Global Information Assurance Certification Paper

Securing the Network Perimeter of a Community Bank

GIAC (GCFW) Gold Certification

Author: Steven M. Launius, SteveLaunius@gmail.com
Advisor: Aman M. Hardikar

Abstract

Allocating the investment for perimeter protection and detection mechanisms can be an unique challenge with the budget of a smaller community bank. This paper's purpose is to raise awareness of the external threats present to confidential customer information held on the private network of community banks, and recommend technologies and designs to protect the perimeter of the network, while taking heed of the limited resources of community banks. The perimeter protection topics will include: routers, firewalls, Wi-Fi, phone systems, publicly accessible servers, and remote access. Current and developing techniques for preventing attacks will be presented as will the importance, type, and frequency of independent audits to ensure the perimeter maintains a secure posture.

1. Introduction

Deploying a network in any small or medium sized business can be an arduous task that brings many risks with it. For community banks, the responsibility of keeping intruders from accessing confidential customer information is mandated by law in the United States (Gramm-Leach-Bliley Act, 1999). This includes protecting a private network from attacks and identifying possible breaches to a bank's private network. To establish a secure network a defense-in-depth strategy where security measures are placed in many layers that create an entire network, from the end user to the Internet, will be essential. The network perimeter layer has historically been the focus of protecting a private network and is still essential for keeping intruders at bay and providing detection of possible intrusions.

The perimeter layer of a network starts when an outside connection is established and ends with access to a private network. Outside connections can be established by an Internet Service Provider (ISP) such as Charter, Mediacom, and AT&T to name a few. A wireless network can also provide connectivity across multiple rooms or floors of a facility as wireless signals can penetrate physical boundaries. Any modems connected to computers provide an additional avenue into a private network. The network perimeter can be comprised of devices that block unwanted traffic, allow remote access, filter for potential dangerous content, and detect or block probable attacks. Additionally, the perimeter may contain email and web servers that provide services to customers and employees externally via the Internet. A private network will be at risk from many threats because of the need to establish connections to other networks, especially the Internet.

Understanding the threats present to a private network is important to properly design the perimeter protection for community banks. Every second of every day, scans are perpetuating throughout the Internet looking for vulnerable hosts that can be exploited. Take a peek at any perimeter firewall or router logs to view the magnitude of these meticulous scans that constantly probe for vulnerabilities. Malicious software can be found on many websites, whether it is a legitimate website or created specifically for

disseminating this type of software. Unsolicited emails, known as spam, are not only annoying but can also contain malicious software and links to malicious websites. Criminals can drive around with laptops looking for vulnerable wireless access points, known as war-driving (Richards, 2008). The old hacks have not gone away either; war dialing (Gunn, 2006) is still being used to find access into a private network through a modem. Employees are also culprits of data breaches either intentionally or unintentionally. The threats are numerous, but protection from these threats has been around just as long.

IT Security industry best practices needed to secure the network perimeter has been proven to reduce the risk of breaches to a private network. The most basic component that separates internal and external networks is the Internet Gateway Router. This device not only separates a private network from the Internet, but can also act as a basic firewall by blocking unauthorized traffic from entering or leaving a private network; this is known as a static packet filter firewall (Mateti, 2008). Software firewalls protect host operating systems while hardware firewalls protect the perimeter of networks by using customized, high capacity appliances. A Virtual Private Network (VPN) can be used to allow remote access to a private network from anywhere in the world using the Internet. The VPN can be used for third-party vendors and employees with mobile computing devices to access private network resources over the Internet. An Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) can be used to monitor the traffic that is allowed through the firewall for detecting and stopping possible attacks. Both of these systems can also detect infected hosts on a private network by monitoring the traffic leaving the network. A proxy is another form of a firewall that can be used to protect web browsing and other Internet capable applications. Filtering can be used in a proxy or a firewall to block known malicious websites or email. Log management systems can provide a view from many different devices that can allow experienced personnel to identify attacks that software alone could never find. Next generation technologies are combining these best practices at different points of the network infrastructure to improve protection.

Emerging technologies are addressing the limitations imposed by the current best practices for protecting the network perimeter, but as with any new technology there are

problems that need to be resolved and they often come with a high price tag. Filtering rules have matured enough to stop confidential information from being sent in emails. Data Loss Prevention (DLP) has extended on this filtering technique to create a system that prevents confidential information from being used in any type of network communication that leaves a private network. DLP has been around for several years already and has mixed reviews among information security experts (Brandel, 2007). Unified Threat Management (UTM) has become the term used for perimeter devices that combine firewall, IDS or IPS, VPN, filtering, antivirus, antispyware and other technologies into a single device (McBride, 2009). UTM is the latest technology for firewalls made possible by high performance processors to manage features that act upon many layers of the OSI model (Tyson). Network Access Control (NAC) are solutions used to control host and user access to private network resources. NAC can place requirements and limitations on any host connecting to a private network, thereby enforcing a standard of security for all hosts. These new technologies promise numerous benefits, but may not be mature enough for easy implementation or affordable for a community bank.

Assessing the configuration of the perimeter devices regularly will provide assurances that they are correctly configured and providing superior protection. New vulnerabilities are discovered by researchers and hackers daily, so the threats the perimeter must guard against are continuously shifting. A standard auditing methodology ensures a thorough security test. Frequent verification of the perimeter devices, both from inside and outside the perimeter can provide management with concise assessments needed to comply with laws and regulations. Independent audits provide unbiased assessments of the configuration and maintenance performed by the network custodian; educating them on the latest security practices and solutions.

By implementing established practices for securing the perimeter of a private network, a community bank can secure itself from the majority of threats without exhausting its' entire IT budget. It is important to realize that no amount of money can purchase impenetrable protection for the network perimeter. However, with the proper knowledge, a small budget can be spent wisely to protect a private network from the majority of vulnerabilities.

Steven M. Launius, SteveLaunius@gmail.com

2. Threats

In order to properly design perimeter protection for a private network, it is necessary to learn about the types of threats present and the damage that can be caused. Threats are not always apparent to every manager, but information security professionals are hard at work finding new threats and presenting the perils to those who seek this information. Staying abreast of every new threat is not necessary, but knowing the common threats will aid in designing a network perimeter to protect from the majority of them.

2.1. Internet Attacks

Network reconnaissance is the act of scanning a network for available information; this is commonly referred to as network scanning. The most popular scanning tool is a free tool called Nmap (http://nmap.org/). This tool will probe an IP address or a range of IP addresses to find ports that are available and try to gather useful information; such as the service provided, the operating system used, or the type of device. Scanning the perimeter over the Internet will reveal the potential holes in the established infrastructure and is commonly used by criminals in the initial phase of an attack. Wireless Access Points (WAPs) can establish a wireless network where a physical line may be difficult or expensive to install. But in doing so can expose a private network to scanning by criminals who may loiter outside a company's facility. Kismet is a free wireless scanning tool which can detect any wireless network, whether the network broadcast name is being hidden or not. Aircrack-ng can break certain encryption algorithms meant to protect data traveling on a wireless network. With these tools anyone connected to a WAP can sniff (view) all the traffic passing through that access point. Sniffing can allow anyone to see plain text login credentials and confidential information transferred over the network from programs like Telnet and FTP. Wireshark and Tcpdump are popular and free tools used for this purpose. The spot chosen to sniff from is important in today's switched networks. Sniffing from a computer will reveal only that computer's network traffic and any broadcast traffic. However, if physical access to the network lines or any perimeter device is compromised, then all traffic on a private network may be compromised. These techniques are used by

criminals and information security professionals alike to obtain the same information. This information is utilized to find vulnerabilities in the devices or services found.

After the network reconnaissance stage is completed, an attack will typically begin with vulnerability scanning. This type of scanning will locate known exploits for the specific services being offered. There are several free vulnerability scanners (Lyon, 2006), but Nessus is the most popular one. Even though Nessus has recently changed licensing and is now a commercial product, it is still one of the most widely used vulnerability scanning tools. OpenVAS is an open source program that has many of the same features as Nessus, since it is a fork of that software. OpenVAS uses the same structured Network Vulnerability Tests (NVTs) as Nessus does to identify security problems in remote computers and appliances. However, Nessus provides many more NVTs than OpenVAS currently offers. Microsoft Baseline Security Analyzer (MBSA) is another popular and free tool that can provide limited security testing. MBSA testing includes finding missing patches for the namesake's software and reporting of the security settings discovered on workstations and servers running Microsoft Windows operating systems. There are commercial tools which accomplish similar tasks that the free tools perform and add advanced features like scheduling, automated exploitation and reporting capabilities. QualysGuard, McAfee Foundstone, eEye Retina, and ISS Internet Scanner are among the most popular of these commercial tools. When vulnerabilities have been discovered, the next stage is to execute the steps necessary to prove the vulnerability exists.

Exploiting vulnerabilities use to be reserved for only the most technically savvy of people, but now software tools allow anyone with minimal computer skills to perform difficult exploitations. Commercial tools like Core Impact and Immunity Canvas will not only find vulnerabilities, but also perform the exploit to prove the vulnerability exists. Metasploit is a free tool that can perform exploits on certain known vulnerabilities and is a framework used to create new exploits. Software purchased on the black market for exploiting vulnerabilities includes updating features that provide fresh attacks as criminals try to stay ahead of the curve. One such exploit kit is named MPack (Sachs, 2007), used primarily for spreading malware. Scanning, detecting vulnerabilities, and performing the exploit to compromise a network device are the primary threats the

network perimeter needs to circumvent. However, penetration is not always the goal of a criminal and not the only way to retrieve confidential information from hosts on a private network.

