realtimepublishers.com™

Tips and Tricks Guide™ To

Secure Content Appliances

McAfee® Proven Security™

Dan Sullivan

Introduction to Realtimepublishers

by Sean Daily, Series Editor

The book you are about to enjoy represents an entirely new modality of publishing and a major first in the industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical technology topics—at no cost to the reader. Although this feat may sound difficult to achieve, it is made possible through the vision and generosity of a corporate sponsor who agrees to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these publications does not in any way diminish their quality. Without reservation, I can tell you that the book that you're now reading is the equivalent of any similar printed book you might find at your local bookstore—with the notable exception that it won't cost you $30 to $80. The Realtimepublishers publishing model also provides other significant benefits. For example, the electronic nature of this book makes activities such as chapter updates and additions or the release of a new edition possible in a far shorter timeframe than is the case with conventional printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that our books are by no means paid advertisements for the sponsor. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100 percent editorial control over the content of our titles. It is my opinion that this system of content delivery not only is of immeasurable value to readers but also will hold a significant place in the future of publishing.

As the founder of Realtimepublishers, my *raison d'être* is to create "dream team" projects—that is, to locate and work only with the industry's leading authors and sponsors, and publish books that help readers do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please send an email to feedback@realtimepublishers.com, leave feedback on our Web site at http://www.realtimepublishers.com, or call us at 800-509-0532 ext. 110.

Thanks for reading, and enjoy!

Sean Daily
Founder & Series Editor
Realtimepublishers.com, Inc.

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

Copyright Statement

[**Editor's Note:** This eBook was downloaded from Content Central. To download other eBooks on this topic, please visit http://www.realtimepublishers.com/contentcentral/.]

Topic 1: Business Justification for Secure Content Appliances

Q1.1: Why does an organization need another security device for securing content?

A: Security professionals are not at a loss for tools and applications to thwart threats to their IT infrastructure. So why do we need to consider yet another kind of application, this time for securing content?

The simple answer is that security tools are tuned for particular problems and no one tool will ever address all security needs. As new threats emerge, so will tools that address those threats. Consider some types of security tools and applications commonly found in enterprise IT environments:

- Network monitoring tools—These programs capture network traffic and allow network administrators to analyze operations on their networks. These are useful for detecting port scans, identifying the source of unusually large volumes of traffic (for example during a Denial of Service—DoS—attack), or probes, such as CGI attacks.
- Firewalls—This ubiquitous security device is a basic tool for controlling the flow of traffic into and out of a network. Firewalls have evolved from being simply a perimeter device to a desktop application that provides protection for individual computers.
- Vulnerability assessment—One of the earliest and best known vulnerability assessment tools, SATAN, garnered mixed responses from security professionals. It provided systems administrators (and hackers) with a single tool to probe computers for a large number of known vulnerabilities, such as unpatched applications. Today, vulnerability assessment tools are considered another essential tool in the security analyst's toolbox.
- Intrusion Prevention Systems (IPS)—These systems began as Intrusion Detection Systems (IDSs) that used sophisticated rules and patterns of network traffic to detect attacks on a network or server. Instead of just detecting attacks, IPS devices can stop them as well by closing down sessions, blocking traffic from specific Internet addresses, and other methods. IPSs can work on either a network or host level.

- Antivirus software—As the name implies, antivirus software identifies and removes malicious code that attaches itself to other programs. Like other security applications, antivirus software has evolved to counter related threats including worms, Trojan horses and blended threats (this type of malware includes multiple malicious programs, such as viruses, worms, keyloggers, file transfer programs, Internet chat clients, and so on).
- Identity management systems—Identity management is the practice of tracking and controlling access to information assets based on a person's—or in some cases, an application's—privileges. Identity management systems combine the features of authentication systems, such as Single Sign-On (SSO) applications, with authorization systems that track a person's roles and privileges.
- Encryption applications—Encryption programs encode data so that only those authorized to see the data may have access to it. This type of application is a basic security technology used in Web protocols, such as SSL; authentication systems; and end-user programs, such as Pretty Good Privacy (PGP). As more and more data is stored on mobile devices and shared storage arrays, such as SANs, encrypting data on disks is becoming more common.

There are other, more specialized tools and applications for security professionals but this list gives a sense of the breadth of security devices already deployed within enterprise environments. Do you really need another security tool thrown into the mix? Couldn't the need be filled by an existing tool or combination of tools?

