Global Information Assurance Certification Paper

Securing the K-12 School Network through Effective Internet Access Control, Network Traffic Monitoring, and Data Analysis.

GABC Gold Certification

Author: Barry L. Young, barry.young.co@gmail.com

Adviser: Jim Purcell

Accepted: August 25, 2008

Outline

1. Introduction

Every year, more technology is being used to educate students in the K-12 environment. With the benefits of technology tools comes the responsibility of protecting students from predators and offensive online content, and the securing of personal and financial data from identity thieves. Internet access control, network traffic monitoring, and related data analysis, are powerful tools available to the K-12 Network Security Analyst to identify and mitigate these threats as part of a comprehensive security policy. This paper addresses current threats, legal responsibilities, and use of these systems to implement a defense-in-depth strategy.

2. Current Threats

The K-12 educational community faces many threats to the safety of children and personal information as a result of the proliferation of technology. Due to the unregulated nature of Internet content, protecting children from harmful content has become a difficult, if not impossible task. Easy access to electronic communication tools (email, instant messaging, social networking websites) have left children vulnerable to child predators.

In addition to these threats are the risks associated with using Web 2.0 technology as

an educational resource. While Web 2.0 content is a rich resource for educators, user-contributed content can contain malware, viruses and phishing software. Many school districts are custodians of the personal information for large numbers of staff and students, rivaling that of a large corporation. The high concentration of personal data as well as a significant operating budget makes a school district an attractive target for criminals.

3. Legal Responsibilities and Concerns

Legal Responsibilities for the Operation of Technology in K-12 School Districts

Under federal law, school districts may have a legal responsibility to protect children from harmful online content and to protect staff and student personal data from theft or observation by unauthorized parties. I have included an overview of current federal laws with a layman's description that describes the legal concepts as they apply to K-12 education. Be aware of the state and federal laws that apply to your organization and consult legal counsel before implementing policies or procedures.

Children's Internet Protection Act (Enacted 2000)

CIPA requires schools and libraries using e-rate discounts to filter Internet traffic to prevent access to web content "that is obscene, child pornography, or harmful to minors..."

The law does not apply to adult access and allows disabling of the filters for adult use.

(See www.fcc.gov/cgb/consumerfacts/cipa.html for detailed information)

CIPA has been challenged in the Supreme Court and was upheld in 2003, unlike its more restrictive predecessors the Communication Decency Act (CDA 1996) and the Children's Online Protection Act (COPA 1998)

Children's Online Privacy Protection Act (Enacted 1998)

The main emphasis of COPPA is to restrict the collection of information from children under the age of 13 without parental permission. More applicable to education however, is the requirement that photos of children that are disseminated online require a parental release.

(See http://www.ftc.gov/ogc/coppa1.htm for detailed information)

Family Educational Rights and Privacy Act (Enacted 1974)

FERPA protects the privacy of student data (grades, discipline, and home life) and prohibits the disclosure of this information to anyone but the child's parents.

(Seehttp://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html for detailed information)

Health Insurance Portability and Accountability Act (Enacted 1996)

Besides the employment aspect of this Act that applies to employers, HIPAA addresses the privacy and security of health information and standards for electronic transmission of that data.

(See http://www.hipaa.org/ for detailed information)

Legal Responsibilities for the Monitoring and Collection Of Network Traffic

Pen Register/Tap and Trace Act

Original Act- 18 U.S.C. §§ 3121-27 (1994) Patriot Act revision- (2001)

The act prohibits identifying the source of a data transmission or phone call (IP source address, phone number, etc). Certain monitoring is allowed if it relates to the operation, maintenance, or testing of the network infrastructure. This act does not address the monitoring of content, only the source and destination of the transmission.

Potential exceptions for K12 institutions:

Exception for service providers

Verification of service

Consent of the end user

Stored Electronic Communication Act

18 U.S.C. §§ 2701-12 (2002)

The Act prohibits the divulging of contents of a communication while in electronic storage by the provider of the service. While the law is directed at "public providers", school districts should seek counsel to determine their responsibilities regarding this statute.

Potential exceptions that may apply to K12 institutions:

Exception for service providers (virus scanners, etc.)

Consent of the end user

Wiretap Act/Electronic Communications Privacy Act

18 U.S.C. §§ 2510-22 (2002)

Prohibits the interception of "wire, oral or electronic information"

Potential exceptions that may apply to K12 institutions:

Exception for service providers

Monitoring of Trespassers

Consent of the end user

To summarize, federal law may require school districts to keep the personal and medical information of staff and students confidential and get releases from parents before posting photos of students on the Internet. If they are receiving e-rate funding, districts are required to protect children from harmful content.

The Pen Register/Tap and Trace, Wiretap, and Stored Electronic Communications Acts prohibit the monitoring of the source, destination and content of information as it is transmitted and stored. While there are several exceptions that may allow a school district to monitor traffic, having end users give their consent may be one way to ensure that you are in compliance.

In addition to federal requirements, many states have enacted laws that have strict requirements for Internet security and access by minors. A thorough understanding of these requirements for your locale will be imperative as you develop security policies, and engineer

a network filter/monitoring system that complies with these regulations. Data collection procedures should also be analyzed to ensure that they comply with the federal rules of evidence and are admissible in court.

