost productivity, additional hardware costs, and additional administrative costs. To calculate lost productivity, start with the number of email users, the average number of spam messages, and the time required to read and delete those messages. The basic formula for calculating lost productivity is:

$$\text{Number of email users} * \text{number of spam messages per day PER USER} * \\ \text{time in minutes to read/delete spam message} * (\text{average hourly} \\ \text{rate} / 60) * \text{number of work days per year}$$

To calculate storage costs, start with the number of email users, the average number of spam messages, the average spam message size, the number of days the message resides on the server, and the average cost of storage. The basic formula for calculating spam storage costs is:

$$\text{Number of email users} * \text{number of spam messages per day per user} * \\ * \text{average spam size} * \text{average cost of 1MB storage per year} / 365 * \\ \text{number of days message stored}$$

To calculate additional administrative costs, you need to estimate the number of minutes per day email administrators manage spam problems and the hours per month, on average, email administrators and systems administrator spend addressing storage and network traffic-related problems as a result of spam.

With these three factors—lost productivity, additional hardware costs, and additional administrative costs—you can estimate the cost of spam to an enterprise. Figure 1.2 shows an example calculation of a payback period.

User Inputs		Results	
Number of email users	500	Software Costs	
Number of years to perform the analysis	1	Lost user productivity due to incoming spam	\$ 100000
Assumptions		subtotal	\$ 100000
Daily number of junk emails received per user	10	Hardware Costs	
Time in minutes to read an email message	0.1	Spam mail storage space costs	\$ 16569
Average hourly employee rate (fully burdened)	\$ 50.00	Cost of managing spam and junk mail infestations	\$ 3000
International factor	1	Email server downtime recovery costs due to large message stores	\$ 900
Annual number of work days	240	subtotal	\$ 20469
Average message size in bytes	17000	Total Spam Costs	\$ 120469
Average cost of storage per MB	\$ 0.28	Cost of McAfee SpamKiller	\$ 7185
Average storage length in days of spam messages	2	Your Saving with McAfee SpamKiller	\$ 113284
Daily time in minutes spent by IT managing spam mail problem	15		
Potential email downtime in hours per month from large message stores or excessive message traffic	1.5	Time to recoup investment (in days)	23

*SpamKiller pricing is based on protection using SpamKiller for WebShield appliances.

Figure 1.2: Example savings and pay-back period on one component of a secure content device—McAfee SpamKiller anti-spam software.

To calculate the ROI of this investment, simply take the net benefit and divide it by 1 plus the discount rate. Assume the net benefit is the savings on spam costs calculated in Figure 1.2, \$120,469, the initial costs are \$7185, and a discount rate of 6 percent. The ROI for this investment is:

$$\text{ROI} = (\$120,469 / 1.06) / \$7,185 = 1581\%$$

For every dollar spent on spam protection, \$15.81 is saved. The cost of other threats to secure content are calculated in a similar manner.

The Cost of Viruses

Spam is constant, so users are always having to deal with it. Viruses, while still prevalent, do not present the same constant and sustained level of success in reaching targets. Therefore, one of the key factors in estimating the value of antivirus devices is understanding the probability that a virus will successfully infect an unprotected device. The other factors, which Figure 1.3 shows, are comparable to those used in the spam calculation.

GroupShield for Exchange Return On Investment Calculator

Number of Clients (Desktop Nodes):	<input type="text" value="1000"/>	
Expected Number of Virus Hits Per Month Per Machine:	<input type="text" value="5"/>	
Expected Rate of Infection Without Protection:	<input type="text" value="0.028"/>	
Number of Infections Per Year:	1680	
Cost to Clean & Restore Machine: \$	<input type="text" value="255"/>	
Annual Clean up Costs: \$	428400	
Annual Lost Productivity: \$	749280	
Annual Economic Impact of Virus Infections - 2002: \$	1177680	
GroupShield per license price: \$	<input type="text" value="38"/>	←----- Enter your price per license here (default is \$38)
GroupShield cost: \$	38000	
In-House Costs: \$	<input type="text" value="75850"/>	
Projected Annual Costs of Protection for the Enterprise Per Year: \$	113850	
Return on Investment for Virus Protection:	\$ 1040276	
Return on Investment Ratio (Amount saved for every \$1 spent on \$ protection):	9.13	
Number of days for GroupShield to pay for itself:	10	

Cost of virus outbreak information Copyright (c) Computer Economics Inc.
 GroupShield costs are approximate, and based on pricing at time of publication.
 In-House costs have been based on one IT Professional earning a gross salary of 100,000 USD per annum.