The answers are, respectively, yes and no. Yes, there is a need for another type of tool to meet threats that are conveyed through content, such as email messages and Web content. The tools mentioned in the previous list are designed and configured to address a narrow range of problems, such as blocking access to ports. With the exception of antivirus software, the tools mentioned do not target the high-level content that moves in and out of a network.

To secure content, you need an application specifically designed for that problem. The characteristics of an appropriate tool include:

- Operates at the application layer of the network—As Figure 1.1 shows, network operations are divided into seven logical layers. Security tools typically function best at one layer; for example, packet sniffers work at the data link and network layers while identity management systems work at the application layer. To effectively analyze the threat embedded in content, the tool must function at the application layer.
- Analyzes all content entering or leaving the network—Email, instant messages, and Web content are the most likely means of brining malware into an enterprise network. Scanning and removing viruses, worms, Trojan horses, and other threats after they reach the server or desktop is one approach; a better method is to prevent it from entering the network at all.
- High-performance analysis—Securing content should not slow email or Web services. Secure content applications should analyze content and allow permissible content to reach its destination with virtually no impact on transmission times.

- Highly accurate analysis—The process for identifying threatening content should have low rates of false positives (categorizing allowed content as not allowed) and false negatives (categorizing non-allowed content as allowed).
- Tamper-proof—The system that is analyzing content should not itself become compromised by malware or attacks.

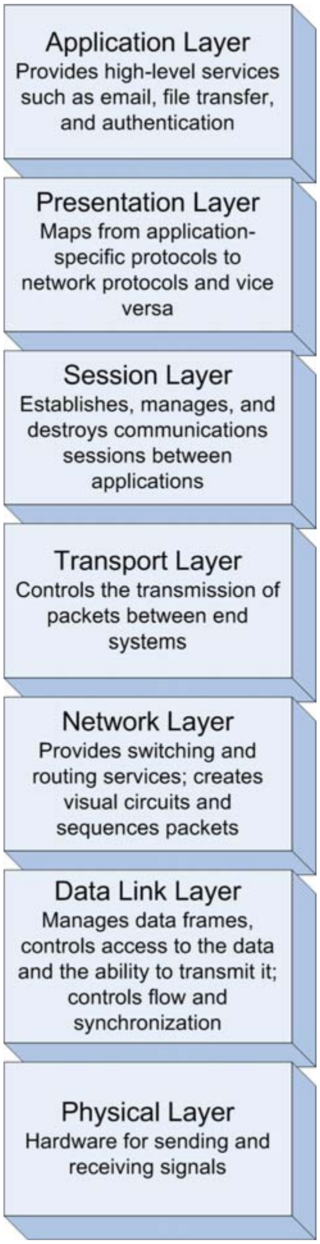
Application Layer
Provides high-level services such as email, file transfer, and authentication
Presentation Layer
Maps from application-specific protocols to network protocols and vice versa
Session Layer
Establishes, manages, and destroys communications sessions between applications
Transport Layer
Controls the transmission of packets between end systems
Network Layer
Provides switching and routing services; creates visual circuits and sequences packets
Data Link Layer
Manages data frames, controls access to the data and the ability to transmit it; controls flow and synchronization
Physical Layer
Hardware for sending and receiving signals

Figure 1.1: The OSI network model includes seven logical layers; security measures must address threats at every layer.

The best method for achieving all these objectives is to deploy a secure content application, service, or appliance.

Q1.2: How does a secure content device complement other security devices?

A: A secure content device compliments several of the security devices mentioned in question 1.1, including:

- Desktop antivirus
- Firewalls
- Intrusion prevention systems (IPSs)
- Policy administration

No single security device can address all security threats; in addition, some degree of overlap provides supplementary protection to an enterprise's information infrastructure.

Desktop Antivirus

Both secure content devices and desktop antivirus software scan for malware—why use both? Ideally, viruses, worms, Trojan Horses, and other malware would never enter an enterprise network. Secure content devices scan network traffic that is likely to carry malware payloads—especially email, file transfer, and Web-based traffic. Secure content devices can identify and block malware at the perimeter of the network; however, there are other means for malware to enter the organization.

Mobile devices, especially laptops, are not continuously protected by secure content devices. Employees take laptops home to insecure home networks. Sales staff travels with laptops, connecting to the Internet from client sites, airports, coffee shops, and other points beyond the enterprise's control. These mobile devices must be protected while they are disconnected from the enterprise network by desktop antivirus software.