4. Policies and End User Acceptable Use Agreements

Before any solution the following topics at a minimum should be addressed in a formal policy:

- Data Capture
    - What data will be captured and recorded?
    - Will there be any data that will not be captured? (Banking transactions, VoIP, etc)
- Monitoring/Analysis Schedule
    - How often are the logs and content reviewed and reported?
- Reporting procedure
    - Who should receive the reports and decide a course of action?
    - Is there a different reporting procedure for each category? (Child porn for

example)

  - Is there a different reporting procedure for staff and students?
  - What is the event threshold that triggers an investigation in each category? Examples- Pornography: 10 hits within 5 minutes, Child Pornography: 1 hit, etc.

- Retention of content and log information
  - How long will the information be retained?
  - Where will it be stored?
- Investigation requests
  - Who in the school district can order an investigation if suspicious behavior is observed?

End User Technology Acceptable Use Agreements

Every user should sign an acceptable network/technology use agreement, either electronically or on paper. To support network monitoring and data collection, the agreement should include the following concepts at a minimum in addition to the terms, conditions and acceptable practices:

1. A statement that there is no expectation of privacy on the network and that all traffic is monitored including but not limited to email, web traffic and Internet searches, and chat.
2. A statement that information gathered may be used in disciplinary proceedings.
3. A statement that the user gives consent- "I agree to abide by these terms and conditions and give my consent for (The School District) to monitor and examine my network traffic, stored data files and computer activity."

5. Monitoring and Filtering Strategies and Goals

Strategy

In order to design, implement, and leverage an effective security program a full understanding of your organization is essential. It is critical to identify:

- What needs to be protected and why. (Your assets)
- What it needs to be protected from. (The risks)
- How to protect it. (Mitigate the risk using technology and policies)

Once this information is identified, a common and proven security strategy is to consider the following when developing goals for Information Security:

- Availability- The system is readily available for access.
- Integrity- The information remains accurate and only modified by authorized persons
- Confidentiality- The information can be modified and accessed only by authorized persons.

After identifying the *assets* and *risks*, I develop a K-12 Internet security plan to mitigate these threats with *policies* and *technology* and I consider these aspects using this slightly different model:

Availability- Can students access the information that they need to support the educational process?

Integrity- Can the system be bypassed, rendering it ineffective? Can it effectively

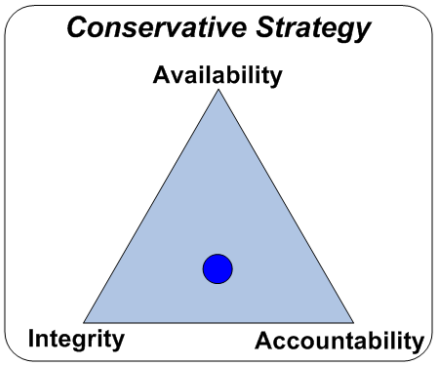
control access to the Internet?

Accountability- Are end users held accountable for their actions by enforcing the use of authentication and linking that access to their electronic identity?

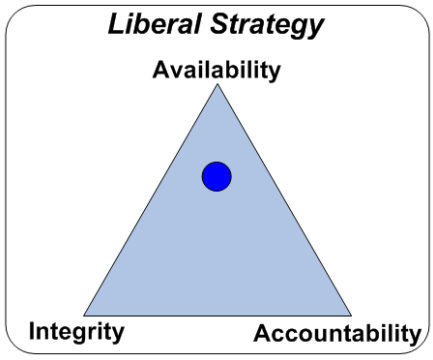
The final strategy should maintain a balance between these three concepts. Integrity and accountability tend to carry equal weight in the equation in a K-12 environment. The challenge in education is to provide availability of Internet resources while mitigating the risk of student exposure to harmful material by ensuring that the integrity and accountability goals are met. How you prioritize the importance of each rule will depend on the culture of your district and the tolerance of risk in your environment.

This balance can be illustrated by plotting a point on a triangle:

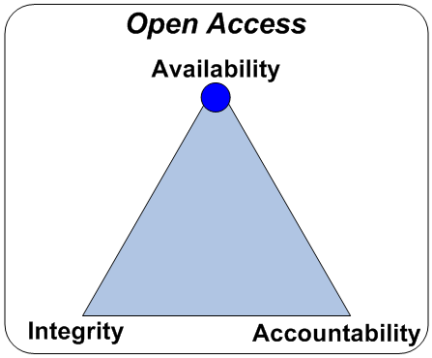
Conservative districts may choose to improve integrity and accountability by limiting student access to the Internet. The end result is that legitimate and safe pages may be blocked.



A more *liberal* strategy sacrifices control over content and accountability for additional access to the Internet. Fewer legitimate pages are blocked, but harmful content may be passed through.



Districts that choose not to filter the Internet provide total access to the Internet with no accountability or access control.