Figure 1.3: Example savings and ROI ratio for antivirus protection.

The Cost of Lost Productivity and Non-Business–Related Web Activity

Checking personal email, shopping online, browsing online casinos, and other non-business–related activities can put a drain on productivity. Secure content devices can prevent not only malware and unwanted content from entering an enterprise network but also users from browsing sites unrelated to business operations. Even a cursory examination of Web logs can give some indication of the level of this problem within an organization. How many users are visiting time-wasting sites? What is the duration of time spent at those sites? With estimates of those two measures, you can calculate the expected savings in productivity by blocking those sites.

However, blocking sites does not guarantee that the time will be used 100 percent productively. When calculating productivity savings, consider using an adjustment factor to account for this fact.

The ROI from a secure content device is substantial even when considering only easily quantifiable measures, such as savings due to spam and virus protection. “Soft” benefits—such as avoiding regulatory fines and preventing the disclosure of proprietary and trade secret information—provide additional, but difficult-to-quantify incentives for investing in secure content devices.

Topic 2: Policies and Procedures for Secure Content Management

Q2.2: How can a systems administrator monitor the effectiveness of current settings?

A: To monitor the effectiveness of a secure content appliance’s settings, administrators must establish a baseline of activity and then regularly examine the volumes and types of events on the network.

Establishing a Baseline

A baseline should be established when the appliance is first installed. The objective is to understand what constitutes “normal” activity on the network, including the number of emails sent and received, volumes of HTTP and FTP traffic, the number of spam messages, and malware applications detected. The baseline should include both absolute measures on protocols, such as the volume of HTTP traffic per day, and percentages, such as the percent of emails classified as spam.

In addition to these measures, the administrator should assess the accuracy of the content filtering to determine the rate of false positives, the number of messages incorrectly categorized as spam, attachments incorrectly identified as malware, and the rate of false negatives (that is, banned content that was not detected by the appliance). This work requires manual review of quarantined messages and careful tracking of malware infections.

Once the baseline is established, administrators should monitor the same measures over time using the same reports and analysis used to establish the baseline.

Reporting on Appliance Performance

The basic reporting tools at the administrator's disposal are:

- Browser-based reports available through the appliance
- Centralized reporting through ePolicy Orchestrator
- Email, Simple Network Management Protocol (SNMP), and Syslogging

Each type of reporting has its advantages and requires varying levels of configuration and integration.

Browser-Based Appliance Reports

The secure content appliance includes several reports providing summary and detailed information about traffic volumes and significant events. Although the details of each of these reports are more thoroughly described in the appliance documentation, let's take an overview look at example reports provided.

For example, a secure content appliance can provide information such as system status that includes details about protocols, hardware, load sharing, and general status information. The protocol status displays counts of the amount of traffic scanned, the number of viruses detected, emails deferred, spam messages blocked, and volumes of HTTP, FTP, and email traffic. You can also gather information about the status of each protocol and the workload processed. The hardware, load, and general status information display low-level details, such as the RAID status of hard drives and MAC addresses of the appliance's NICs (see Figure 2.2).