Also, although the majority of malware threats propagate through networks, they can still be transferred through shared storage devices. The earliest viruses traveled on floppy disks that were passed between PC users. Today, flash memory devices have largely replaced floppy disks as the preferred storage device for transferring data, but the problem remains the same: infected programs and documents can easily move from one computer to another. Desktop antivirus software can readily scan flash drives and eliminate known malware before it can infect another device.

Firewalls

Firewalls are the standard means for controlling the type of network traffic that enters and leaves an enterprise network. Firewalls are configured to allow traffic on necessary ports—for example, TCP port 80 for HTTP, 21 for ftp, and 23 for Telnet. When a service provided by a port is not needed, the port is blocked. Firewalls provide a first line, course-grained line of defense; finer-grained security is required in addition.

The basic limit of firewalls is that they work with the structure of network traffic, not its content. For example, an infected file can be transferred into a network using ftp as long as the sender authenticates with the ftp server (assuming anonymous logins are not allowed) and the sender does not violate other basic constraints, such as exceeding storage limits. Similarly, a malicious application could use HTTP tunneling to transfer malware or use otherwise blocked protocols to communicate with malware already infecting a local device. This situation is especially problematic because of the high volume of HTTP traffic in enterprises. In one study of a large institution, more than 40 percent of all incoming and 90 percent of all outgoing traffic used HTTP.

📖 For more information about HTTP tunneling and detection methods, see “Detecting HTTP Tunneling Activities” at http://www.ll.mit.edu/IST/pubs/Pack-IEEE2002.pdf.

Firewalls provide essential security functions but alone they are not enough. Secure content devices examine incoming traffic once it has passed the firewall (or before it reaches the firewall in the case of outgoing traffic). Rather than examine just the structure of the traffic (for example, “this is an SMTP packet”), it examines the content (“Lose weight while you work at home”) allowing the secure content device to identify spam and other unwanted content. IPSs are closely related to firewalls.

Intrusion Prevention Devices

There are two types of intrusion prevention: host-based and network based. Host-based IPSs protect individual servers and workstations from attacks that cannot, or at least are not, stopped by perimeter defenses, such as firewalls. Host-based IPSs detect anomalous behaviors on servers as well as truly suspect actions, such as an attempt to write a file from a Web browser or the escalation of local privileges.

Host-based IPSs can do some things that other network-based approaches cannot. For example, a host IPS can analyze the content of an encrypted message after it is decoded; a secure content device that monitors network traffic does not have access to the decrypted traffic.

Network-based IPSs use signatures, or patterns of traffic, to detect anomalies in network activity. As with host-based IPSs, there are some attacks that are difficult at best to detect with other methods. One of these attacks is known as Address Resolution Protocol (ARP) poisoning.

ARP is used to map from IP addresses to MAC addresses, the unique physical address on a network interface. ARP, like other Internet protocols, is quite trusting. Devices do not need to authenticate to send an ARP message to another device; any device (or attacker) can send a message telling a server that IP address A maps to physical address B. The server will store that information in an ARP table and use the physical address when addressing messages to IP address A. With ARP poisoning, an attacker can effectively re-route traffic away from a legitimate device to another, compromised machine. Network-based intrusion detection can detect this type of attack in the lower levels of the OSI network model.

Complementing Secure Content

Both host-based and network-based intrusion detection provide defenses against particular types of attacks. Both protect information infrastructure, such as the integrity of network routing and the operating system (OS) access controls. These complement secure content devices that analyze the content that depends on that information infrastructure.

Policy Administration

The foundation of a secure infrastructure is a set of well-defined policies governing several aspects of information security, including:

- Authentication
- Authorization
- Vulnerability scanning
- Database access
- Remote access
- Password
- Wireless networking

Information security policy administration tools are relatively new but are emerging to address the difficulties in managing silos of security. One of the key reasons to use policy administration is to centralize management of policies and reporting. This complements secure content devices by providing the means to report on events and defined policies within the secure content device.

> 🕮 For more information about security policies, see the SANS Security Policy Project at http://www.sans.org/resources/policies/.

Deploying multiple defensive layers is a standard practice in information security. Some countermeasures, such as network intrusion detection and firewalls, protect the transmission of network traffic. Host-based intrusion prevention and desktop antivirus software protect the integrity of OSs, applications, and data. Secure content devices protect against the introduction of malware, spyware, spam, and phishing attacks from entering a network. Together these and other tools provide a security infrastructure that can provide a layered defense and address a multitude of threats.

Topic 2: Policies and Procedures for Secure Content Management

Q2.1: What topics should be addressed in secure content policies?