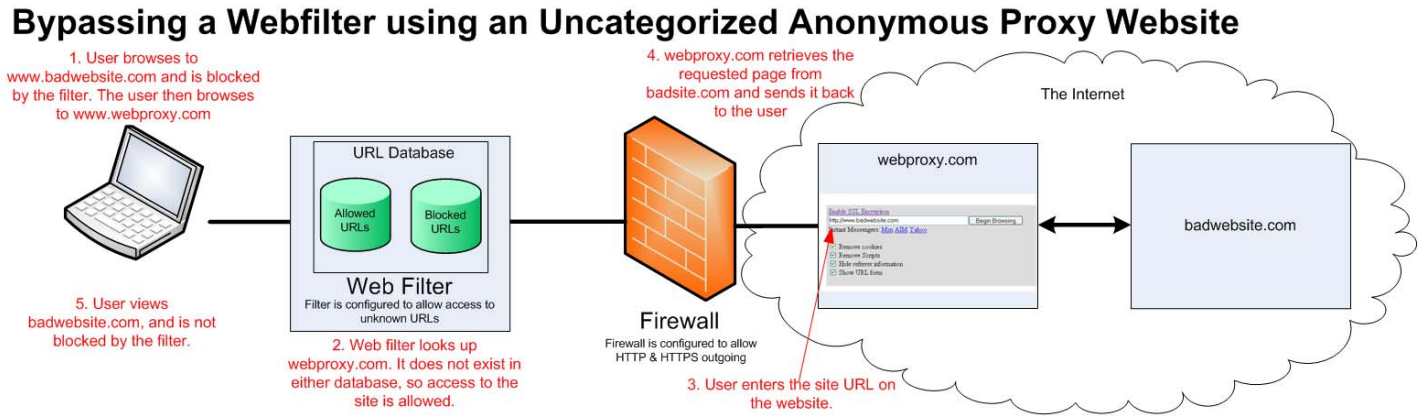
Technical Challenges

Uncategorized websites

Traditional filters use lists of known URLs to categorize websites. Thousands of websites are added to the Internet daily and can be accessed through a traditional filter that is configured to allow access to uncategorized websites. In a typical organization, thirteen to fifteen percent of the websites that are accessed are not categorized by the web filter. Most web filters give the option to allow or block uncategorized sites, but experience has proven that blocking them will disable many legitimate websites by blocking helper links within the pages.

Anonymous Proxies

End users will often attempt to use anonymous proxies (anonymizers) to bypass web filtering and content monitoring. New proxy sites are created each day, sometimes by the end users themselves on a personal website. The URL web filter may allow access to the proxy site as it is often too new to be categorized, and the proxy retrieves the information unblocked to the end user. If the proxy site offers an SSL encryption, the encrypted data is difficult, if not impossible to monitor and identify as harmful. Proxy products like Ultra Surf from UltraReach (designed for the Chinese to fight Internet censorship) are sophisticated programs that when executed from user computer will provide an encrypted tunnel to the Internet.



Encrypted Traffic (Secure Socket Layer and Encrypted Data)

SSL and other encryption technologies are effective when used ethically and can prevent the observation of sensitive data by malicious third parties. Because the content of the encrypted

network traffic cannot be viewed by conventional network scanners, this technology is often used to conceal criminal activity.

Web 2.0 Content

The original World Wide Web (Web 1.0) consisted mostly of static web pages that were created and modified by the owner of the page. While not a recognized standard, Web 2.0 refers to a new model of the Internet that is growing exponentially with copious web applications that encourage user-provided content. Blogs, Wikis, and Social Networking Sites are good examples of Web 2.0 sites that are built by the end-users themselves without much input validation. Malicious code is often added by users (unknown to the site operator) and passed on to visitors. Offensive content is often present on the same website as useful educational content. Flickr.com for example, contains pornography and Library of Congress information. MySpace.com contains material that supports classroom instruction, but also hosts material that is both harmful and dangerous to children. This mix of content in a single website can render traditional URL filtering ineffective. *Many experts also believe that Web 2.0 will become a greater threat vector for viruses and malware than SMTP within the next year.*

Web Graphics and Multimedia Content

The most common form of offensive content on the Internet is present in a graphical, video or audio format. These files require human analysis to determine if the content is offensive.

Search Engines and Image Search Engines

Internet search engines today are state of the art and any topic can be accessed rapidly. The challenge comes when students search on words that have both a slang connotation as well as proper English meaning. Image searches often return content directly from the search engine image cache rather than the originating site, rendering traditional URL web filtering techniques ineffective.

Filtering and Monitoring Goals with Associated Risks

- Address Web 2.0 issues
    - Identity theft
    - Malware/Virus
    - Offensive content

- Monitor and block inappropriate content access by students
    - CIPA non-compliance
    - Litigation
    - Exposure of students to harmful material
    - Waste of bandwidth and time.
- Prevent the use of proxies by end users.
    - Access to unauthorized content
    - Concealed theft of district information
- Monitor and report inappropriate content access by staff.
    - Exposure of students to harmful material
    - Waste of resources
    - Potential risk to children from a predator within the district.

- Identify acts of sabotage and information theft.
    - Data loss or corruption
    - Denial of service
    - Extortion
    - Embezzlement
    - Information and identity theft.
- Block access to malicious code and phishing websites.
    - Information, credit card, and identity theft
    - Increased computer maintenance,
    - Botnet attack (denial of service)
    - Computer compromise.
- Manage access to high-bandwidth resources (multimedia, voice over IP)

  - Loss of employee and student productivity.
  - Reduced network availability.
  - Litigation due to copyright issues.

