Global Information Assurance Certification Paper

Introduction to Enterprise Content Filtering

Bradley Cohen
SANS Security Essentials
GSEC Practical Version 1.2c

Content Bourne Threats

Every day one reads of new threats and attacks on the electronic transmission of data that is so crucial to business. These threats can take several forms such as viruses, Trojans, denial of service, and malicious executable code. Any one of these threats can literally stop all electronic transmission of data through e-mail, ftp, and the web. Once an attack has been discovered it also takes a great deal of staff resources to recover from. It could be hours, or days, or even weeks before normal business can resume.

So how do these threats get into a tightly controlled corporate environment, especially since most corporate environments have a security policy, a firewall and desktop virus protection? The answer unfortunately is: quite easily in most cases. Viruses and Trojans are most commonly transmitted through files attached to E-mail, and easily hide in MS-Word or Excel documents. Desktop virus protection software is only effective if the virus signatures are maintained on every computer in the organization including those that connect to the corporate network remotely from travelers and home offices. This is a daunting task for most organizations. Malicious applets are easily launched from websites. Denial of service attacks can be launched from a variety of methods.

Misuse of Resources

Misuse of an organizations resources can be both intentional and unintentional. One common type of misuse is using the organizations Internet connection for personal use. It is common for employees to surf the web for personal use at times; in most cases this is not a problem, and can in fact save time over the long run. However, there are times when an employee will misuse this privilege by either surfing for excessive amounts of time, or viewing inappropriate content and possibly exposing the organization to litigation by exposing other unwilling employees to the material. Some other common examples of misuse include day trading, sending very large files, and chat gateways. Not only do these take up valuable bandwidth, but they also keep employees from being productive. Sometimes if the bandwidth drain is too great, the result might even be a sort of self-denial of service attack. Another threat to productivity is unsolicited e-mail containing advertising, hoaxes, jokes etc. commonly referred to as Spam. Many of us see jokes circulating around via email and take a few minutes to read them. What we don't often realize is that if the amount of time and resources devoted to these jokes were multiplied by the number of people receiving them, the result would be astronomical.

While Spam is mostly thought of as an inbound problem, it is important to understand that persons within an organization often perpetuate Spam by resending hoaxes and jokes to friends and colleagues both inside and outside of the enterprise. Also originating from inside the organization are messages containing inappropriate language or material that

might expose the enterprise to litigation and damage reputation. Intellectual property as well as sensitive data and applications are also at risk of leaving the enterprise through electronic transmission.

Content Filtering Concepts and Terminology

Content filtering is the process of examining incoming or outgoing data for a variety of problems and attributes. Action can then be taken based upon the type of problem or attribute encountered. A key feature of content filtering is the ability to customize the list of problems and attributes and what actions should be taken on them. This customization normally can be modeled after elements contained within the enterprise security policy.

Here is a list of some commonly used concepts and terms relevant to further discussion of Content Security.

- Forward – The process of forwarding clean data to the recipient.
- Quarantine – Placing infected or suspect data in a separate holding area for further inspection and treatment.
- Park – Temporarily holding data that can be delivered at a later time. For example: a very large email message containing attachments may be parked so as to not clog up the network during peak hours.
- Clean – The process of removing a virus or piece of malicious code from data.
- Block – Disallowing access to data that may contain malicious or inappropriate content.
- Delete – The process of purging infected, malicious, or inappropriate messages and data.
- Inappropriate Content – This can be defined as any type of data that goes against the policy of an organization. This type of data may be free of viruses and malicious code. For example web sites containing: pornography, hate mongering, drug culture, chat gateways, games, etc. Inappropriate content is defined by the organization and will differ from place to place.
- Lexical Analysis – The process of examining text in incoming and outgoing messages and data for specific words or phrases. For example a company may want to look for the word "Resume`" in all outgoing mail.
- Spam – In the context of content security this is the practice of sending unsolicited material such as advertisements, hoaxes, jokes etc. to many recipients.

Content Filtering Software

When one hears the term *Content Filtering* one thinks of software that is commonly available to control access to the web by children. Parents and schools deploy software titles like Net Nanny for this purpose.

There are families of software products aimed at the enterprise that can help mitigate most content borne threats. Not only will it filter inappropriate web content, but it will also filter almost all kinds of inbound and outbound content as well. Content filtering software works by scanning e-mail messages, e-mail attachments, web pages, active-x, and Java applets for possibly hostile or inappropriate content before they enter and exit the internal network. While there are variations on how this is implemented within a network, they mostly follow Figure 1 Typical Content Security Network Implementation.