A: Content policies can be organized around two dimensions: first, services provided on the network, including:

- SMTP email
- POP3 email
- HTTP
- FTP

Second, based on threats, such as

- Spam
- Viruses and other malware
- Disclosure of private or confidential information
- Banned content
- Use of time-wasting Web sites

There is clearly overlap, for example, between how spam is handled in an SMTP email system and a POP3 email system. At the same time, different protocols or services have different vulnerabilities and require different types of monitoring. For example, private or confidential information can be transmitted via email or FTP; however, FTP's long history of vulnerabilities warrants attention to those conditions.

Policy Types

Polices are rules applied to groups of users. Policies can be either all users, known as global policies, or non-global policies, which apply to groups of users. It is preferable to place as many content rules in global policies as possible. Non-global policies should be used for exceptions to the rules. For example, as a global policy, you might limit the size of attachments to 10MB but want to allow attorneys and others in the legal department, who tend to work with large volumes of documents, to accept attachments as large as 20MB.

Non-global policies are assigned to groups of users. In general, the groups should be logically related by their organizational function rather than common characteristics of the policies that are applied to them. For example, both the legal and marketing departments might be allowed to receive attachments as large as 20MB. However, that similar requirement is basically a coincidence; tomorrow the requirement of one of the departments may change. Thus, an administrator would want to establish separate legal and marketing groups rather than a single 20MB Attachment group.

Content Policies

Content policies need to address a range of topics, including scanning, encryption and digital signatures, disclaimers, and content size. Scanning is a broad set of activities geared toward ensuring unwanted content is not allowed into an organization and protected content is not allowed out. Scanning policies should define rules for

- Antivirus
- Anti-spam
- Banned words and phrases
- Private, proprietary, and trade secret information

Antivirus scanning will use both signatures (binary patterns indicating a virus or other malware) and heuristic analysis (general patterns that indicate the existence of malware, such as an attempt to modify files with prior user command) to detect malware. Antivirus policies should define how an infected file is handled. It could be deleted, quarantined, or cleaned and passed through. Often the best option is to clean and pass through; the recipient gets the message but not the malware. One drawback to this approach is that the message is changed and so any associated digital signature will no longer match when a new signature is calculated upon arrival. Antivirus policies should include frequent updates of virus signature files as well as patches and upgrades to the virus detection engine.

Anti-spam scanning policies need to balance the need for comprehensive rules that capture most spam while not restricting access to legitimate email with false positives. To ensure the best possible spam protection, keep spam files up to date. Also, use the white list feature, Permit Sender, to list senders allowed to bypass spam scanning, which prevents the chance of false positives (legitimate email classified as spam) from trusted senders. Similarly, blacklists are used to prevent known spammers from sending messages. This setup prevents potential problems, as spammers routinely hijack email accounts so that legitimate emailers may have their messages blocked.

Policies should define how spam should be handled once it is identified: it can be refused, deleted, or forwarded to a special recipient who is monitoring spam activity on the network. Another option is to add a message to the email indicating the message is potential spam and let the recipient decide how to deal with the message.

Both incoming and outgoing messages should be scanned for banned words and phrases. Content rules should include checks to words or phrases in email messages that might be considered as contributing to an offensive or hostile work environment. Outgoing messages should be checked for private, proprietary, or other confidential information. This setup can require careful crafting of rules.

Consider a healthcare provider that uses email to transmit patient information between doctors. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) regulation places restrictions on how protected health information is shared among doctors, insurances companies, and others involved in healthcare. Sending an email with an attached patient record might violate HIPAA unless the recipient is allowed by the patient to receive that information. Of course, the email system or content filter will not have access to databases or paper files that identify legitimate recipients of protected healthcare information. In such cases, a provider may require that all patient records are sent from a single email account that is used only by patient records personnel. A set of content rules could then be defined to block the transmission of the message with indicators of protected patient information, and forward it to an email account for further review (see Figure 2.1).