- Prevent the abuse of SSL encryption
  - Access to prohibited content without detection.
  - Transmission of sensitive content.

- Prevent the inappropriate use of File Encryption
  - Loss of personnel information and financial data.
  - Prohibited content can be stored or transferred without detection.

- Prevent the inappropriate use of search engines and image search engines
  - Exposure of students to harmful content when dual-meaning search words are entered.
  - Exposure of students to harmful content when prohibited search words

are entered.

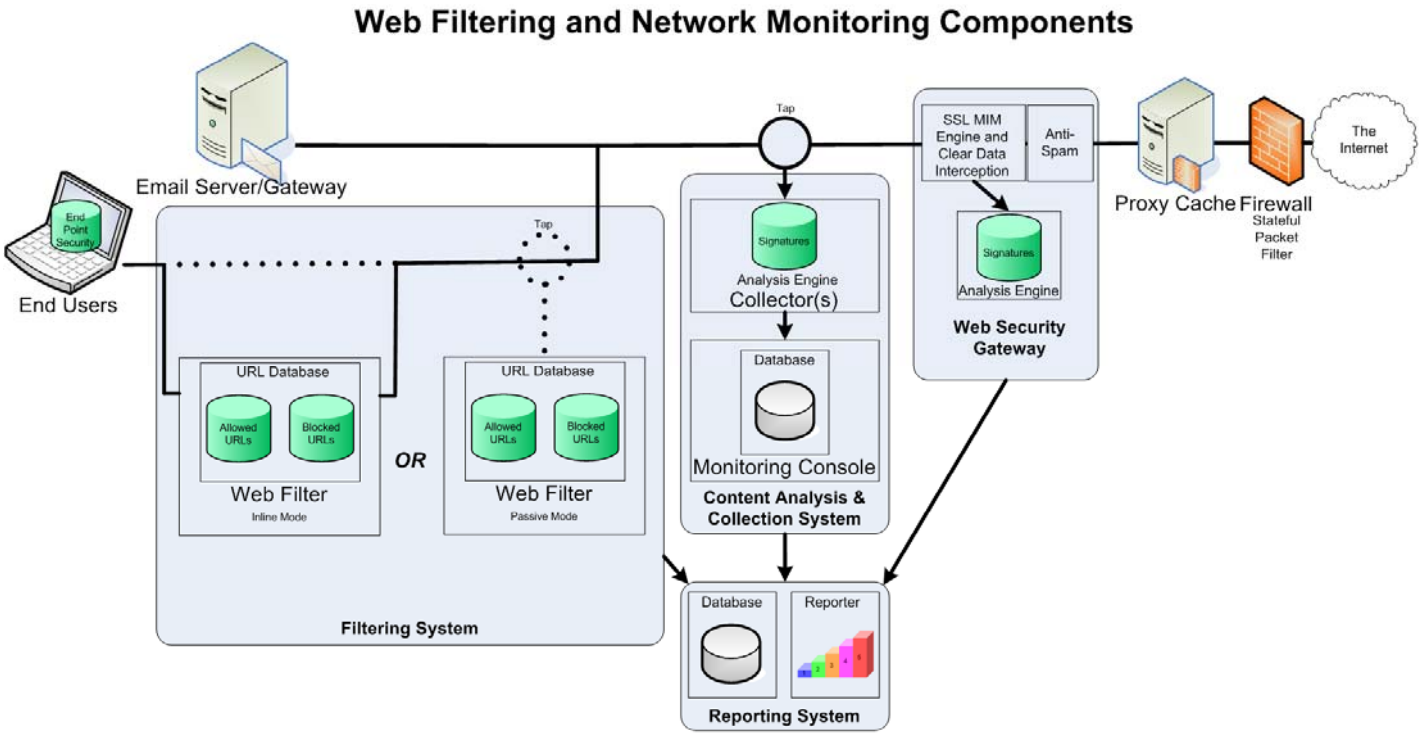
- Provide evidence of policy violations and intent.
    - Innocent users may be wrongfully accused.
    - Guilty users cannot be disciplined or prosecuted effectively.
- Identify content that is related to the exploitation of children
    - Child pornography.
    - Online predator correspondence.
    - Inappropriate relationships between adults and students.

6. Technology Tools for Access Control and Data Monitoring

Technology hardware and software should be selected and configured to address all of the identified filtering and monitoring goals. Present and future bandwidth requirements should be considered as the system is designed to prevent a bottleneck in the data flow. There is a wide

variety of equipment available that may either be purchased as a complete system or as separate components. The system should interface with a central authentication system (Active Directory, LDAP, etc.) to identify the end-users.

Web Filtering and traffic monitoring is not an exact science due to the constant change of the Internet. A system that will modify itself proactively to match the latest threats will offer the best value and will provide dependable and predictable service. The following design will provide a conservative balance between availability, integrity and accountability when configured properly.