A Denial of Service (DoS) attack will either exploit a vulnerability or send a flood of packets to an address that overloads the device preventing it from responding to legitimate service requests (Franklin, July 2000). A more effective variant of this attack is called a Distributed Denial of Service (DDoS) attack, which floods a single IP address with massive amounts of data packets that originate from many different hosts (Strickland, 2007). The source of packets typically comes from zombie computers, or computers that have been taken control of by criminals. The zombies create a "botnet" under the direction of "command & control" servers that are administered by these criminals. The DoS on a website or email server can stop a business from performing vital functions for its customers, employees, or vendors. A DoS attack will commonly be accompanied with extortion for money to stop the attack. For community banks, a DoS attack is not a grave threat, as their customers can visit branches and ATMs to perform the same tasks as they do online. However, management should keep in mind the impact a negative reputation can have on customers when an outage of Internet services occurs. Although a DoS attack is not a serious threat to community banks, protecting the customer's data is vital to these banks and criminals have many ways to get at this data.

2.2. Alternative Attacks

A computer virus is not the only type of malware program. Trojans, worms, backdoors, root kits, key loggers, screen scrapers, spyware, adware, and dialers are among the other types of malware (Walsh, 2005). Because malware attacks have been on the rise, antivirus vendors have begun to include antimalware features into their antivirus products. Most malware is designed to gather information for criminals. Criminals are interested in confidential information, mainly personal identifiable information of customers such as: social security numbers, credit card numbers, and bank account numbers. This information alone can cause a customer's credit to be ruined, but combined with customer's public information such as their full name and address a criminal can take over their identity. Besides gathering information, malware programs

can also discover credentials that can aid a criminal in obtaining access to confidential information. Malicious websites are set up by criminals to steal username and password credentials using phishing. Phishing attacks lure victims to a website that masquerades as a legitimate authentication web page that the target recognizes (Wilson, 2005). Malware can be spread through emails directly by inserting malicious documents or programs as attachments. Legitimate websites are also vulnerable to exploits that can cause visitors to become infected with malware. A lot of vulnerable websites exist because security for programming methodologies is nonexistent or inadequate. Worm malware programs will propagate through a network finding all vulnerable computers in order to take control of them. A root kit is a malware program that hides itself on the host it has infected. Root kits are typically accompanied by key loggers and screen scrapers to capture sensitive information. A key logger will capture all of the user's keystrokes, which include usernames and passwords. A screen scraper will take snapshots of the screen just as the user sees it, which includes potentially confidential information. This can include capturing screen shots when a mouse click is performed for login screens with virtual keyboards.

Although malware has become popular among criminals, the phone system has been and continues to be another avenue of attack. Modems, PBX systems, and VoIP systems are at the boundary layer of a private network and vulnerable to attack. When the Internet was budding, phone modems were used to connect computers together to establish a network. Even though most of them have been replaced, phone modems and modern phone systems are still vulnerable. War dialing is used to dial a large block of phone numbers and search for interesting responses. A criminal's main interest is a computer, Private Branch Exchange (PBX), or Voice-over-IP (VoIP) system. A PBX can be compromised and used for profit by criminals who illegally sell discount long distance rates ("PBX hacking moves", 2009). New VoIP systems are replacing PBX systems, but criminals have similar reasons for targeting them. A free tool named Warvox can speed up the process of war dialing by using VoIP lines (Lemos, 2009). Unfortunately, security for phone modems and systems can easily be over looked because phone modems are infrequently used and phone systems are often rushed through implementation to quickly reap the benefits of these systems.

There currently are many known threats to the network perimeter and new threats are found every day. The ingenuity of criminals and number of vulnerabilities found in the perimeter suggests this trend will continue for some time. As new attacks are launched, businesses large and small have to respond. These responses have allowed IT Security professionals to establish the best practices to be used to keep a private network as secure as possible.

3. Composition

The design of the network for each community bank will be different, but all of them should contain essential security characteristics to protect the network perimeter. These basic features of the network perimeter should exist in some form to secure all private networks. No matter who is servicing this network perimeter, the internal IT department or an outsourced third-party provider, a company must put these best practices in place. The more simplistic the design the lower the cost will be for initial setup and continued maintenance. As networks grow and services are added to the network, changes in the perimeter are required to keep the network secure. If a company requires or permits Internet access, then an Internet connection will need to be established for internal hosts to communicate with external servers.

3.1. Basic Components

The Internet Service Provider (ISP) will establish the connection between the Internet and a company's private network. This is where the network perimeter layer will be built. The connection will be established from the ISP to a company's router, which serves as a central point where data is transferred between the networks. ISPs use a variety of medium to connect to this Internet Gateway Router, otherwise known as the gateway.

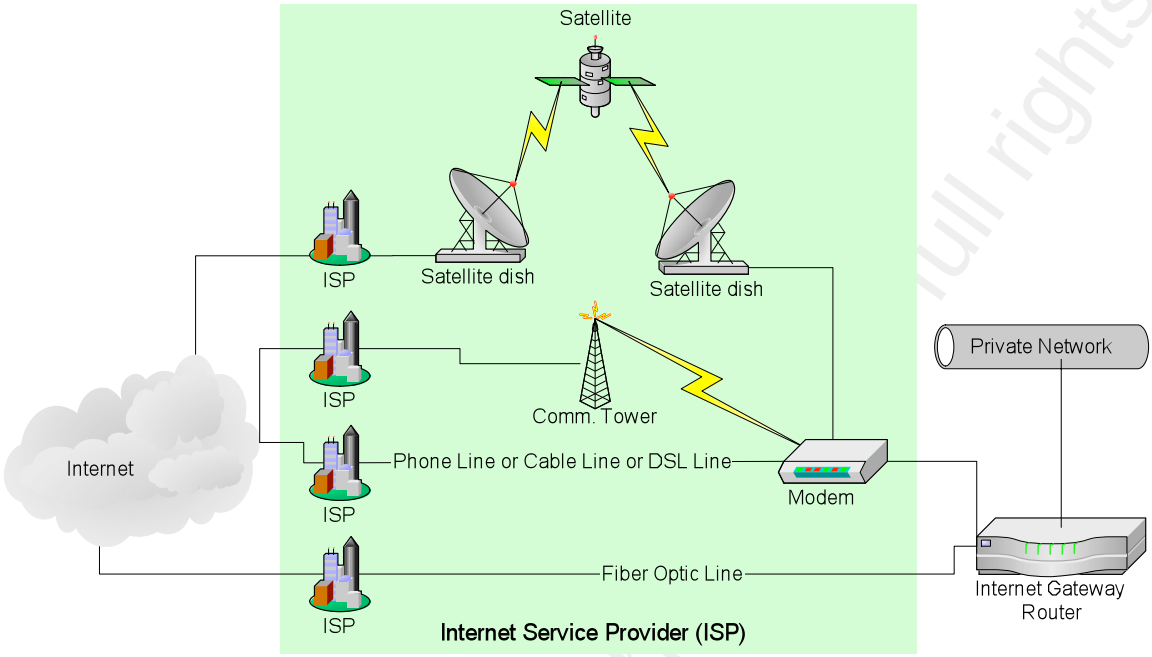

Diagram A. Different ISP methods of delivery for Internet access to their customers.

Modems provide the communication capabilities between the ISP and the customer. Phone modems were the first consumer methods of Internet access and are rarely used today due to their slow connection speed. Cable and DSL modems are the most popular methods of connection and are referred to as broadband. Cable connections use the cable company's coaxial line to share access to the Internet among many subscribers (Franklin, September 2000). DSL uses phone lines to provide a direct line to the Internet that can have a variety of connection speeds depending on the technology used (Franklin, August 2000). A satellite modem transmits a wireless signal between a dish connected to the customer's facility, to a satellite in orbit around the earth, back to a dish connected to the ISP's facility. A wireless modem can be used with an ISP that provides an Internet connection using a communication tower that emits radio signals. Wireless connections can have a variety of speeds depending upon the wireless protocols in use and the distance between the tower and the modem. A fiber optic line connects directly to the gateway and provides the greatest connection speeds. A T1 line is the most commonly used fiber optic cable ("How does a T1 line work?", 2000). As connection speeds increase for these network bridging conduits so does the price. Every established ISP connection has a single IP address that facilitates the sending and receiving of network traffic that consists of data packets, thus establishing the connection to the Internet.

Steven M. Launius, SteveLaunius@gmail.com

When an ISP assigns this static IP address to a company they can expose a bank's information in the domain registration. Anyone can query the domain registration by using WHOIS (Kayne, 2003) as this is publicly available information. This may seem harmless but any information identifying this publicly available IP address as a bank in the domain registration will make it an attractive target to criminals. Even seemingly mundane information such as an employee name, phone number, and email address can provide a criminal with valuable information useful in social engineering attacks.

The gateway router directs the network traffic to and from modems so internal hosts can communicate over the Internet. The router accomplishes this task by using Network Address Translation (NAT) (Tyson, 2001). NAT permits all Internet traffic to flow through a single router for many hosts on a private network. This is accomplished by transposing the public IP address, given by the ISP, into the source field in the header of all data packets leaving a private network. Conversely, when network traffic is received from the Internet, the router will insert the appropriate private IP address into the destination field of the packet header so that the correct internal host receives the correct data packets.