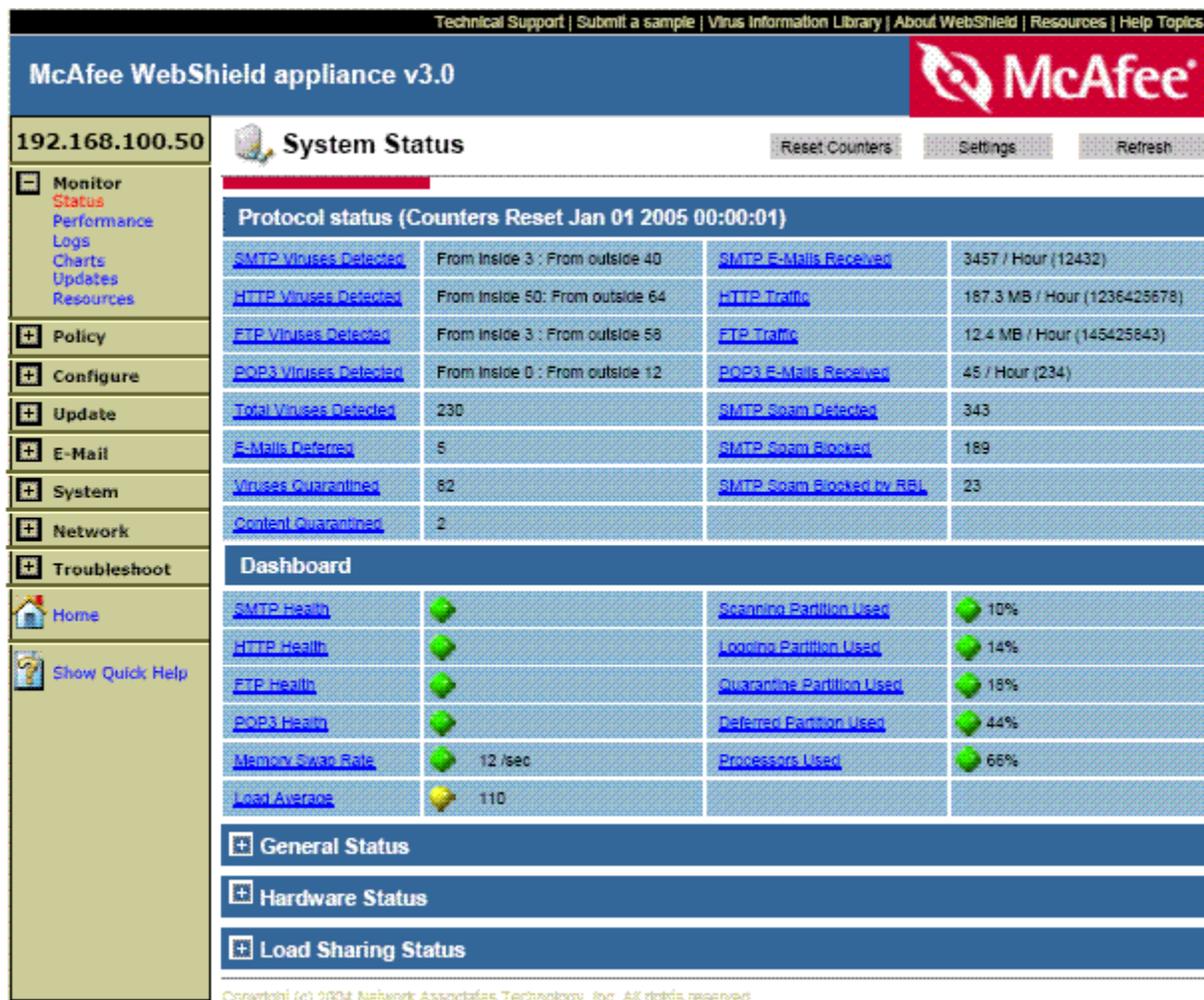


Figure 2.2: An example report provided by the secure content appliance.

Additional information provided by a secure content appliance includes Web pages that let administrators see the history of selected counters over a 24-hour period. For example, an administrator can track the number of email messages originating inside and outside the network (see Figure 2.3).



Figure 2.3: Examining a historical view of select counters.

In addition to storing performance detail on the appliance, administrators have the option of centralizing reporting with a third-party tool or basic network event monitoring tool such as SNMP traps and syslog. Events are filtered and sent to reporting tools based on three criteria:

- **Protocol**—Protocol filtering allows administrators to monitor events by traffic type; for example, all email traffic might be consolidated in a third-party tool-provided report, while FTP reporting is consolidated in a legacy syslog reporting application.
- **Severity**—Severity settings are used to control the volume of events by limiting reporting to only events deemed severe enough to warrant an administrator’s attention.
- **Event type**—Event type classifies events into antivirus, anti-spam, content filter, and system events.

Third-Party Tool Reporting

A third-party tool, such as McAfee’s ePolicy Orchestrator, centrally manages security policies and procedures across a network. These applications passively monitor activity on a network, prevent changes to system configurations, and ensure that workstations and servers remain in compliance with security policies. These tools provide consolidated reporting and library of predefined reports.