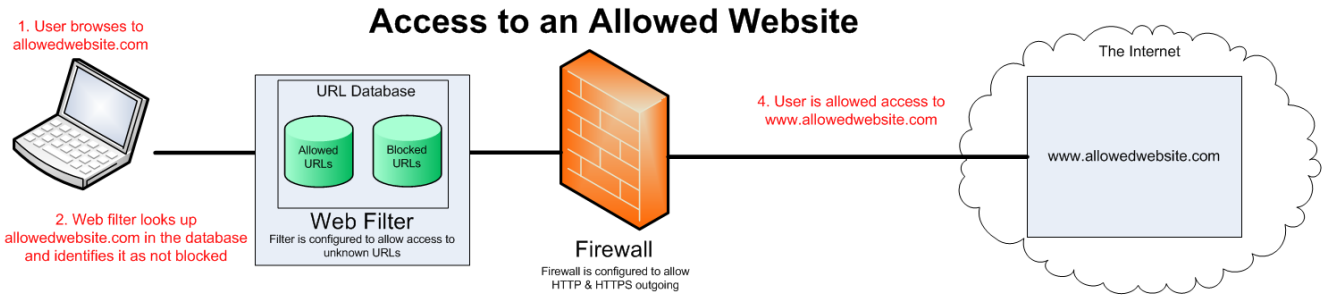


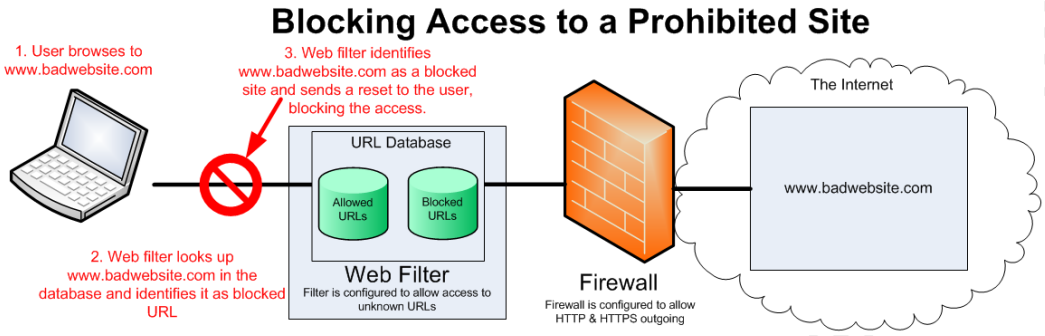
End Point Security and Control

Anti- Virus/Malware/Trojan software is typically used on the desktop to protect user's computers from attack and will sometimes include access monitoring and control. Many of these programs can also be used to identify and report the presence of files or software of interest on the hard disk or removable media. (Proxy, file sharing, games, etc)

Filtering System

A web filter should be specified that provides URL filtering using identified URLs. To provide acceptable availability, uncategorized URLs are set to pass through. The URL database should be updated at least daily. There should be an automated process that reports uncategorized URLs to the filter provider for prompt categorization.

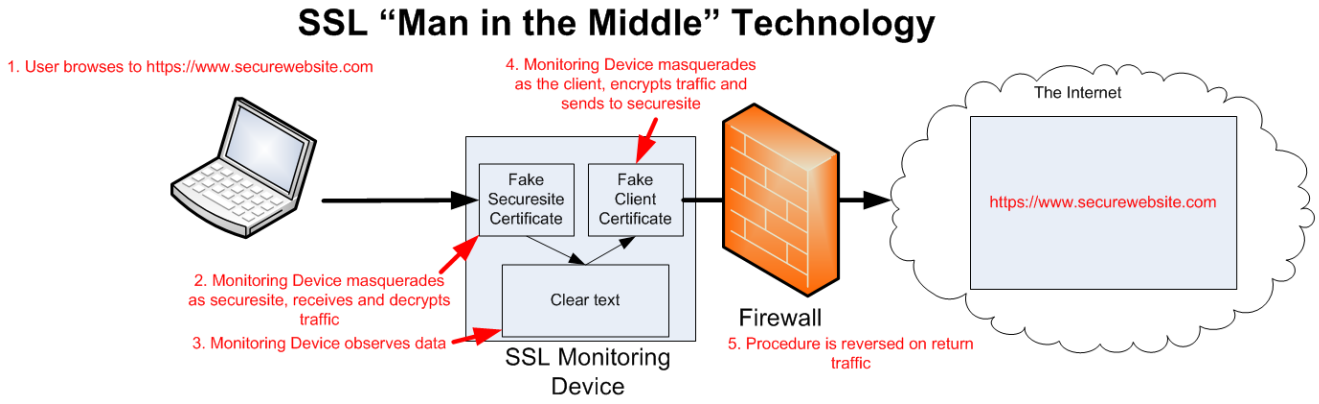




Web Security Gateway [Web Application, Unified threat Management]

This system monitors the data stream real-time and actively blocks malware, viruses, and trojans. Web application access should be identified and the access controlled on any port or protocol by individual computer or user account. Packet shaping (bandwidth management) features should limit bandwidth and access to specified protocols and web applications by URL and by user. The firewall should allow the administrator to monitor and block data transmission based on a custom list of keywords and file signatures (proxy traffic, inappropriate language, etc.). It is also possible to view SSL content using “Man in the Middle“ technology that is available on these devices. SSL anonymous proxies and inappropriate traffic can be identified and analyzed “in the clear”. Before implementing MIM SSL technology, the potential legal liability of viewing encrypted personal financial transactions should be analyzed and addressed. Any active intervention system requires hardware with a

generous reserve of processing power to prevent latency as the payload of each packet must be analyzed. This must be considered when sizing the system.