A firewall is the traffic cop for a network perimeter, making it the central point of defense in the network perimeter layer. Firewalls can be simple or complex and come in the form of software that runs on top of an operating system or as an appliance. Firewall appliances provide the greatest speed as the software and hardware are custom built for this purpose. Their cost will depend on how much bandwidth the firewall can handle without losing or delaying any traffic and the features installed. The network perimeter should contain firewall appliances that can standalone or be combined with other devices, such as a router.

There are several different types of firewalls, each solving a different problem of how to police traffic on the network. A static packet filter firewall is the simplest of firewalls and can be found in a router or can be a standalone appliance (Mateti, 2008). This type of firewall filters network traffic by blocking network packets based on the information in the packet header. If configured to block all incoming traffic, then almost all scanning from the Internet can be blocked. Stopping connection request from entering

a private network is a simple rule set, but not always possible as some companies will host their own web or email servers and provide remote connections for vendors or employees. If a company provides any of these external services, rules can be configured to allow Internet originating traffic to reach the appropriate server. Static packet filtering can also block unwanted traffic leaving a private network. Most inbound and outbound traffic should be blocked unless it meets the standards established by a company. These standards need to specify which software can be used on a private network so that the appropriate outbound rules can be formulated. These rules can allow or block web browsing, instant messaging, or other network traffic from leaving a private network. Network traffic originating from a private network that contains an IP address which is not used internally, called IP spoofing, should also be blocked from leaving the perimeter. This type of traffic should normally not appear on the network and is potentially harmful; blocking it is considered being a good Internet neighbor. Since static packet filtering firewalls looks at the header information of the data packet, this type of firewall is the fastest type. However, all traffic appearing to be part of an already established connection is passed through the firewall, whether or not the traffic originated from this interface. Because of these limitations this type of firewall is not typically deployed independently, rather it is often found as a feature in a stateful inspection firewall or router.

A stateful inspection firewall (SIF) maintains a record of all traffic leaving a private network in order to allow only traffic that matches the corresponding outgoing requests. This is similar to NAT mentioned above but matches all incoming traffic with a corresponding outgoing request. SIF products typically include a static packet filter feature to provide a complete package for their appliance. This type of firewall can block any type of scan initiated from the Internet and prevent IP spoofing with minimal configuration. SIFs are the most common firewalls used today. Because more data is inspected with SIF, as compared to static packet filters, they are slower. But with the processing capabilities possible today, low cost SIFs can easily handle large bandwidths.

A proxy firewall acts as the middle man in the communication session between two hosts and can protect from application layer attacks. A private network host will communicate with the proxy that resides on the network perimeter and the proxy will

communicate with the Internet host on behalf of this internal host. This means all the network traffic is stored on the proxy allowing filtering rules to be applied at the application level. This makes the proxy firewall the slowest type of firewall. However, since the proxy contains a copy of all requested network traffic any request made for the same information by another host on the same network can be returned quickly, which is called caching. An encrypted session, such as SSL, will not be subject to caching or inspection by the proxy. Many proxy firewalls exist for specific applications that have network capabilities. A web application firewall is a type of proxy firewall that inspects all traffic sent to and from a website looking for malicious activity. This type of firewall will examine the network traffic for a specific application looking for any web application attacks. A spam filter is another example of a proxy firewall. The spam filter will monitor all email traffic on a private network and classify emails as spam based on the application layer filters. The proxy is the most complex of the firewalls which often makes it the most expensive as well.

An intrusion detection system (IDS) or intrusion prevention system (IPS) augment firewalls by analyzing network traffic and matching patterns to identify malicious activity. An IDS or IPS can monitor both the traffic that is allowed in through the firewall and the traffic leaving the network for potential malicious activity. This permits the discovery of infected computers on a private network. The IDS provides detection of possible network intrusions or attacks by notifying the administrator. This is considered safer than stopping potentially critical business network traffic as an IPS would do in case of a false positive. These systems can monitor network connections at the host or the gateway to the Internet. A host based system can provide thorough coverage for hosts that are being monitored, but can be costly even for a small network. A network based system residing on the network perimeter will monitor only the traffic traversing the perimeter and provide the most economical complement to a firewall.

A Virtual Private Network (VPN) provides a secure remote connection for a host outside a private network by using the Internet to connect. Securing the remote connections for employees or vendors is vital for banks protecting its customer's information. The VPN allows for this secure connection by establishing an encrypted tunnel between a host on the Internet and a company's Internet gateway (Shinder, 2001).

This tunnel creates a virtual network by allowing private network resources to be shared with a host across the Internet. A VPN is commonly included with firewall appliances and provides a path through the firewall for users with the correct authentication means. Most network administrators will setup users with a username and password to authenticate. Sometimes network administrators will install a digital certificate on the host connecting to the VPN and this certificate holds a digital key that allows the connection to the VPN. Some VPNs use authorization which allows network administrators to give certain permissions on a private network to certain users. VPNs are the most common method of remote connections, but a remote connection can also be an unintentional consequence of technology.

A wireless network, called Wi-Fi, can extend a private network where wires will not reach and provide a convenient remote connection for wireless computers (Brain, 2001). Since Wi-Fi uses radio signals, it opens an access point into a private network that can be obtained from outside a facility. Therefore, protecting this access point is critical to the security of a private network. Many Wi-Fi access point devices, called Wi-Fi routers, come with firewalls built-in; however, if none is present then these devices should be connected to the perimeter firewall device before entering a private network. Wi-Fi routers support different encryption protocols to transport the data traveling on the radio signals securely. Several of the old protocols have been found to be vulnerable and should no longer be used, such as WEP ("WPA vs WEP", 2009). The encryption protocol that is commonly used and currently secure today is called WPA2 and should be used on all Wi-Fi routers. Even this latest protocol lacks the assurance of reliability because of its underlying structure ("WPA vs WPA2", 2009), so it is important to upgrade to the latest secure encryption protocol when it becomes certified by security professionals. Wi-Fi routers come with a default wireless network name or identifier called SSID. Changing the SSID name can help prevent anyone from identifying the type of router being used. Most Wi-Fi routers also allow you to hide this network name. There are tools that can find hidden wireless network names, but a hidden SSID prevents unintentional connection attempts. The location of the Wi-Fi router is important as well. A Wi-Fi router located near the center of the facility may have some signal leak outside the facility. But when located near a window or exterior wall the wireless signal may be

picked up across the street, in nearby buildings, or even inside homes. With the Wi-Fi located centrally in the facility a criminal would most likely need to be in the parking lot or closer to the facility in order to obtain a strong enough signal to attempt breaching this router.

The phone system can provide a path for criminals to enter a private network, abuse this resource, or gather information. Whether it's a Private Branch Exchange (PBX), Voice-over-IP (VoIP) system, a Remote Access System (RAS), or single modem connected to a computer, phone systems can provide access to a private network. Vendors often have access to the phone systems they set up in a company's facility and this access needs to be controlled by a company. Phone modems should only be powered on or connected when they are needed.

Filtering technology has been maturing and has become a very useful and economical solution for containing confidential information and preventing malware. Filtering is used in many different appliances to monitor the network traffic for particular criteria and either allow or block this traffic. Filtering can also be performed using a blacklist or a whitelist. A backlist is used to keep track of known threats, like a malicious website, and prevent the user from accessing it. A whitelist is used to keep track of acceptable items, like websites that users are allowed to visit. Blacklisting is a reactive response to malicious activity and dependent upon frequent updates to the list, usually performed by a third-party vendor. Whitelisting is a proactive response to malicious activity since the management of a company must decide what is acceptable. A whitelist only needs updating when a new item is approved. Vendors have many robust standalone hardware appliances mostly for the popular email and web traffic. Email filtering technology has been used for years to stop spam email messages using criteria and blacklists created by users and third-party vendors. Email filtering can also be used to stop confidential information from accidentally or intentionally leaving a private network (Skoll, 2009). Web filtering can be used to limit the pool of available websites that employees may browse, thus reducing the risk of infection by malware. Such web filters have typically used blacklists, but need constant updating to include the latest malicious websites. Since processors speeds have dramatically increased, filtering

technology has been combined with many perimeter appliances increasing their features without decreasing performance.

Secure management of these hardware perimeter devices is very important since they protect access to a private network. Most of these devices have a default administrator username and password. These usernames and passwords may be blank or short dictionary words and can easily be found by searching the Internet. Selecting a strong password for all network hardware devices will ensure only a company can modify their configuration. Additionally, restricting management of these devices to a single, internal IP address or subnet will further enhance security by guaranteeing only the network administrator can make configuration changes. It is also recommended to change the default configuration of some appliances which allow remote management from external sources. Once these devices have been configured and the security has been verified through an audit, their configuration should be backed up. This ensures that the same settings can be restored in case the device fails or is replaced. Firmware updates are released by the manufacturer to patch bugs or vulnerabilities found with hardware devices. Firmware for network perimeter devices should be kept up-to-date as a vulnerability in one of these devices can compromise the entire network.