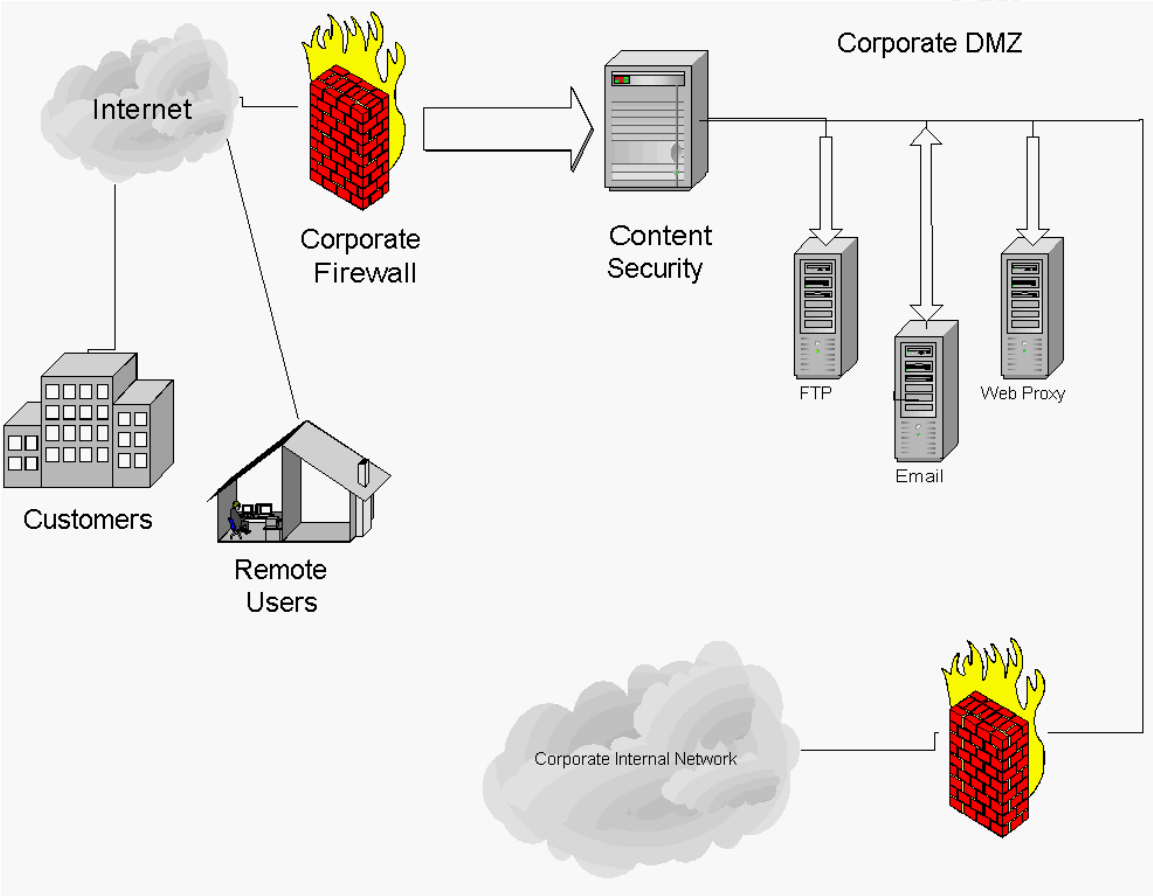


Figure 1 Typical Content Security Network Implementation

In general rules are defined to forward, quarantine, park, clean, block or delete any data passing through the server depending the results of the scan. Typical items that would be caught by the filter and possible action taken on them could be:

1. Email attachments infected by a virus or Trojan might be cleansed or quarantined.
2. Spam email might be deleted.
3. Malicious code could be cleansed or deleted.
4. Extra large files might be parked for delivery at off peak hours.
5. Outgoing emails containing vulgar language might be blocked and deleted.
6. Sensitive data leaving the company might be blocked.