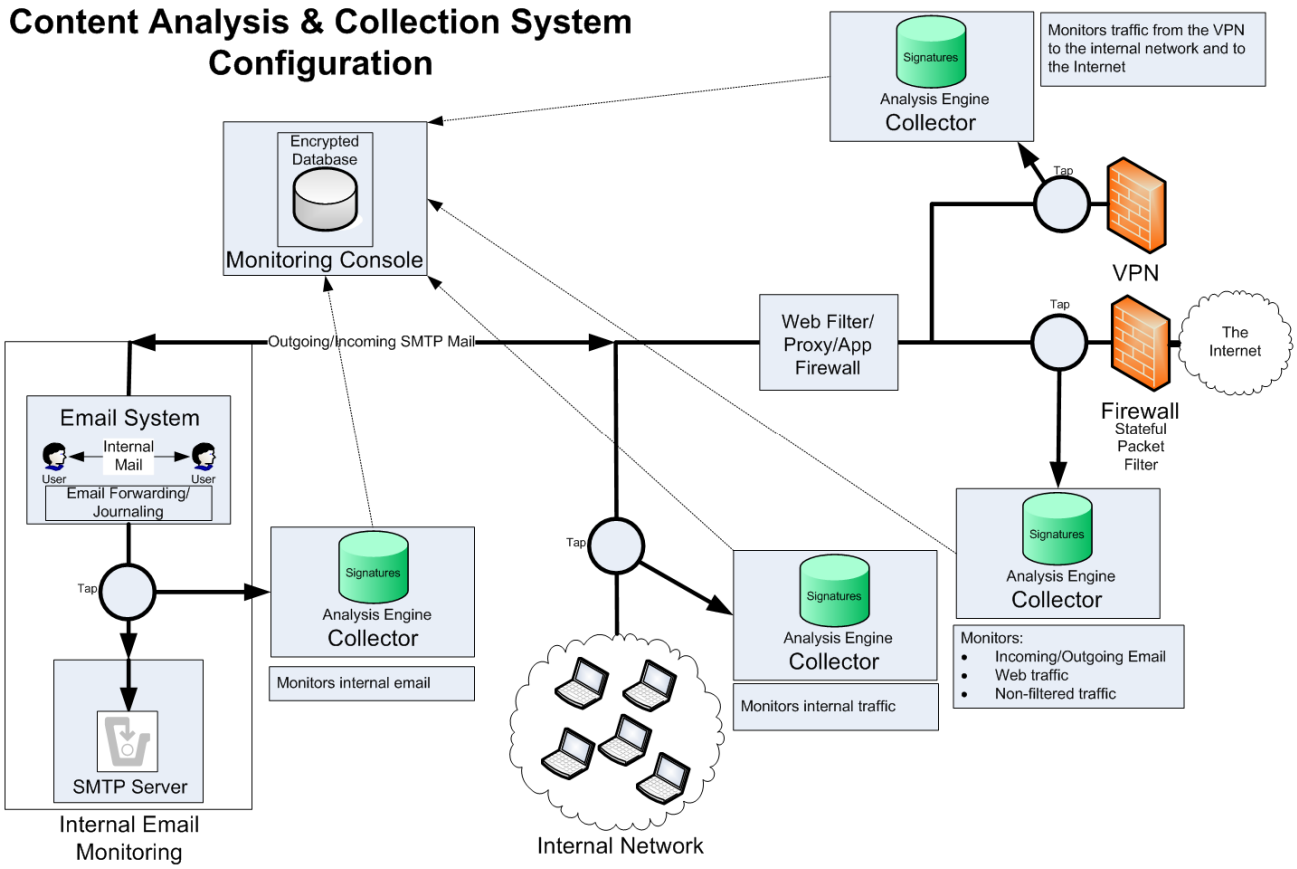
Content Analysis and Monitoring System

This system captures network traffic sessions based on content and stores them in an encrypted database (Chat, web mail, email, web traffic, email attachments, etc). Encrypted secure storage is necessary to protect the integrity of the evidence from tampering, rendering it useless for prosecution.

These systems also provide defense in depth by continuously monitoring the filter system and identifying inappropriate web site access that has been allowed by the filter. They can also monitor servers and computers that have a direct route to the Internet (no filtering).

Collectors (sensors) are used at various locations on the network to monitor traffic. They can be used inside the network and at entry and egress points to achieve the desired results.

One particular challenge is email that is sent between internal users on an email server (Microsoft Exchange for example). Monitoring and archival software is available but can represent a substantial financial investment. Using the journaling process in MS Exchange or simply forwarding all internal mail to a local, secure SMTP server is an inexpensive solution. The traffic can be intercepted, analyzed, and then deleted when it arrives at the SMTP server.



Reporting System

This system consolidates logs from the devices and provides reports for analysis by filtering and monitoring category, time accessed, machine name, IP address and username. The reporter should export data to common formats- PDF and CSV at a minimum.