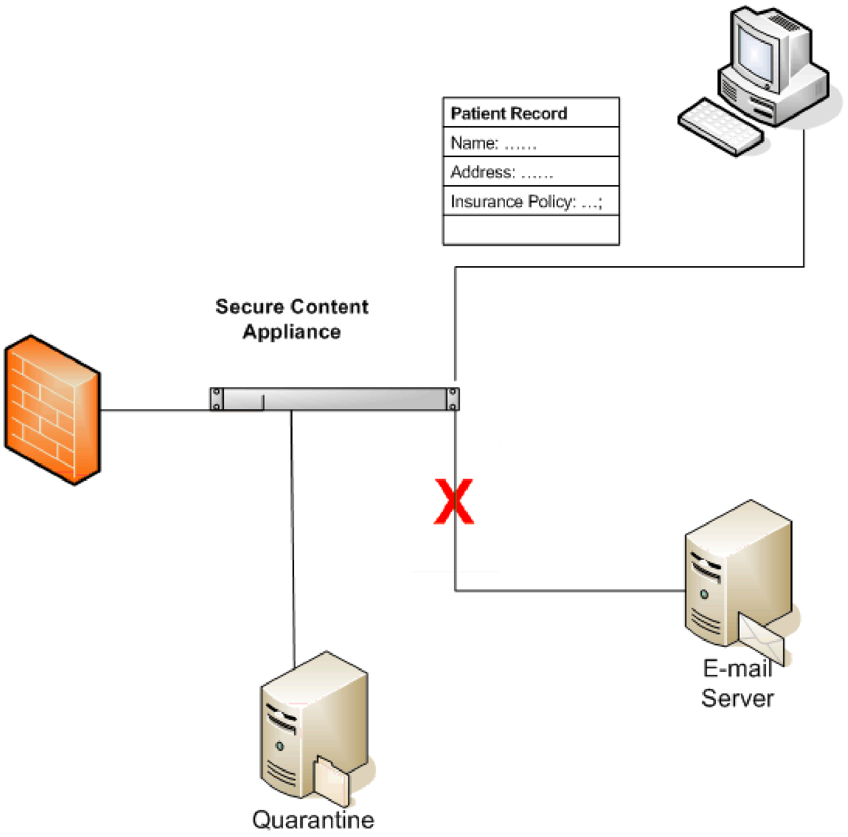

Figure 2.1: Quarantine areas can be established to retain sensitive information so that it can be reviewed before sending it outside the organization.

Proprietary and trade secret information is protected in a similar way. Policies should include rules for blocking or quarantining confidential information before it leaves the email system. This setup will require the custom definition of a dictionary of terms and phrases, such as project and process names, that are kept confidential.

Another area that should be addressed in content policies is time-wasting Web sites. Although many organizations have no interest in blocking occasional visits to news sites, those same organizations have no need for gambling or adult sites. Policies should be defined that block access to known time-wasting, non-work–related sites. Content policies cover a broad range of topics but are essentially rules for filtering what you would want coming into or going out of your organization.

Topic 3: System Architecture and Secure Content Management

Q3.1: Where should a secure content appliance be placed?

A: Secure content appliances are used to control what is allowed to enter and leave an organization's network. It follows logically that the device should be located on the perimeter of the network. Perimeters can use a single layer of defense with a single level of firewalls that block ports and filter network traffic at the lower levels of the OSI network model (see question 1.1 for more information about the OSI network model). A common configuration creates a multi-level perimeter known as a DMZ (de-militarized zone).

DMZs use multiple network segments to create three zones: the external zone, which includes the Internet; the internal zone, which includes an organization's network, servers, desktops, and other devices accessible to the internal network; and the DMZ, which lies between the internal and external zone.

Typically, the Web servers are located in the DMZ. These servers need to be accessible from the Internet but also protected from it. Applications running on the Web server invoke applications and services running on servers on the internal network. For example, an application running on the Web server may query a customer database, located in the internal zone. Internet users have no direct access to the database server; all interaction is through a proxy application on the Web server. This configuration balances the need for accessibility with the need for controlled access to the mission-critical servers (see Figure 3.1).