Log monitoring is necessary to find intrusions into a private network. Each of the network perimeter devices described above have logs generated by the activity they monitor or block. In order to properly interpret and correlate events a trained technician should be employed. Although alerts to malicious activity will be present in these logs, only a human can interpret the events from these devices to conclude an actual intrusion occurred. Management should receive regular executive summary reports from the review of these logs to stay apprised of the security of their network. Security Information and Event Management (SIEM) systems can correlate logs with an event associated with network activity. This can provide more clarity than just monitoring long log files and can help identify the most probable attacks on a private network. SIEM systems are more useful in larger networks that have complex perimeter configurations and are often too costly for smaller banks.

3.2. Designing the network perimeter

Assembling the perimeter devices discussed above to protect a private network is key for implementing the perimeter security. The choices for the devices will depend on many factors for each company, but the essential devices that must be included to accomplish this task are a router and firewall. The router will serve as the first line of defense and the firewall will act as the traffic cop allowing only the desired network traffic. An IDS or IPS should be included in the perimeter to detect and stop any malicious activity on a private network. The overall network perimeter complexity will depend on the services provided over the Internet.

A simple network where no Internet services are provided to customers will be the easiest to defend. The router and firewall separate the Internet from a private network, the IDS or IPS monitors all traffic, and the VPN provides remote access; all of which provide the necessary defense-in-depth features for the perimeter.

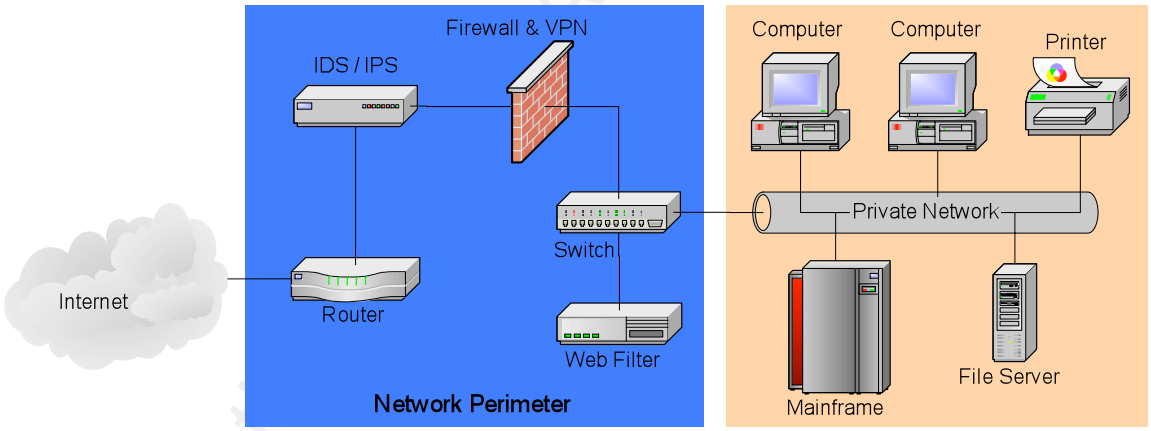

Diagram B. A simple network with no email or web servers hosted on a private network.

Configuration of the firewall rules for such a network will be straightforward. The firewall has two main sets of rules called ingress and egress rules that determine what network traffic is allowed to enter and leave, respectively, through this appliance. Almost all the network traffic attempting to connect to a company's private IP address should be blocked by the ingress rules, using static filtering, of the router or firewall. An exception needs to be made for remote connections if permitted by a company. Remote connections should use a secure connection like a VPN to connect. The VPN may be integrated with the firewall or provided by a separate appliance residing behind the

firewall. Either way ingress rules will need to be configured to allow this traffic to connect. A 'ping' program determines if an IP address is currently active. This 'ping' uses a special protocol, called Internet Control Messaging Protocol (ICMP). Although, ICMP is used primarily to determine availability of network resources and to troubleshoot latency problems on a network, it can also be used maliciously (Shinder, 2008). Most firewall analysts recommend dropping ICMP packets at the gateway or at least using filtering rules to permit only essential packet types from this protocol, such as those necessary for IPSec and PPTP. The ingress rules will also need to allow network traffic that is in response to a private network request. Web browsing, email, and instant messaging are examples of such network traffic. The firewall's ingress rules, using stateful inspection, allows for this type of network traffic. These ingress rules work in conjunction with the firewall's egress rules that allow traffic to leave a private network. Management can use their policy on Internet activity to determine the rules for the type of network traffic that is allowed to leave. For community banks it is common to allow web traffic out, but to deny instant messaging traffic. This allows employees to browse the web, but limits their ability to use business systems for personal activities. Only permitted traffic should be allowed to leave while all other traffic should be denied from exiting a private network. This will protect a company from employees initiating remote communications and using unauthorized Internet capable applications. However, if web traffic is allowed through the perimeter then there is an increased risk since this traffic can carry confidential information or malicious programs. A web filtering appliance can be used to reduce the risk of visiting a malicious website or transmitting confidential information. This appliance can also provide management with reports on what type of websites employees are visiting while browsing the Internet. A network switch is a hardware appliance with the sole purpose of directing network traffic to its intended recipient. A switch can direct the web browsing traffic to the web filter so it is not overloaded with superfluous traffic.

Traffic Type	Ingress	Egress	Action
Session (traffic in response to a request)	Private		Allow
ICMP	Private		Deny
Remote connections via VPN	Private		Allow
All other	Private		Deny
Web browsing		Private	Allow
ICMP		Private	Allow
All other		Private	Deny

Table A. Summary of firewall rules for a private network.

When web and email services are hosted by a community bank, a more complex perimeter design needs to be used in order to provide a secure perimeter. Web and email servers are more vulnerable to attack because of intricate configurations and unsatisfactory programming methodologies that fail to plan for security from the start. These servers need to reside somewhere on a private network, but isolated so communication with internal hosts is denied. This isolation is commonly accomplished by using a special subnet called a Demilitarized Zone (DMZ). One way of implementing the DMZ would be to use two firewall appliances and placing the DMZ subnet in between them. The additional cost and maintenance of this design can only be justified for networks with significant bandwidth. Typically the DMZ is implemented using three network interfaces on the firewall appliance used for the Internet, DMZ, and private networks. Because the DMZ network and the private network are not physically connected an IDS or IPS appliance can be placed in front of the firewall in order to capture all network traffic. Since Internet traffic will be allowed to connect to servers hosted by a company, they are confined in a DMZ. Confinement in a DMZ prevents this potentially malicious traffic from entering a private network. An anonymous SMTP relay server placed in the DMZ allows emails from outside the company to be received and forwarded to the internal email server on the private network. This protects the internal email server from abuses it may face. The SMTP relay server will take the brunt

of abuses since anyone can connect to it for the purpose of sending and receiving email messages. This includes manipulating the server to send spam emails anywhere on the Internet if it is not protected properly. Providing email is a crucial business function, so these issues can best be alleviated through the use of an SMTP gateway appliance. An SMTP gateway will monitor all email messages sent to and from the SMTP relay server to detect and block spam email messages. This appliance may also include features to detect and block confidential information. Placing the SMTP gateway in just front of the SMTP relay server restricts the traffic monitored by this appliance to only email messages.

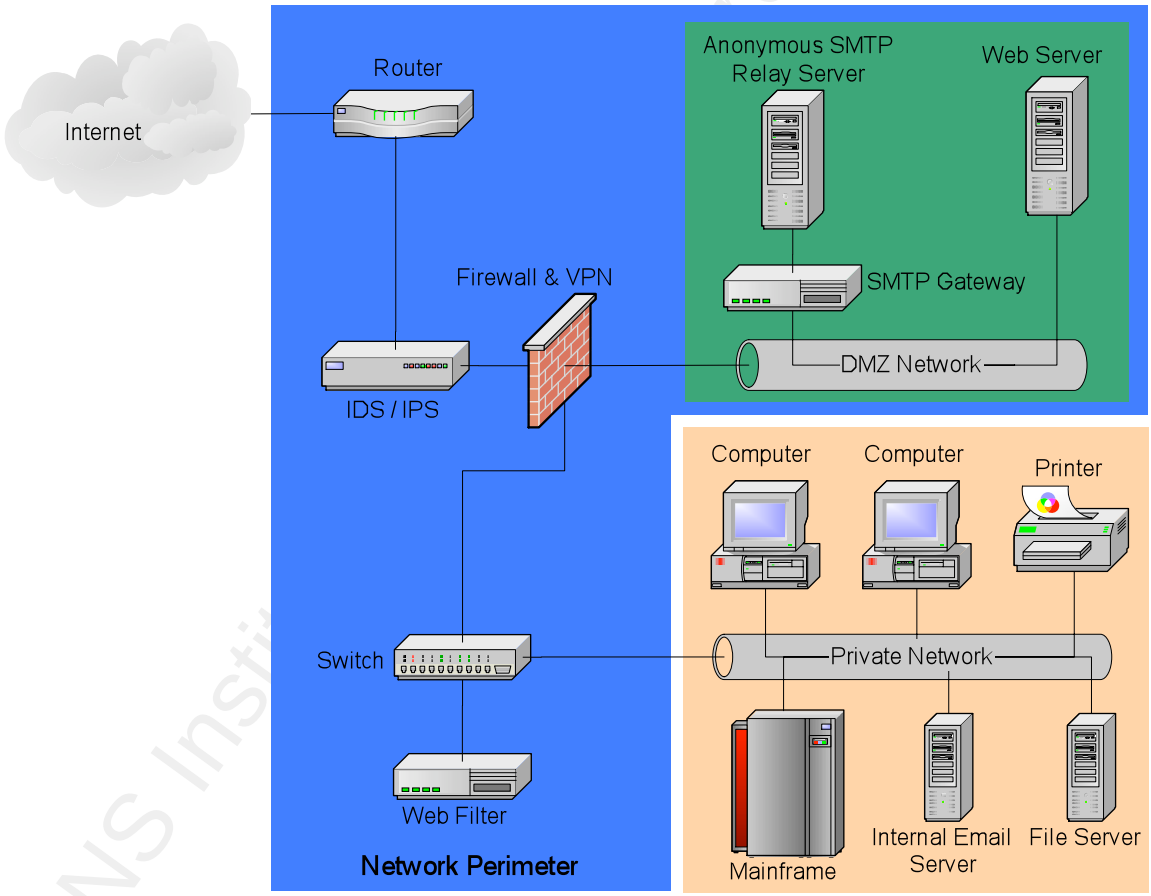

Diagram C. A network with email and web servers isolated in a DMZ.