Addressing the Identified Filtering and Monitoring Goals using the Filtering and Monitoring Systems

Address the Web 2.0 issues (Web Applications)

- Allow access to content that supports education (Web applications are essential for proper integration of technology).
- Block harmful material and time wasters using filtering system and Web Security Gateway.
- Monitor and block obvious offensive language using the Web Security Gateway.
- Develop applicable appropriate use policies and educate users on their existence and purpose.
- Detect and prevent the delivery of malware/virus payloads using the Web Security Gateway.

- Monitor and block inappropriate content access by students
  - Block known (categorized) offensive websites by URL using the Web Filtering

System.

- Block offensive websites that are not categorized by analyzing the traffic and blocking offensive keywords using the Web Security Gateway.
- Block offensive web searches using the keyword filtering feature on the Web Security Gateway and Filtering System.
- Monitor email, web mail and chat for offensive content using the Web Security Gateway.
- Identify offensive images and multimedia by using the Web Security Gateway and Content Analysis and Monitoring System to analyze the text information that accompanies the traffic.

- Prevent the use of proxies by end users.
  - Block categorized *http and https* proxy sites using the Web Filtering System.
  - Block uncategorized *http* proxy sites by identifying proxy signatures using the Web Security Gateway.

- Block uncategorized *https* proxy sites by verifying the validity of SSL certificates before allowing access. A high percentage of these sites have self-signed certificates.

- Analyze all SSL proxy traffic using a “man in the middle” process on the Web Security Gateway. Block all known proxy patterns.

- Capture all webmail and chat sessions using the Content Analysis and Monitoring System.

- Identify proxy software on the local hard disks and removable media using the Endpoint Security System.

- Monitor and report inappropriate content access by staff.

  - Monitor and log categorized offensive websites by URL using the Web Filtering System.

  - Monitor and log offensive websites that are not categorized by analyzing the traffic and logging and capturing offensive activity using the Web Security Gateway and Content Analysis and Monitoring System

- Monitor and log offensive web searches using the keyword filtering feature on the Web Security Gateway and Content Analysis and Monitoring System.
- Monitor and capture the full content of all email, web mail and chat and scan for offensive content using the Web Security Gateway and Content Analysis and Monitoring System.
- Record transaction evidence using the Content Analysis and Monitoring System.

- Identify acts of sabotage and information theft.
  - Monitor and log traffic that contains personal information (Social security numbers, credit card numbers, medical ID numbers, etc.) using the Web Security Gateway and Content Analysis and Monitoring System.
  - Record transaction evidence using the Content Analysis and Monitoring System.

- Block access to malicious code and phishing websites.
  - Block categorized malicious code sites with the Web Filtering System
  - Identify, intercept and block malicious code by signature using the Web Security

Gateway.

  - Identify malicious code using the email spam filter and Endpoint Security System.

- Manage access to high-bandwidth resources (multimedia, voice over IP)
  - Use the Web Security Gateway to control access to any multimedia source by protocol and application.
  - Use the Web Security Gateway to limit bandwidth to multimedia during peak usage times. (Internet radio for example)
- Prevent the abuse of SSL encryption and file encryption
  - Develop clear and concise policies that address the use of encryption by end-users.
  - Monitor the use of encryption technologies using the Web Security Gateway.
  - Allow the use of district-supplied encryption programs for legitimate purposes that will allow administrative access to any file using an administrative

encryption key.

- Prevent the inappropriate use of search engines and image search engines
    - Enforce the use of safe search options on reputable search engines when possible and use child-safe engines.
    - Disable the image search engines if possible on non-safe-search sites.
- Provide evidence of policy violations and intent.
    - Use the reporter and Content Analysis and Monitoring System to identify violations by category.
    - Create custom categories for threats specific to your organization.
    - Implement policies that protect the chain of evidence.
    - If inappropriate content is found, investigate a link to related searches.
- Identify and Report Content that is Related to the Exploitation of Children
    - Create policies that define the monitoring and reporting process related to this

type of content.

- Develop a working relationship with local law enforcement/FBI and seek guidance that will assist in the identification and reporting of contraband.

- Create custom keyword lists for use in the Web Filtering System, Web Security Gateway, and Content Analysis and Monitoring System. Your law enforcement contact may be able to help you identify search terms to include in the monitoring list.

7. Strategies for the Analysis of Collected Data

A school district of even moderate size can generate a large amount of log data, statistics, and captured content. The bulk of the data will only be reviewed if needed to identify trends and daily behavior of the individual(s) who are under investigation. Only a small percentage of this information requires in-depth daily analysis to identify offenders.

Event thresholds can be used to help determine if the access was deliberate or accidental. Total number of hits, search engine searches and the time spent accessing the pages can be helpful indicators of intent. For example, it is not uncommon for multiple offensive web sites to be spawned in a few seconds, especially if pop-up blockers are not

used.

The following strategies will help identify users that are in violation of the Acceptable Use Agreement and may prove whether the access was intentional.

Email and Webmail Analysis

- Monitor and identify content in the text of the email and attachments that are not permitted and generate reports by category (Sensitive information, abusive speech, obscene content, attachment type etc.).
- Perform visual spot checks on webmail attachments; multimedia and photographs are of particular interest.