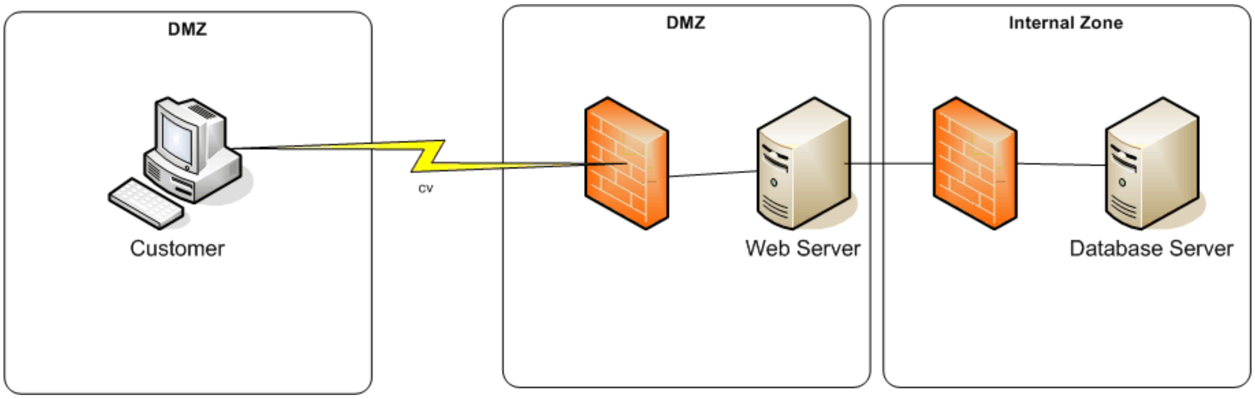

Figure 3.1: DMZs provide additional protection of mission-critical servers by limiting access to those servers to trusted proxies in the DMZ.

Secure Content Device Operational Modes

In addition to the existing configuration of a network, a secure content administrator needs to consider how the device will be configured. There are three options:

- Explicit proxy mode
- Transparent router mode
- Transparent bridge mode

The choice of mode determines whether other devices are aware of its use, how the secure appliance is configured and connected to the network, and how much configuration work is required during installation. The focus here is on how the device is connected to the network.

Explicit Proxy Mode

In explicit proxy mode, servers that communicate with the secure content device are configured to communicate directly with the device. For example, incoming mail is routed from the Internet to the secure content device and then passed to the internal email server. When in explicit proxy mode, only HTTP, SMTP, POP3, and FTP traffic should be routed to the secure content device; all other protocols are refused by the device.

In explicit proxy mode, administrators have great flexibility in placing a secure content server. The one configuration rule is that the secure content appliance must be located behind a firewall; other than that, the device can be placed anywhere in a DMZ or internal network.

The reason for the flexibility in positioning the devices is that other devices that use the secure content device are configured to explicitly send traffic to and receive traffic from the device. For example, in a switched network, the secure content device can be connected to any router or switch in the network. Although, the device can be placed anywhere in the network, some positions will still be better than others.

Consider the flow of traffic. As all incoming and outgoing email and Web traffic will pass through the device, it should be located in a segment that minimizes additional traffic. For example, if an email server and Web server are in the same network segment, it makes sense to position the secure content device there because traffic will eventually flow into that segment to reach the email and Web servers.

Also consider the bandwidth utilization on a segment. If network traffic is near capacity on a segment, adding a secure content device to that segment will only increase the network load.

Transparent Router Mode

In transparent router mode the secure content device acts as both a content filter and a router. As in explicit proxy mode, the secure content device should be behind the firewall.

In transparent router mode, clients are not reconfigured to send and receive traffic to and from the secure content device. Only the firewall and other routers must be reconfigured to direct traffic to the secure content device. This setup eliminates the need to change client configurations but it does limit options for placing the device.

It is recommended that a secure content device in transparent router mode be placed between the firewall and a router. In cases in which the secure content device is the only router, it should be placed immediately after the firewall.

Transparent router mode is recommended for networks that use firewall rules to control traffic. In explicit proxy mode, packets are redirected to the secure content device making the client's IP address unavailable to the firewall rules engine (see Figure 3.2).

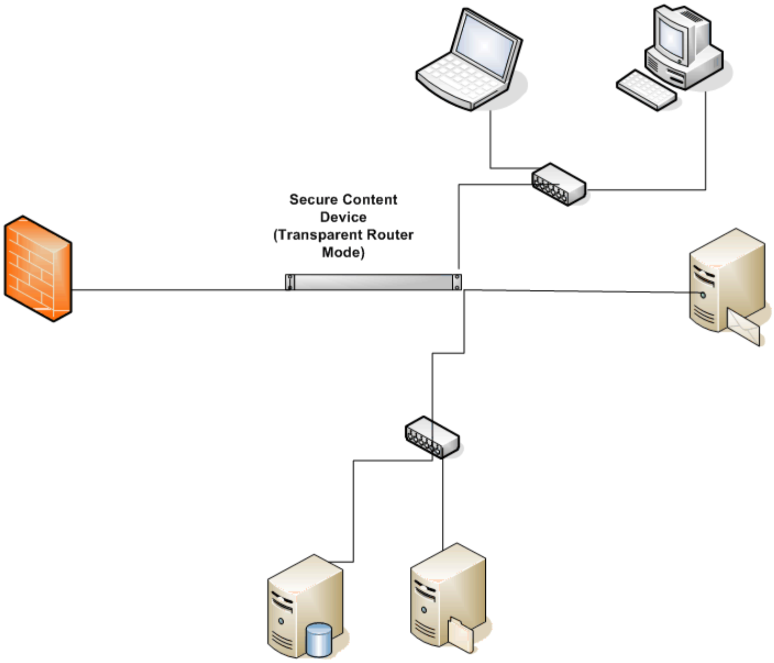

Figure 3.2: In transparent router mode, the secure content device functions as both a content filter and a router.