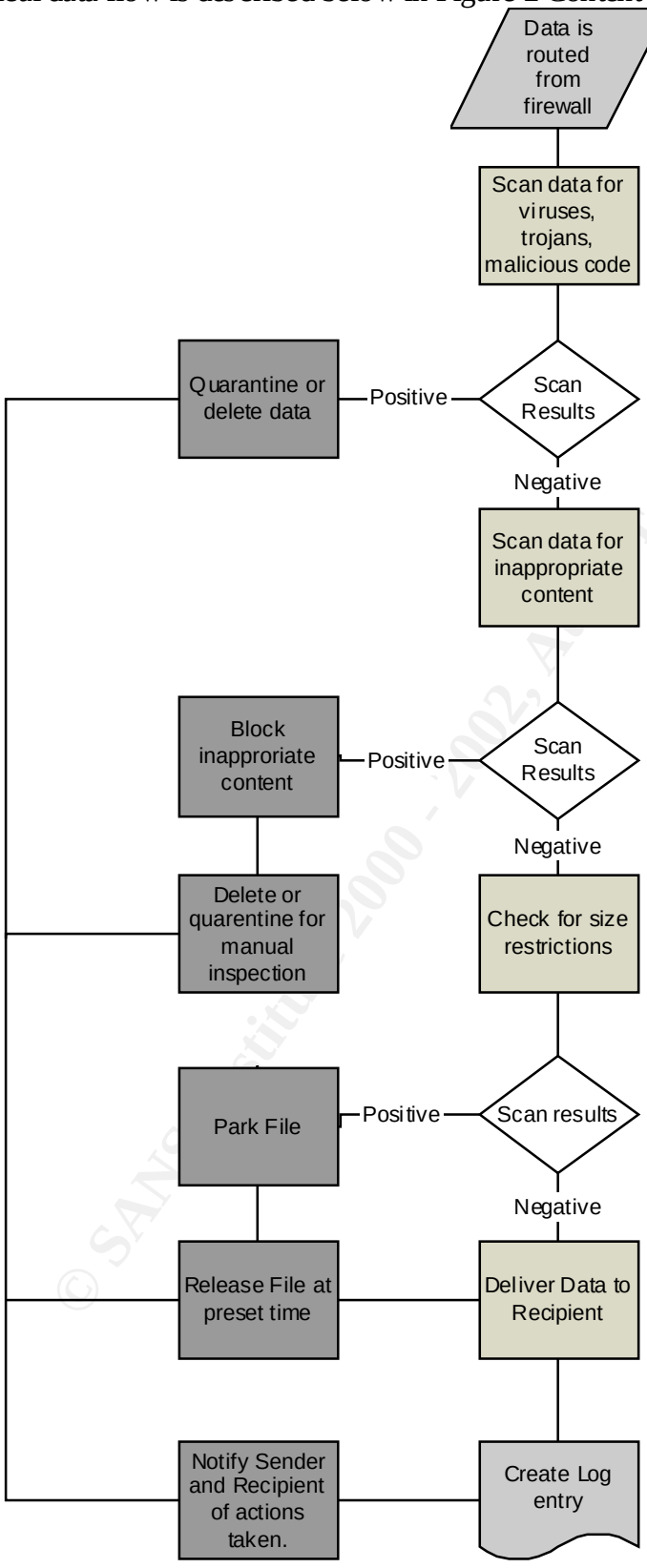
In all cases a detailed log is maintained describing the type of data being scanned and the disposition of that data. Web traffic is filtered by one of three popular methods:

1. Subscription to a service that provides categorized lists of websites such as: adult, games, chat etc. The enterprise can then configure the software as to which categories should be blocked.
2. There are voluntary rating scales that web site publishers can rate their sites to. One of the most popular is the one used by the Internet Content Rating Association known as PICS (Platform for Internet Content Selection). Filters can be set to block sites based upon these voluntary ratings. General categories in the PICS rating system include: Chat, language used on the site, nudity and sexual content of the site, violence depicted on a site, gambling, hate, drugs etc.
3. Filters can be customized to block specific sites based on the enterprises requirements.

Whenever an action other than simply passing the data on is performed, a message can be sent to both senders and recipients describing the action taken and why it was taken. This is a critical feature since a recipient may be waiting for an important message and must be told if and why it is not going to be delivered.

All activity is logged and can be reported on using a reporting tool that is included in most content filtering packages. This is another critical feature in case evidence of misuse is required for legal or other proceedings. Depending upon how the content filter is set up the log can useful in echoing all traffic on web, SMTP, and FTP servers.

A typical data flow is described below in Figure 2 Content Security



Flow.