For example, when an ePolicy agent is installed on a secure content appliance, events are sent to the ePolicy Orchestrator and included in that application's reports. Reports specifically designed for the WebShield secure content appliance include:

- Content Filter Report by Rule
- Content Filter Report by Rule and Time
- Content Filter Report Rules Triggered
- URLs Blocked
- Viruses Detected
- Spam Detections by Appliance
- Top Ten Spammers
- Infection History

Other reports provide statistics on throughput and more detailed information on viruses and spam prevention. In addition to the predefined reports, administrators have the option of defining custom reports using Crystal Reports, an industry-leading reporting application.

Email, SNMP, and Syslogging

Many organizations may already have existing event reporting systems or practices in place based on email alerts, SNMP messages, and syslog. Third-party tools usually support email notification of an administrator when an event occurs.

SNMP is a protocol designed for sending messages from a managed device to a network management system. An agent resides on the managed device—in this case, the secure content appliance—and sends messages to a management device that logs the message. Syslog is an application that allows distributed systems to centralize their logging information.

 For more information about SNMP, see <http://www.snmpLink.org/>. For more information about syslog, see the Syslog RFC at <http://www.faqs.org/rfcs/rfc3164.html>.

Regardless of how administrators choose to log events and report on performance, the overall monitoring process is essentially the same.

Monitoring Tasks

There are several steps to maintaining an effective monitoring procedure.

Task 1: Establish a Monitoring Policy

The first step is to establish a monitoring policy that defines which measures will be tracked, how often measures will be taken, who is responsible for collecting measures, who is responsible for reviewing measures, who is responsible for acting on particular information, and the conditions that warrant the creation of a new baseline set of measures.

Task 2: Establish a Baseline

The baseline should be documented along with secure content policies and current appliance configurations. The baseline document should include:

- Volumes of traffic by protocol. Regular variations from the average, such as peak periods of FTP traffic at the end of the week caused by backup files copied to an offsite location, should also be noted.
- Number of email messages sent and received.
- The number and percent of total messages of viruses and spam and phishing messages detected over a period of time, such as a day or week. Track these by protocol as well.
- The number of misclassified spam and phishing messages, both false positives and false negatives.
- Number of URLs blocked.
- Number of reports of mistaken URL blocks.
- Number of reports of missed viruses and other malware.

The negative measures, such as missed viruses and mistaken URL blocks, will be relatively infrequent, so those should be measured over long time periods to get reasonably accurate measures.

Task 3: Analyze Reports

Once the baseline is established, administrators should review reports, event logs, and other information collected to monitor variations from the baseline:

- Substantial increase in virus detections
- Detection of new, high-volume spamming sources
- Users with unusually high number of blocked URLs
- Blocked sites with unusually large number of attempts to access
- Unexpected changes in traffic by protocol

Task 4: Verify Accuracy of Content Filtering

Checking the accuracy of content filtering is a time-consuming task and can rarely be performed as frequently as analyzing reports. As time permits, administrators should review message quarantines and reports of virus or other malware infections to determine the number of errors in the filtering process. Depending on the type of error, one of several actions may be warranted:

- Notifying the appliance's vendor about missed spam or emailing the miscategorized message to customer support
- Adding or removing names from white lists and black lists
- Educating users about browsing non-business-related Web sites
- Verifying the version and patch level of secure content appliance software and libraries to ensure the latest versions are used

In addition to the regular four tasks, administrators may need to redefine their baseline under some circumstances. Significant changes in network infrastructure and number of users, the introduction of new enterprise applications, or major organizational changes, such as a merger, typically justify creating a new baseline measure for secure content monitoring.

Topic 3: System Architecture and Secure Content Management

Q3.2: Why are desktop antivirus software and personal firewalls still needed?

A: There are two primary reasons for deploying desktop antivirus software and personal firewalls on networks that contain secure content devices:

- No security device can address all potential security threats; multiple layers of security are required to maintain network and system integrity
- Mobile devices are not protected by a secure content device when they are not connected to the network

All organizations are subject to the limits of any single security technique or tool and a growing number are faced with the challenge of managing and securing mobile devices.

Layered Security

The principal of layered security dictates that multiple forms of countermeasures are required to ensure the integrity of a network and related infrastructure. This approach is also known as defense-in-depth—security measures are placed throughout the network on the perimeter, servers, workstations, and mobile devices. Defenses also operate at different levels of the network; for example, network firewalls can filter based on protocols and ports and application firewalls can examine XML message content to identify invalid or unauthorized messages.