Transparent Bridge Mode

Transparent bridge mode is similar to transparent router mode, but simpler. As Figure 3.3 shows, the secure content device does not route traffic, it simply passes traffic between two network segments. No clients, firewalls or routers must be reconfigured. In transparent bridge mode, the secure content appliance should be placed between the firewall and the router.

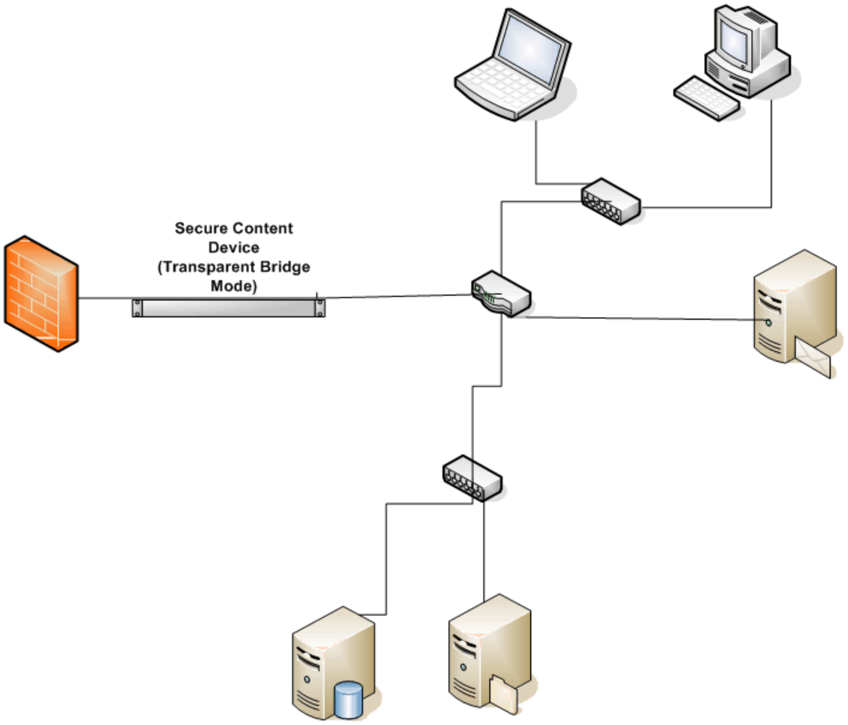

Figure 3.3: In transparent bridge mode, the device joins two segments of a network and passes traffic between the two without routing.

Secure content appliances should be placed inside a well-configured firewall. Administrators should also determine which mode the appliance will use. Transparent bridge mode is the easiest to configure; however, all traffic will pass through and be filtered. In high-traffic networks, you may find better performance by configuring the appliance in explicit proxy mode and sending only relevant traffic (for example, HTTP, FTP, SMTP and POP3). Of course, if the routing features of the appliance are used, the appliance should be placed at the junction of two or more network segments.

Topic 4: Secure Content Appliance Performance

Q4.1: What are threats to content and information assets must organizations address?

A: The major threats to information assets include:

- Viruses, worms, and other malware
- Spam
- Phishing scams
- Spyware

Left unchecked, these threats can leave organizations with compromised computers, security breaches, loss of information, identity theft victims, and reduced ROI on information technology (IT) investments because resources are consumed with non-business related content.

Viruses, Worms, and Other Malware

Malicious programs have evolved from small, machine-language programs propagated by sharing floppy disks to sophisticated collections of programs that can gain control of systems, steal personal information, and replicate rapidly. This malicious software, or malware, falls into several broad categories:

- Viruses
- Worms
- Trojan horses
- Keyloggers
- Backdoors
- Rootkits

Viruses

Viruses are malicious programs that attach themselves to other programs to execute and propagate. Viruses can run either as executable programs or as macro-viruses embedded in applications, such as Microsoft Word. Viruses consist of two basic parts, a replication mechanism and a payload, the destructive part of the virus.