A DMZ attached to the firewall will create two sets of ingress and egress rules, one set for the DMZ and one set for the private network. Because servers in the DMZ will remain vulnerable to Internet risks, persistent connections between the DMZ and a private network should be blocked by the firewall rules. The DMZ ingress rules will

need to permit web and/or email traffic that initiates a connection. The DMZ egress rules will need to allow outgoing email connections and the traffic from an established session with the web server. The ingress rules for a private network will need to block all traffic including the ICMP protocol and DMZ originating requests. The egress rules for a private network need to permit email traffic destined for the DMZ and the ICMP protocol. Already established connections also must be permitted in the ingress rules of both networks using the stateful inspection capabilities of the firewall.

Traffic Type	Ingress	Egress	Action
Session (traffic in response to a request)	DMZ		Allow
ICMP	DMZ		Deny
Web page requests	DMZ		Allow
Arriving email messages	DMZ		Allow
All other	DMZ		Deny
Sending email messages		DMZ	Allow
Web page responses		DMZ	Allow
All other		DMZ	Deny
Session (traffic in response to a request)	Private		Allow
ICMP	Private		Deny
Remote connections via VPN	Private		Allow
All other (including from the DMZ)	Private		Deny
Web browsing		Private	Allow
Sending email messages to DMZ		Private	Allow
ICMP		Private	Allow
All other		Private	Deny

Table B. Summary of firewall rules for a private network with a single DMZ.

One downside to a single DMZ design is that data stores residing on a private network are inaccessible to any servers residing on the DMZ network. If a data store has to be accessible by a web server (for example to provide an Internet banking system) then there are at least two secure scenarios. The first scenario involves manually connecting to the web server to upload a static data store and retrieve transactional data changes. An egress firewall rule allowing an internal IP address to connect to a secure FTP server running on the web server is a secure implementation of this scenario. The second scenario involves creating two DMZs to separate the "publicly" available information from the private by using DMZ networks called anonymous and authenticated. This design can be implemented using a firewall with four network interfaces. Authentication should be used to permit a internal IP address access to a secure FTP server residing on the authenticated DMZ network. All connections made to the authenticated DMZ need to require an encrypted channel and account credentials, which a secure FTP server achieves. The egress and ingress rules between the two DMZs need to be configured to allow access to this data store by the web server. This will provide the web server residing on the anonymous DMZ network with the ability to present the information in the data store and record changes performed by users. This anonymous/authenticated DMZ design also permits scaling as the network grows. Additional servers can be added in the appropriate DMZ network depending upon their services. A public DNS server provides anyone on the Internet with the ability to locate a company's web and email servers. The public DNS server, web server, anonymous SMTP relay server, and SMTP gateway will go in the anonymous DMZ. A frontend email server, called webmail, can provide out of network email access for employees without giving complete access to the private network. This webmail server belongs in the authenticated DMZ with the secure FTP server (Shinder, 2006).

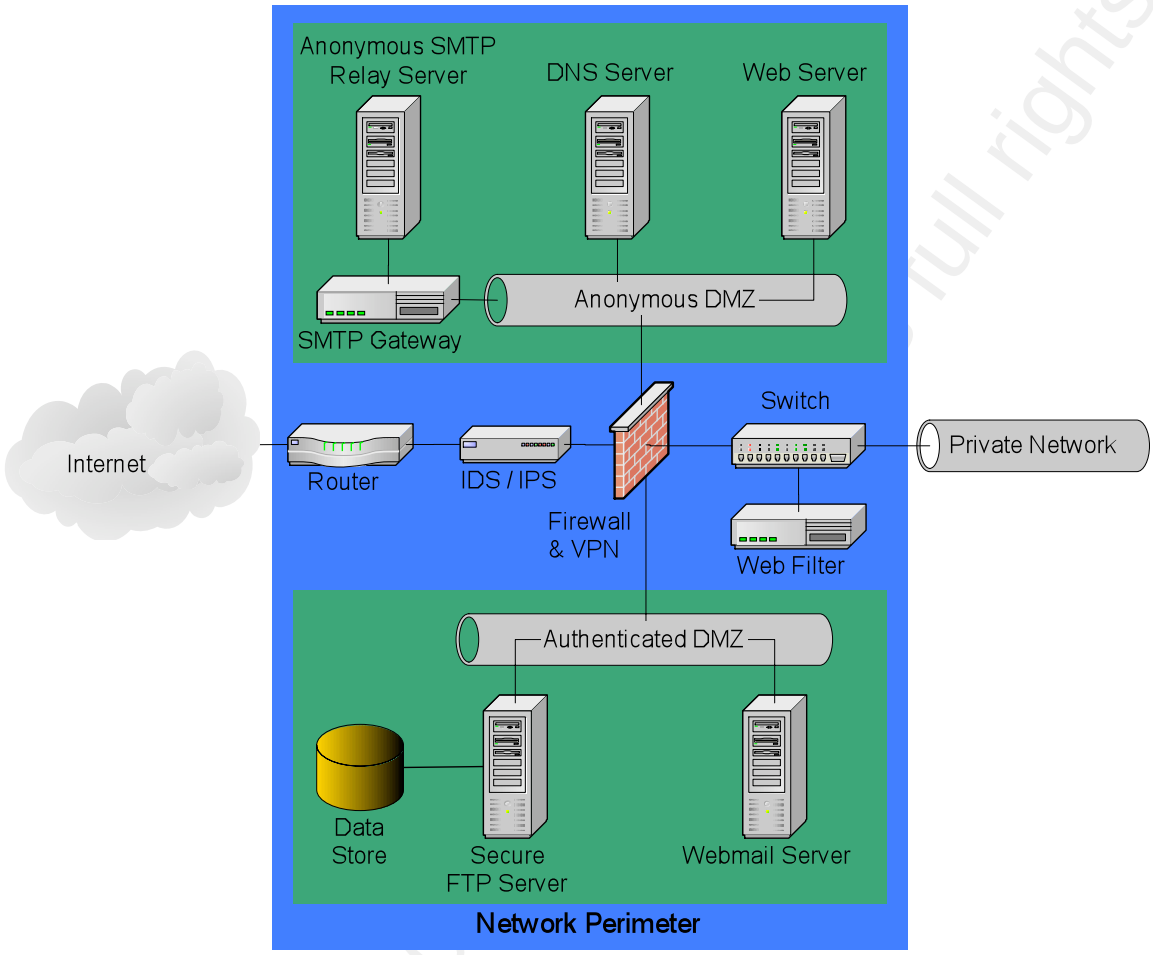

Diagram D. A dual DMZ design is used to separate public and private information.

Another drawback to a single DMZ design is that all servers residing together on the DMZ network are at greater risk if any of the other servers on the same network are compromised. This is a problem that an individualized DMZ design can resolve, but by imposing such tight security much overhead will be created. This design will assign each server its own DMZ that can have customized firewall rules to match the security suited for that particular server. This is implemented using a firewall and switch that support Virtual Local Area Network (VLAN) technology. VLANs separate network traffic, like a router would, between different logical network segments defined by assigning subnet traffic to a particular port on a network switch. Separate ingress and egress rules for each DMZ VLAN will need to be established to accommodate the specific communication channels of each server. This type of design is complex which increases the odds for mistakes to occur during implementation and maintenance. The IDS or IPS appliance is

still monitoring all network traffic entering and leaving the private network, because of its placement in front of the firewall.