Example: Firewall Rules

Take a simple example. A company's network includes an IBM mainframe, a Microsoft SQL Server system, and a number of desktop and laptop Microsoft Windows clients. Let's assume the mainframe and SQL Server support business partners in a supply chain by providing access to parts and inventory information. Many users within the organization do not need access to those applications but their desktops and laptops are connected to the same network so they are exposed to the same traffic. By installing personal firewalls on those devices, the network administrators can block traffic on ports that must be open on the network but are not used locally. This action provides an extra layer of defense against threats that are propagated on those protocols or ports (see Figure 3.4).

Similarly, if a device were to become infected with a blended threat that included a keylogging program, a personal firewall could prevent the transmission of information over, for example, an Internet Relay Chat (IRC) protocol. There may be legitimate reasons for others to use that protocol, so the network firewalls would allow the traffic through. Using a personal firewall, one can configure finer-grained rules and better protect information flow.

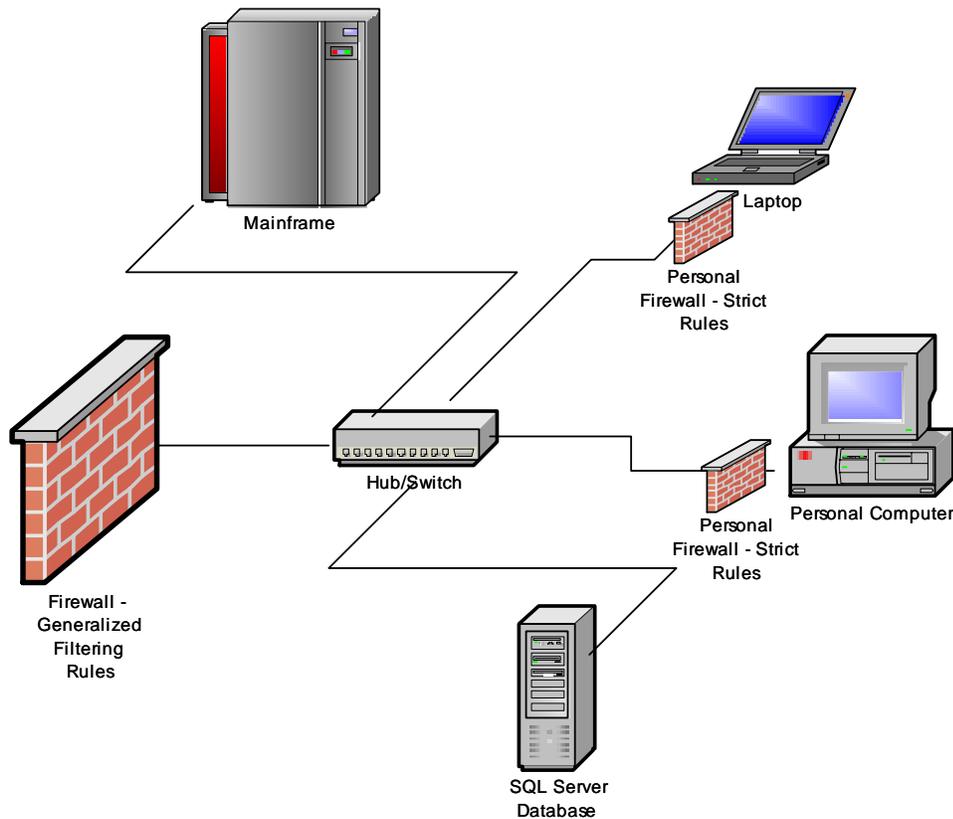


Figure 3.4: Defense-depth allows for both course-grained security for the overall network and fine-grained filtering localized to systems that require it.

Example: Antivirus Protection

Another example of the benefits of layered security involves the use of encryption. To ensure the privacy and integrity of messages, email users can encrypt a message and apply a digital signature to an email. Encryption scrambles the message so that it may not be read in transit to its destination. A digital signature is a string of characters appended to a message that is generated using a hash algorithm and a code known as the sender's private key. Upon receiving the message, the receiver uses another code, called the sender's public key, to decrypt the message and recalculate the digital signature. If the calculated signature matches the one in the message, the recipient knows the message is authentic and has not been tampered with.