Web Traffic

- Generate reports on the Web Filtering System that list access by user to each prohibited category. A report that spans multiple days will indicate trends and reduce the chance of false positives.
- Generate reports on the Content Analysis and Monitoring System and Web Security Gateway to identify users that have bypassed the Web Filtering System using anonymous proxy websites that are unknown to

the Web Filtering System.

- Review the logs from the AV solution to identify malicious programs and proxy software
- A report on offensive search keywords will help to establish motive and intent.
- Use the Web Security Gateway to identify users that have accessed prohibited services by protocol- Bit Torrents, VoIP, Internet Radio, encryption, etc.
- Identify offensive images and multimedia by analyzing the accompanying text using the Web Security Gateway and Content Analysis and Monitoring System

Data Storage

- Identify prohibited files on user computers and removable media using the End Point Security Software (AV) reports.
- Use administrator access and operating system tools to search and analyze content on end users computer.

- Perform active scans on the central data storage device using an AV solution to identify malicious and prohibited content. Content and keyword searches can also be performed manually or scripted to identify offensive content or file types of interest.

8. Web Filter and Monitoring Topics/Categories for Students

Each system may categorize and identify these topics differently.

Offensive Content

- Pornography, Child Pornography, Obscene, Tasteless, Hate and Discrimination, Racism, Explicit Art, Social Networking, Unmoderated Web Based Newsgroups, Webmail, Streaming Multimedia, Unmoderated Blogs and Message Boards.

Criminal Skills

- Hacking, Traditional Criminal Skills (Lock Picking, Safe Cracking, Burglary, etc), Terrorist/Militant/Extremist.

Ethical Issues

- School Cheating, Plagiarism, Gambling.

Search Engines

- A conservative approach is to deny access to all search engines and image search engines that are not identified and verified as safe for children.

Safety/Health

- Tobacco, Alcohol, Illegal Drugs, Social Networking, Chat, Webmail, Weapons.

Network Security

- Adware, Malicious Code/Virus, Phishing, Remote Access (GoToMyPC, etc),Spyware, Web Proxies/Anonymizers, Peer to Peer File Sharing, Social Networking, Chat, Freeware/Shareware.

Resource Management- Bandwidth

- Voice Over IP Services, Streaming Multimedia, Internet Radio, Games, Web-based storage.

Resource Management- Productivity

- Games, Sports, Online Stock Trading, Online Auction, Greeting Cards, Real Estate, Travel, Fashion, Shopping, Entertainment, Streaming Multimedia, Internet Radio, Message Boards.

9. References

Children's internet protection act. (2008, April 1). *Wikipedia.* Retrieved April 1, 2008, from http://en.wikipedia.org/wiki/Children's_Internet_Protection_Act

Children's internet protection act- fcc consumer facts. (2008, April 1). *Ftc.* Retrieved April 1, 2008, from http://www.fcc.gov/cgb/consumerfacts/cipa.html

Children's online protection act. (2008, April 1). *Wikipedia.* Retrieved April 1, 2008, from http://en.wikipedia.org/wiki/Child_Online_Protection_Act

Communications decency act. (2008, April 1). *Wikipedia.* Retrieved April 1, 2008, from http://en.wikipedia.org/wiki/Communications_Decency_Act

Children's online privacy protection act. (2008, April 1). *Wikipedia.* Retrieved April 1, 2008, from http://en.wikipedia.org/wiki/Children's_Online_Privacy_Protection_Act

Children's online privacy protection act. (2008, April 1). *Ftc.* Retrieved April 1, 2008, from http://www.ftc.gov/ogc/coppa1.htm

Family educational rights and privacy act. (2008, April 1). *Wikipedia.* Retrieved April 1, 2008, from http://en.wikipedia.org/wiki/Family_Educational_Rights_and_Privacy_Act

Family educational rights and privacy act (ferpa). (2008, April 1). *Www.ed.gov.*

Retrieved April 1, 2008, from http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Heath insurance and portability act. (2008, April 1). *Wikipedia.* Retrieved April 1, 2008, from http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

Heath insurance and portability act. (2008, April 1). *Hipaa.org.* Retrieved April 1, 2008, from http://www.hipaa.org/

Nolan, O'sullivan, Bronson, Waits(2007). *First responders guide to computer forensics.* Pittsburgh, PA, Usa: Cert.

Scoudis, Ed (2008). *Cutting Edge Hacking Techniques-Security 517.* Bethesda, MD, Usa: Sans institute.

Cole, Fossen, Northcutt, Pomeranz, Wright (2006). *Sans Security Essentials.* Bethesda, MD, Usa: Sans institute.

Carnegie Mellon University. (2008). *Managing enterprise information security: a practical approach for achieving defense-in-depth.* Pittsburgh, PA, Usa: Cert.

Bouchard, Mark, Sweeney, Patrick. (2008). *Security Strategies for Web 2.0 and Social Networking.* Irvine,CA, Usa:Techrepublic.com.

SOPHOS. (2008). *Security Threat Report 07/2008.* Boston, MA, Usa:Techrepublic.com