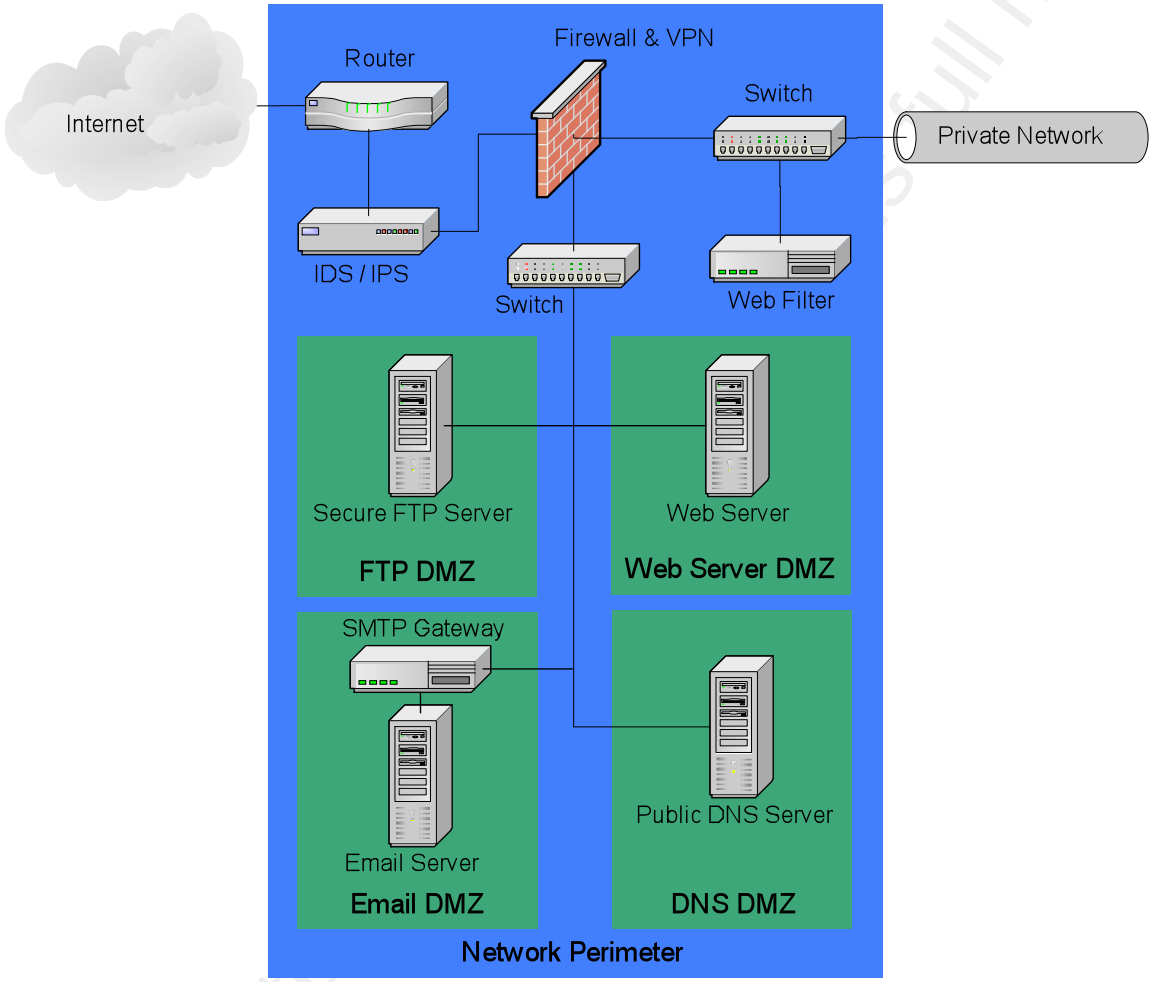

Diagram E. An individualized DMZ design has one server per DMZ.

The single, authenticated/anonymous, and individualized DMZ designs are all secure designs that provide the best protection for various network sizes. The single DMZ is respected for its simple design which separates itself from a private network. The authenticated/anonymous DMZ classifies servers and the data they protect in order to segregate servers that need strong access controls from the ones that do not. The individualized DMZ gives the greatest security for a mature network, but also has the highest setup and maintenance costs. All of these secure DMZ designs are susceptible to a poorly configured server which can allow a criminal access to a data store or worse, the entire private network. The larger private networks with abundant features will require

complex network perimeter designs, while simple private networks can implement designs that are straightforward and affordable.

4. Emerging Technology

Innovation for perimeter technology has been mostly stagnant until recently. As processor speeds increased, products have been able to increase the features offered in these appliances. Several technologies have emerged that may change how confidential information is protected on a private network. Some of these new technologies are complicated to implement and have exceedingly high costs. Before choosing any vendor to deploy a new solution always perform proper due diligence by inquiring about the experience other companies have had with a particular solution.

4.1. Data Loss Prevention

Data Loss Prevention (DLP) is a new technology designed to prevent a costly and public confidential customer data breach. DLP solutions aim to prevent confidential information from escaping a private network. Gartner defines content-aware DLP as

> "a set of technologies and inspection techniques used to classify information content contained within an object (for example, a file, an email message, a packet, an application, or a data store while at rest [in storage], in use [during an operation] or in motion [across a network]). It also describes the ability to dynamically apply a policy (for example, by logging, reporting, classifying, relocating, tagging, encrypting, or applying enterprise digital rights management[EDRM] protections)." (Ouellet, & Proctor, 2009, page 1).

Not only can DLP solutions create a clear picture of how confidential information is dispersed on a network and where it travels, it will also reacquaint employees with a company's security policies through notifications and denial of operations. DLP solutions typically fall in to one of two categories: an enterprise solution or a more basic single channel solution which is typically integrated with email and web proxies (Howard, 2009). The top rated enterprise solutions from Symantec Corp., RSA, and Websense Inc. consist of three channels: network (data in motion), host (data in use) and content discovery of data stores (data at rest) (Ouellet, & Proctor, 2009). Network DLP

systems normally only sit at the perimeter since deep packet inspection of heavy traffic loads, as private networks typically have, is not yet possible. This DLP gateway provides protection against all hosts whether being managed or not by a host solution. Host DLP systems involve an application that monitors and controls end user interaction with classified information. Content discovery DLP systems classify content on data stores ubiquitously on a private network. The enterprise solutions provide a central management console from which these three separate systems can be configured, controlled, monitored, logged, and reported. Compliance with regulations on securing customer confidential information and the maturity of products offered may allow premium prices for the enterprise solutions to become practical for community banks in the near future (Ouellet, & Proctor, 2009). Some single channel network DLP solutions that come integrated with other appliances are already affordable. For example, an email proxy that provides advanced filtering capabilities. As DLP is still relatively new, security analysts recommend developing well defined security policies as well as going in at a moderate pace during implementation. Since DLP solutions act as the "policy police", strict enforcement of the rules can potentially cause critical tasks to be blocked. Hence logging, reporting, and notification features should only be used until policies are adapted to management's preference before blocking commences. Security policies should also have a well defined data classification system because success during content discovery will depend on what data is classified as confidential. Of course, criminals will find ways around this new security technology, as they have all others, but knowing the weaknesses of this solution will help mitigate those risks. Encrypted information is one weakness of DLP since if the content cannot be read, it cannot be classified (Messmer, 2009). Data classification is currently limited to text, but could be integrated with document imaging systems in the future. A risk assessment can identify which risks can be managed using DLP technology and will help identify which solutions are economically feasible for a company. The current prices for enterprise DLP solutions will keep it out of the reach of most community banks. However, a single channel DLP solution might be a good fit for management to control a particularly high risk area.

4.2. Unified Threat Management

Advanced processors have allowed new appliances to perform more checks on the traffic flowing through the perimeter without a performance loss in bandwidth. Unified Threat Management (UTM) is the name of the next generation firewalls. These standalone appliances combine many security features into a single device (Cobb, 2009). UTM combines firewall, IDS/IPS, VPN, email and web filtering appliances.

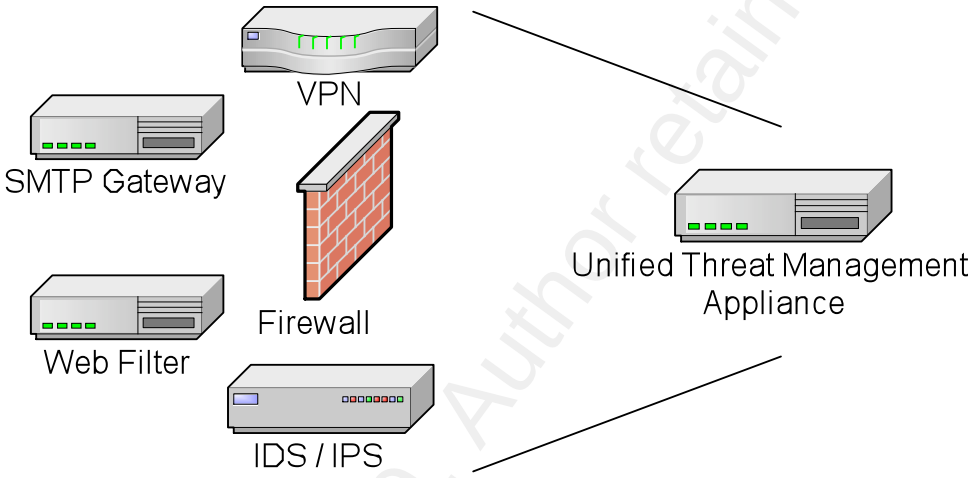

Diagram F. A UTM appliance combines perimeter technologies into a single device.

Advanced features are also found in UTM appliances. Antivirus and antimalware scanning has been limited to host computers until UTM came along. UTM can include filtering technology for several types of network traffic including web, instant messaging and email (Chee, & Franklin Jr., 2009). This technology does create a single point of failure which can be mitigated by redundant Internet connections and failover UTM devices. Most community banks will find redundant connections and failover devices too expensive to justify unless the Internet connection is vital to the operations of a bank. Because UTM appliances implement many advanced features in a single device, each feature that is enabled will reduce the bandwidth the appliance can handle. This is especially true of the antivirus and antimalware detection features since many packets must be reassembled on the appliance in order to peer into this application layer information. Because most community banks do not have large bandwidth requirements, UTM offers an economical and defense-in-depth solution in a single appliance for perimeter protection. Cisco, Checkpoint, Sonicwall, McAfee, and Symantec are

examples of companies that create such UTM products that may fit the budget of community banks while coping with all the necessary network traffic.