In the early days of antivirus protection, vendors could discover identifying patterns within a virus that uniquely identify that virus. This identification allowed researchers to create libraries of signatures to detect a virus that could then be removed or at least quarantined. Virus writers responded with encryption to hide the tell-tale signs of a virus, then with the development of mutating viruses, which change in structure but retain the same functionality.

Mutating viruses require a radically different detection approach: rather than look for the same pattern, antivirus researchers must look at the behavior of a program to determine whether it is malicious. Some indicators are commands to change a file without first being commanded by a user and writing to particular memory locations used for low-level system tasks.

Worms

Worms are similar to viruses in that they are malicious programs that self-propagate. Unlike viruses, worms do not depend upon other programs. Worms exploit vulnerabilities in systems and move, sometimes quite rapidly, from one system to another.

One of the most famous worms is SQL Slammer, which flooded large sections of the Internet within 15 minutes of it release. SQL Slammer exploited a vulnerability in Microsoft's database, SQL Server, forcing unpatched servers to generate database server requests sent to random IP addresses. The worm was not sophisticated in how it targeted other victims; instead it depended upon flooding the Internet with packets knowing at least some of the requests would target a SQL Server database.

> 🕮 For a description of the spread of the worm from the perspective of an Internet operations center, see Paul Boutin's "Slammed!: An inside view of the worm that crashed the Internet in 15 minutes" at http://www.wired.com/wired/archive/11.07/slammer.html.

SQL Slammer demonstrated the need for both patching and content filtering. Once a malicious piece of software is released on the Internet there may be little time to craft a custom response.

Trojan Horses

Trojan horses are programs that appear to serve one purpose and actually perform another. A program that promises to synchronize your desktop computer's clock with a highly accurate atomic clock but also collects personal information about your surfing habits is a Trojan horse.

Trojan horses, unlike other malware, may be installed intentionally on a system. A user may not realize that a peer-to-peer (P2P) file sharing application he or she downloads to share music files also contains a program to capture usernames and passwords that are then transmitted to an attacker's server. Again, content filtering can help identify malicious programs that are brought into a network intentionally, albeit, under false pretenses.

Keyloggers, Backdoors, and Rootkits

Keyloggers, backdoors and rootkits are some of the most dangerous forms of malware. Keyloggers simply record keystrokes and send the captured information back to an attacker for analysis. Text scanning programs can quickly analyze those files for personal information, such as Social Security numbers, bank account numbers, credit card numbers, as well as usernames and passwords.

Backdoors are changes to a system's configuration and create a way for an attacker to gain control of a system. Creating an administrator or root account controlled by the attacker is one example of a backdoor.

Rootkits allow attackers to gain control of a system but also hide the attacker's tracks, making detection especially difficult. As rootkits can gain control over any aspect of an operating system (OS), the only way to ensure the malware is eliminated is to format all drives and restore the system from a known uninfected backup.

Spam

Spam is unwanted, unsolicited email. Spam not only wastes the time of end users but also taxes system resources, such as storage and bandwidth. In addition, it places demands on email administrators who have to manage the additional volume of email.

The key to controlling spam is to identify it as it comes into the network and deleting or quarantining it. This ability assumes that the spam detection software is highly accurate: it does not identify legitimate mail as spam (known as a false positive) or miss identifying spam (a false negative).

Phishing scams

Phishing scams are cons that use email to lure victims into divulging personal information of sending money to a bogus charity or get rich scheme. Phishing scammers masquerade as legitimate businesses (banks, eBay, and PayPal are favorites of phishing scammers) by sending emails with official logos and urgent messages about the need to update account information or verify personally identifying information.

Once they have the victims' attention, scammers lead victims to Web sites that appear legitimate but are actually phony versions set up to capture information such as bank account numbers, usernames, and passwords. Phishing scams are difficult to detect and user education is one of the best defenses for this threat.

📖 To learn more about phishing, see the Anti-Phishing Working at http://www.antiphishing.org.

Spyware

Spyware, sometimes called adware, is malicious code that captures information about users and their online activities without their knowledge. In addition to violating users' privacy, spyware can negatively impact system performance. Consequences of spyware include:

- Loss of privacy and identity theft
- Decreased system performance
- Disabling security software, such as antivirus and firewalls, which leaves systems vulnerable to other malware infections
- Displaying unwanted pop-up advertisements
- Changing host files and other networking files causing users to unintentionally navigate to spyware-promoted sites.

As with other malware, spyware can be removed, but it is better to prevent its introduction in the first place by filtering content and blocking spyware.

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.realtimepublishers.com/contentcentral/.