Digital signatures and encryption are well-designed to meet the needs of privacy and integrity, but what happens when a virus is attached to a protected message? Secure content managers have a few options:

- The secure content appliance can reject the email and not deliver it to the recipient.
- The secure content device can remove the virus and send the rest of the message to the recipient. In that case, the content of the message has changed, so the recipient will not calculate the same digital signature; he or she will not know if any change other than removing the virus has occurred.
- The administrator can leave the virus embedded in the message and have a desktop antivirus program detect and remove the malware.

None of these options is ideal. Administrators must choose between denying a service to a user (either reliable delivery of email or message integrity checks) or allow a known piece of malware into the network (see Figure 3.5).

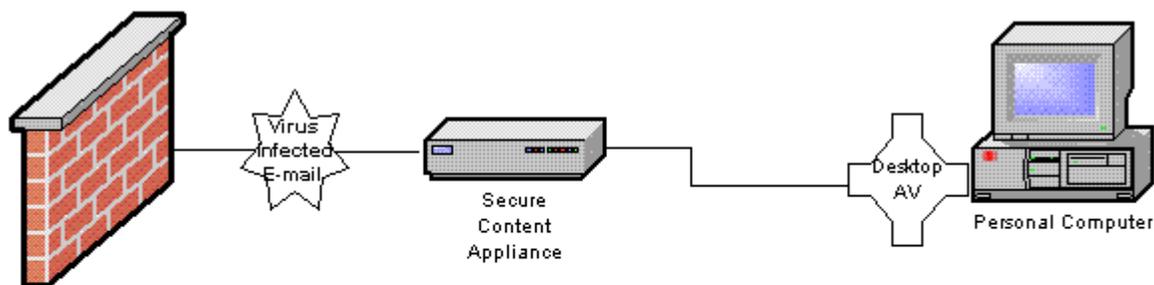


Figure 3.5: Encrypted, digitally-signed emails are sometimes better handled by desktop antivirus than by network-level scans.

By combining countermeasures at different points in the network and using multiple types of security tools, network and security administrators have more options for configuring security mechanisms that allow them to accommodate the needs of users and applications within the network. This type of layered defense also provides multiple points of protection should a single point become compromised. However, even within a well-secured network, mobile devices present security challenges.

Securing Mobile Devices

One of the advantages of using a network appliance for securing content is that any content entering or leaving the network is protected. Unfortunately, network devices do not always stay put. Laptops and PDAs with network access pose a particular threat to network security because they are allowed to physically disconnect and reconnect to the network, often at will.

Consider how easy it is to circumvent perimeter defenses with mobile devices. Imagine an employee who is blocked from browsing his favorite music sharing site during his lunch hour, so he decides to disconnect his laptop from the internal network, walk across the street to the local coffee shop with a WiFi hotspot, download music files (and unknowingly, some spyware), then return to the office to reconnect to the network. Spyware, that would have been blocked by the antispyware mechanism in the secure content appliance had the appliance not blocked the URL (another example of a layered defense) is now within the organization's network.

A single point of detection and prevention is not sufficient with mobile devices. As mobile devices will not always have the security services of the network available to them, these devices must have local versions of antivirus, anti-spyware, and personal firewalls.



For additional protection of mobile devices, consider a third-party tool such as McAfee ePolicy Orchestrator, which can ensure devices remain in compliance with security policies. If a device is changed and no longer in compliance, a third-party tool can enforce compliance and updates as well as notify administrators when threats or rogue systems attach to the network.

Layered security is considered a best practice among security professionals and should be practiced to levels appropriate to an organization's needs and capabilities. A secure content appliance adds a layer of protection and in fact uses multiple layers within itself (for example, malicious content missed by URL blocking can be caught by antivirus software). Mobile devices by their nature circumvent perimeter defenses such as firewalls and secure content devices. They must have their own localized security tools in addition to those available on the network.

Topic 4: Secure Content Appliance Performance

Q4.2: How can an organization protect against spyware?