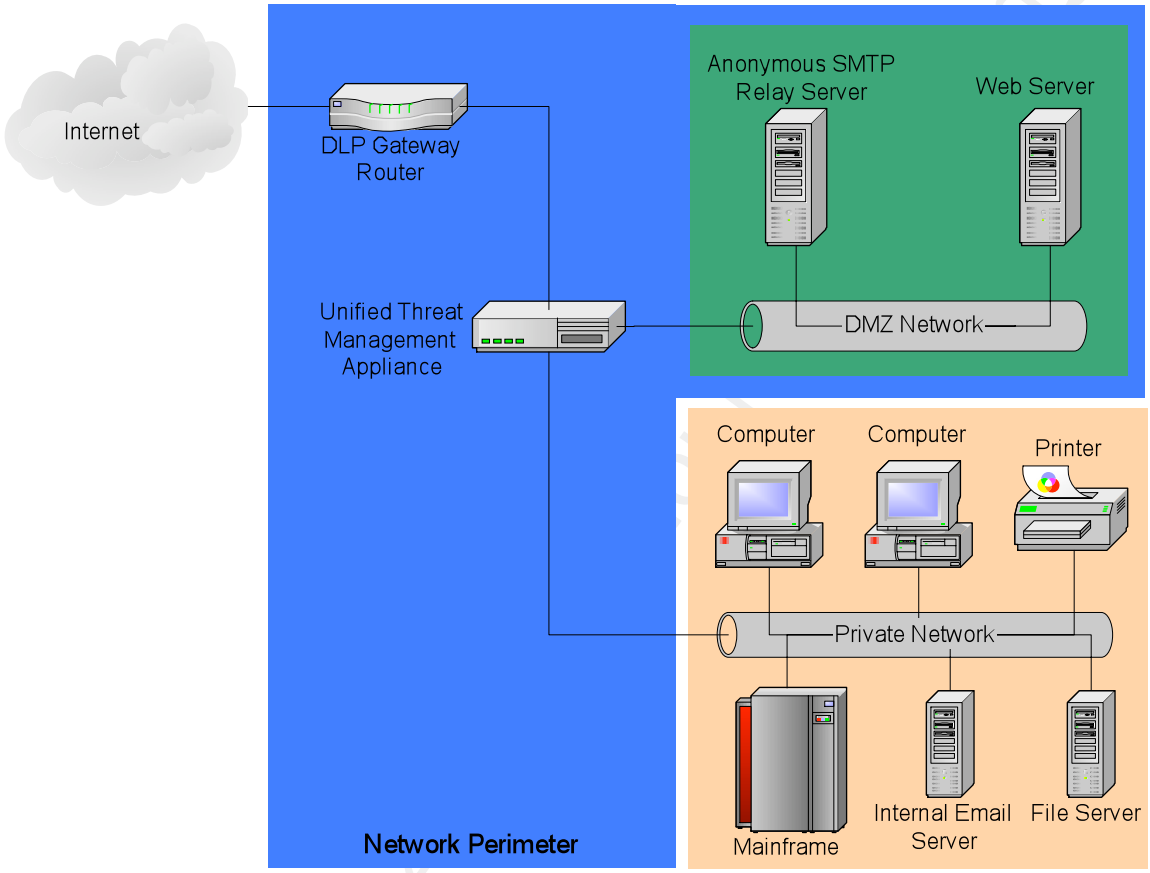

Diagram G. A network utilizing a UTM appliance and DLP technology.

4.3. Network Access Control

Cisco and Microsoft have developed technologies to extend the perimeter around workstations which establish connections to a private network. This is accomplished by determining the "health" of the hosts when they connect to the network and enforcing security requirements on them before access is permitted to resources on a private network. Two leading companies offering Network Access Control (NAC) solutions come from Cisco's Network Admission Control and Microsoft's Network Access Protection. NAC solutions are designed to allow servers to permit access based on the security status of hosts and authorization of accounts (Perry, 2007). They do this by determining the antivirus, antimalware, firewall and operating system patch status running on the host. Currently support for minority hosts such as Apple, Linux, and

UNIX operating systems is limited. This technology is difficult to implement in homogeneous environments with a single switch vendor and a uniform operating system, not to mention onerous to integrate in diverse environments (Jabbusch, 2009). This is due to the many integrated components necessary and because vendors have no interoperable standards for this technology. Each solution requires specific hardware and software running on the network that will lock the customer into that vendor's particular architecture (Conry-Murray, 2005). The NAC solutions are good for dynamic networks that have many hosts entering and exiting its network on a continual basis. However, community banks have mostly static homogeneous networks that can be managed adequately by enforcing hosts to have a standard configuration for their hardware and software. Smaller companies can monitor the patch management, antivirus, and antimalware systems by regularly reporting their status to senior management in order to maintain a healthy network. Because of the complicated implementation, exclusivity, and costs of enterprise NAC solutions, this technology will remain out of reach for most community banks in the near future.

The latest emerging technologies for perimeter protection will always demand premium prices, be complex to implement, and come with limitations. Several of these emerging technologies will not provide protection from network traffic that is encrypted. Look for solutions that remedy this problem by implementing encryption proxy features. Such a system will insert itself in the middle of encrypted communication channels in order to view the data being exchanged. However, this is an additional complexity that can be difficult to implement and maintain, not to mention expensive. As proxy technology for encrypted channels matures look for this feature to be included in many security solutions in the future. After a new solution is installed regular independent audits will verify that all of its systems are performing as intended and are being kept well maintained. Additionally, every system in any solution purchased should be backed up after its configuration is verified to be secure. This is in case a system fails or needs to be replaced. Managers of smaller companies will need to maintain and verify their current security systems are configured correctly until these new technologies mature enough to become viable.

5. Audits

Audits performed for the purpose of determining the security stance of a private network are known as security tests. Several publicly available methodologies for performing a comprehensive security test currently exist. The Open Source Security Testing Methodology Manual (OSSTMM) is one of the best known because of its thorough tests and is currently in its third version (Herzog, 2009). An OSSTMM audit can be used to verify compliance with the laws set forth in Gramm-Leach-Bliley Act, regulatory requirements imposed during examinations, and with a bank's internal IT security policies. Formal methodologies used to perform an IT security audit can prevent security breaches which inflict legal, reputational, and monetary damages.

5.1. Open Source Security Testing Methodology Manual

This OSSTMM audit classifies common types of tests and channels of attack to create the scope. The OSSTMM defines six of the many possible security test types by delineating between what information the auditor possesses of the target and what details the target has of the audit. Several of these test types are appropriate for community banks; a blind test is one such example. A blind test is performed when the auditor has no prior knowledge of the targets' defenses, assets, or channels of entry. The target will know the scope of the audit, the channels tested, and the vectors to be tested. Examples of blind tests include Ethical Hacking when auditing the electronic appliances of the network perimeter and War Gaming when performing social engineering and the facility's security when auditing physical security. A channel is the means of interaction with an asset and an asset is what has value to the owner. Assets can be physical property, like a firewall appliance or a server, or they can be intellectual property, like customer information or business processes. OSSTMM categorizes channels as physical security, spectrum security, and communications security. Physical security is composed of the human interactions whether they are physical or psychological and interactions with non-electronic objects, like the door to the server room. Spectrum security entails all wireless communication interactions, like Wi-Fi radio emanations. The communications security channel is comprised of the interaction of data with any electronic device on a network and interactions occurring over a telephone line.

The definition of the scope will determine the costs associated with third-party audits. The scope consists of targets as determined by the selection of channel, test type, and vectors. These targets are then indexed to allow for unique identification by the test vector. The vectors represent how the security of a channel will be tested. The more channels and vectors in a scope, the longer it will take to complete an audit. By excluding social engineering, or the human channel, community banks may reduce the time and costs a blind test will take. If the human channel is removed from the audit, management will be unable to properly implement controls for this risk, thus accepting a higher risk rating for this threat. An Ethical Hacking (EH) test performed on only the external vector is a good example that provides a limited scope. The EH test may be part of an external security assessment meant to exclude the physical security channel. This is a multichannel audit that performs a thorough security assessment of the external facing perimeter appliances. Testable assets include the external IP addresses, discovered phone lines, and any detected wireless networks. The Nessus tool, discussed earlier, can be used to complete many tasks in this audit, but such feature rich tools do not exist for all tasks. An important final module in the OSSTMM methodology is the review of alerts and logs produced during an audit. This verifies many of the tasks were actually tested providing a document trail for these tasks.

After the initial audit of perimeter devices following installation, audits of the perimeter need to be performed regularly by an independent auditor. Management and vendors have been known to expedite implementation of new network perimeter solutions to capitalize on the financial benefits. Because such a process is prone to mistakes, the initial audit will need to cover both internal and external vectors to be considered thorough. When new perimeter appliances are purchased or configuration changes are made then an audit evaluating both internal and external vectors will be necessary. New vulnerabilities are discovered regularly by security researchers, so responsible vendors will consistently update their appliance definitions to detect the latest threats. Performing an external security assessment on the perimeter at least annually is recommended and should be affordable since only the external vector is tested. Self-assessment audits could be used to verify rules configured for firewall, IDS and spam filtering devices. The audit needs to be performed independently from whoever installs,

configures, and manages the perimeter to ensure impartiality. If the custodian of the perimeter performs the audit, they may make assumptions and skip vital tests. By having an independent audit, management can be confident the auditor will report only the facts.