Figure 2 Content Security Flow

1. E-mail, web, and ftp traffic come into the firewall. If the traffic is allowed in it is routed to the Content Security Server.
2. The Content Security Server scans the traffic for viruses, Trojans, inappropriate content, file size, and malicious applets.
3. If the scanned data is free of problems it is passed to the appropriate server and into the internal corporate network.
4. If the data is infected with a virus or Trojan, the content management server can be configured to delete the file, quarantine the file, or clean the file.
5. If the data contains malicious Active-X or Java code, the content security server can be configured to remove the offending code, or block the page entirely.
6. If the file contains inappropriate content, the content security server can be configured to block the offending materiel.
7. If the file is too large to move through the network during peak work hours it can be parked on the content security server for automatic later delivery.
8. If any action was taken other than to deliver the data the sender and recipient can be notified if applicable.
9. A detailed log entry is created.

Outbound Data

Another key feature of content filtering packages is to allow the scanning of outbound data. This scan will detect any viruses or Trojans that are being sent out from the internal organization. A lexical analysis can also be performed that scans e-mail messages for words and phrases that might be viewed as inappropriate for use in company e-mail. The lexical analysis can also save possible litigation against an organization by preventing inappropriate content including hoaxes and Spam from leaving the organization. In addition a lexical analysis might include searches for key words and phrases indicating that sensitive data is leaving the enterprise.

Reports

Most content security packages contain tools to generate reports from their logs. This can be useful in identifying patterns of activity from both inside and outside the organization. These reports can also be used for event correlation with other device logs when a possible intrusion attack is suspected. Reports can also be generated for activity of an individual or group of individuals, which can later be used to track misuse of enterprise resources. This provides an excellent source of non-repudiation.

Product Examples

Two products stand out as being able to aptly perform the features listed above. The two products are Aladdin Knowledge Systems eSafe family of products, and Content Technologies (now a part of Baltimore Technologies) MIMESweeper family of products.

eSafe Protect Gateway

Aladdin Knowledge Systems eSafe product provides both virus scanning and malicious code detection. eSafe Protect Gateway scans and cleans HTTP, FTP, and SMTP traffic. It has real-time scanning of all file types including MIME, UUE, and BinHexattachments. Infected files can be cleaned, removed, or quarantined. eSafe also filters malicious code in Java, ActiveX, JavaScript, VBScript, and Jscript. In addition it can be configured to do URL filtering and cookie control. Updates to the virus signatures can be scheduled and automated. Aladdin Knowledge Systems is a Checkpoint OPSEC partner and eSafe integrates easily with Checkpoints' VPN-1 firewall product.

MIMESweeper

The MIMESweeper family of products from Baltimore Technologies is a comprehensive content filtering solution that provides virus scanning and malicious code detection. MIMESweeper can filter SMTP and HTTP traffic. MIMESweeper uses 3rd party virus scanners as its virus scan. It can use multiple virus scanners to provide extra security. MIMESweeper also provides protection against malicious Java and ActiveX code. A differentiating feature of MIMESweeper is that it can provide lexical analysis of messages both incoming and outgoing. This feature is useful in enforcing company policies and preventing Spam mail from entering. There are MIMESweeper versions available for Microsoft Exchange, Lotus Domino and generic SMTP mail.

Summary

Content filtering software can be used to help mitigate the risk of viruses, Trojans, malicious Active-X and Java applets, inappropriate content and Spam. This extends to data both entering and leaving the organization. Content filtering software can be configured to perform a lexical analysis on e-mail messages, and park large files for later delivery to reduce stress on the organizations network. These features can save an organization the need for a disaster recovery from a virus, employee productivity, exposure of sensitive data, and legal litigation. Content Filtering systems can be somewhat costly, but with the benefits listed above can an organization afford not to have it? These systems are now an integral part of any well-layered overall security architecture. As with any security control, Content Filters must be deployed in conjunction with an entire security architecture and within the context of a good security policy.

References

- Aladdin Knowledge Systems, Content Security Resource Center, http://www.eSafe.com/home/csrt/index.asp (04/09/2001).
- Baltimore Technologies, MIMESweeper home page, http://www.us.mimesweeper.com/home.asp (04/07/2001).

- Internet Content Rating Association Homepage, http://www.rsac.org/ (4/20/2001).
- Morgan, Lisa "Content Security: Filter it Out" Internet Week. April 12, 2000 URL: http://www.internetwk.com/lead/lead041200.htm (4/16/2001).
- Resnick, Paul, "Filtering Information on the Internet" Scientific America. March 1997. URL: http://www.sciam.com/0397issue/0397resnick.html
- Shepard, Michael, "Content Filtering Technologies and Internet Service Providers" (03/22/2000) http://www.cs.dal.ca/~shepherd/filtering/ISPweb.htm (4/09/2001).

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event