A: Spyware, and its slightly more benign variation, adware, are programs that track user's activities and gather information without the user's knowledge. Unlike viruses and worms, spyware is not intended to cause direct and immediate damage to IT infrastructure. Instead, these programs are designed to collect information about users' identities, including account numbers, drivers' license numbers, usernames, passwords, Social Security numbers, and other personal details. This information is transmitted back to those who deployed the spyware.

Regardless of the original intent, spyware often leads to poor system performance and unstable systems. Multiple infections result in numerous processes consuming system resources and interacting in unpredictable ways. Some spyware changes system configurations, for example, turning off firewalls to ensure the spyware can function as expected. This behavior leaves infected systems open to further damage from other malware. Spyware is used to distribute advertisements, aid in identity theft, and perform affiliate fraud to steal fees from legitimate referring sites.

Keeping Spyware Out

The best way to deal with spyware is to keep it off your network. Perimeter defenses, including a secure content appliance, can block spyware as it enters the network. Spyware, like viruses and spam, can be detected using signature matching engines. This detection requires a library of up-to-date spyware signatures and a high-performance pattern-matching engine that can scan incoming traffic.

Define a Spyware Policy

Using the Internet inherently requires a balancing of risks and benefits. Spyware is one of those risks, and organizations should articulate the tradeoffs they are willing to make in balancing the utility of Internet services. A policy should include:

- A statement of acceptable use with regard to Internet sites. Spyware is often downloaded from popular entertainment sites and peer-to-peer networks.
- A description of the protocols that will be scanned, how spyware will be disposed of, and acceptable impact on network performance by spyware-scanning tools.
- A general approach to monitoring and event response. Procedures should be defined with detailed descriptions of how to respond to particular events; for example, if more than x pieces of spyware are detected from a site, the URL for that site will be added to the content filter blacklist.

Once a spyware policy is in place, its objectives should be implemented using a secure content appliance along with user education and maintenance procedures.

Scanning Multiple Protocols

Spyware can travel over multiple protocols. Someone browsing a peer-to-peer site opens up his or her system to downloading spyware at the same time. A blended threat piece of malware attached to an email can include keylogging and cookie tracking programs that record a user's online activity. Spyware can also come in a Trojan Horse, such as a utility downloaded via FTP that supposedly keeps your computer's clock synchronized with an atomic clock. It is essential to scan HTTP, FTP, SMTP, and POP-3 traffic as it enters the network.

Monitoring Spyware Detection

In addition to understanding the importance of blocking spyware, security administrators must grasp the volume of spyware reaching the network perimeter. Sudden spikes in spyware detection may indicate:

- An increase in spyware deployment on the Internet in general
- Better detection of spyware by the secure content appliance
- An increase in user browsing and downloading at sites from which spyware is launched
- An increase in spyware components included in blended threat viruses

We will likely have to live with the ever-increasing spyware deployments on the Internet for the foreseeable future; there is not much we can do, from a technical perspective, to slow that trend. Legislative and legal means might ameliorate that problem some. but we should assume spyware, like viruses, are a threat that cannot be eliminated but can be controlled. Better detection methods will also lead to increases in spyware detection and of course are welcome.

The third cause of increased spyware detection is best addressed by user education and clearly defined policies on legitimate use of IT infrastructure. Analysis of logs can identify the sites at which spyware is entering the network and the URLs can be blocked using content filtering functions of the secure content appliance.

As companies and other organizations get better at patching operating systems (OSs) and locking down networks, attackers will find other vulnerabilities to exploit in the never-ending cat-and-mouse game of creating new threats in response to countermeasures deployed by security professionals. Keylogging and URL hijacking are just two ways attackers can collect useful information—both can be done with spyware.

Understanding changes in the patterns of spyware detection can help administrators better pinpoint the specific threats to their organizations.

Educating Users

Like so many other areas of information security, user education is a key element of a successful strategy. Users must understand how spyware works, how it gets onto computers, and how to minimize the chance of getting stuck with it. When users understand this malware can steal personally identifying information, reduce system performance, and lead to unstable systems, they will have plenty of incentive to help address the problem.

Content Central

[Content Central](#) is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, learning about new development tools for Windows and Linux, or deploying new enterprise software solutions, [Content Central](#) offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

Download Additional eBooks!

If you found this eBook to be informative, then please visit Content Central and download other eBooks on this topic. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to other great IT eBooks and video guides. Please visit: <http://www.realtimerepublishers.com/contentcentral/>.