6. Conclusion

Any determined criminal can circumvent the security put in place to stop unauthorized access to confidential information. This is one reason why the budget for the IT department cannot be spent entirely on security. Implementing protections against the majority of attacks and keeping records of network activity will be the most economical means to protecting the network's perimeter and identifying intrusions. Using the best practices followed by the IT Security community can provide sufficient security for community banks.

Applying a defense-in-depth strategy at the perimeter layer of a private network is recommended to maintain a secure network. A router using NAT will be necessary for allowing many internal hosts to communicate over an Internet connection. A UTM appliance that incorporates several of the essential perimeter devices will be the most economical solution. The stateful firewall will be the central security feature in this layer providing protection from many attacks originating from the Internet. The firewall also enforces company policy by denying the communication of unauthorized network applications. An IDS or IPS feature will supplement the firewall by detecting potentially harmful network activity traversing the perimeter and help identify compromised hosts on a private network. The VPN feature will work with the firewall to provide secure remote connections. Web filtering features can protect host systems from employees browsing potentially malicious websites. An anonymous SMTP relay server will protect the internal email server, while a SMTP gateway will eliminate most spam from entering and leaving the SMTP relay server using filtering technology. These filtering features may also provide the ability to detect confidential information. While UTMs can include antivirus and antimalware features, they can bog down the scanning capabilities reducing overall bandwidth. Placing antivirus and antimalware on host systems can be more economical than purchasing a powerful UTM capable of handling all of these features

without greatly reducing bandwidth. The network switch will separate the traffic for the DMZ and private network VLANs.

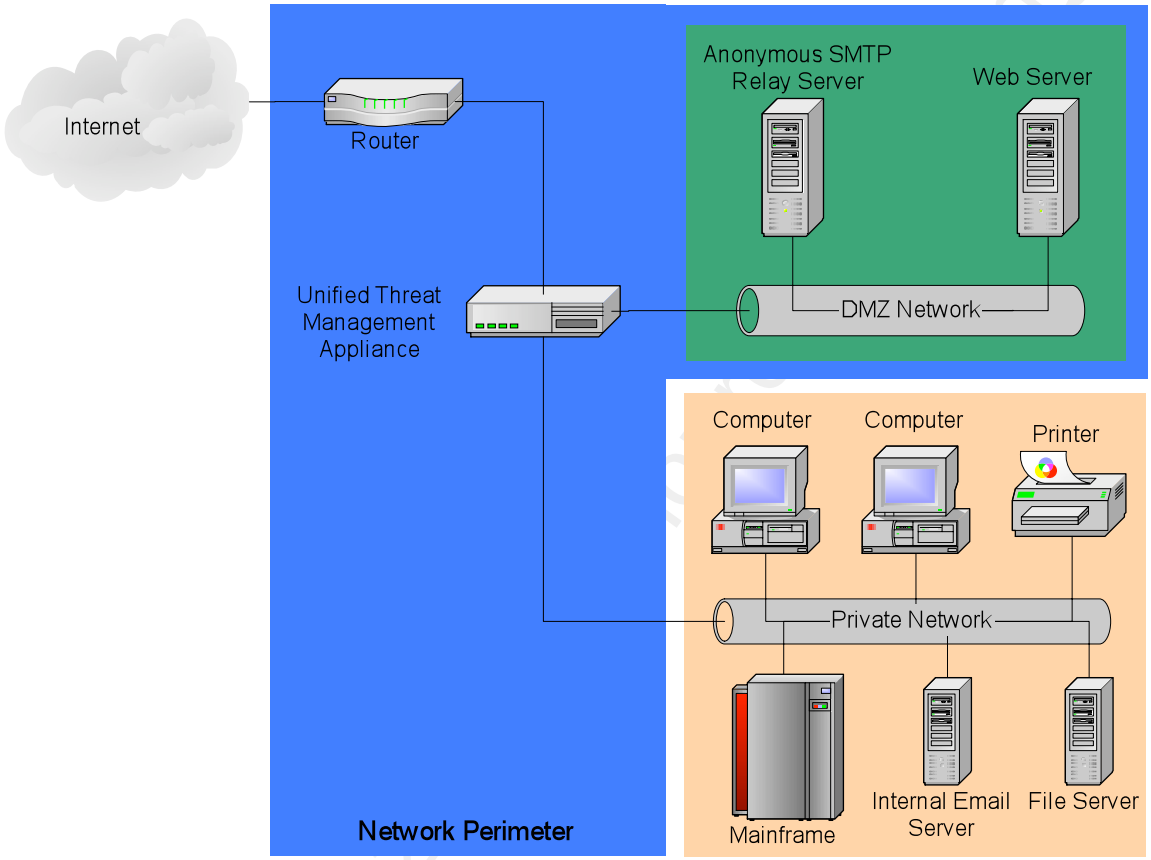

Diagram H. A recommended network perimeter configuration.

Monitoring and maintaining this perimeter can be accomplished with a few resources and trained IT professionals. All the devices should have their logs reviewed regularly in order to reveal intrusions into a private network. If a company does not have an employee qualified to perform this task there are vendors that offer this service. Performing regular audits with a proven audit methodology will provide complete security assessments of the network perimeter and give assurances that the appliances have been configured correctly. An independent audit performed by qualified IT professionals provides solutions and educational opportunity for IT management who wish to stay apprised of the perimeter security posture. Senior management needs to stay informed on the security stance of the perimeter by receiving executive summary reports from all log reviews and audit findings.

The Internet is a beneficial resource for community banks that brings risks with it, but these risks are manageable with solutions that are affordable. The solutions presented are industry best practices that IT Security professionals use to provide any network with perimeter protection. Without these protections the risk of confidential information being compromised is very high. The consequences can impact the reputation and bottom-line of a bank. The costs could be significant for notifying customers and providing protection to their credit, as well as the potential loss of business caused by a negative reputation. The U.S. government has taken these risks to financial institutions seriously enough to pass legislation enforcing controls that can mitigate those risks. Perhaps one day businesses in every industry sector will be required to provide the same protections to their customers no matter the size of a company.

7. References

Gramm-Leach-Bliley Act. Pub. L. 106-102. 12 Nov. 1999. Stat. 113.1338.

Richards, J. (2008, August 7). *Analysis: what is wardriving?* Retrieved July 12, 2009 from http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4470120.ece

Gunn, M. (2006, June 9). War Dialing. *SANS Institute InfoSec Reading Room*, Retrieved July 12, 2009 from http://www.sans.org/reading_room/whitepapers/testing/war_dialing_268

Mateti, P. (2008, May 22). *Firewalls / internet security lectures.* Retrieved July 12, 2009 from http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/Firewalls/index.html

McBride, G. G. (2009). *Integrated threat management*. Retrieved July 12, 2009 from http://www.infosectoday.com/Articles/Integrated_Threat_Management/Integrated_Threat_Management.htm

Brandel, M. (2007, October 10). *Data loss prevention dos and don'ts.* Retrieved July 12, 2009 from http://www.csoonline.com/article/221272/Data_Loss_Prevention_Dos_and_Don_ts

Lyon, G. (2006). *Top 10 vulnerability scanners.* Retrieved July 16, 2009 from http://sectools.org/vuln-scanners.html

Walsh, J. (2005, October 21). *Malware: computing's dirty dozen.* Retrieved July 27, 2009 from http://www.sitepronews.com/archives/2005/oct/21.html

Franklin, C. (2000, July 31). *How routers work.* Retrieved July 27, 2009 from http://computer.howstuffworks.com/router.htm

Strickland, J. (2007, September 10). *How zombie computers work.* Retrieved July 27, 2009 from http://computer.howstuffworks.com/zombie-computer3.htm

Wilson, T. V. (2005, November 23). *How phishing works.* Retrieved July 27, 2009 from http://computer.howstuffworks.com/phishing.htm

Sachs, M. (2007, June 20). *MPack analysis.* Retrieved July 27, 2009, from http://isc.sans.org/diary.html?storyid=301

(2009, June 15). *PBX hacking moves into the professional domain as arrests stack up.* Retrieved August 1, 2009 from http://www.infosecurity-us.com/view/2182/pbx-hacking-moves-into-the-professional-domain-as-arrests-stack-up-/

Lemos, R. (2009, March 4). *War dialing gets an upgrade.* Retrieved August 1, 2009 from http://www.securityfocus.com/brief/918

Franklin, C. (2000, September 20). *How cable modems work.* Retrieved August 1, 2009 from http://computer.howstuffworks.com/cable-modem.htm

Franklin, C. (2000, August 7). *How DSL works.* Retrieved August 1, 2009 from http://computer.howstuffworks.com/dsl.htm

(2000, May 3). *How does a T1 line work?* Retrieved August 1, 2009 from http://computer.howstuffworks.com/question372.htm

Tyson, J. (2001, Feburary 2). *How network address translation works.* Retrieved August 15, 2009 from http://computer.howstuffworks.com/nat.htm

Shinder, D. (2001, April 12). *Putting the "private" in virtual private networking.* Retrieved August 16, 2009 from http://articles.techrepublic.com.com/5100-10878_11-1057214.html

Brain, M., and Wilson, T. V. (30 April 2001). *How WiFi works.* Retrieved August 16, 2009 from http://computer.howstuffworks.com/wireless-network.htm

Kayne, R. (2003). *What is WHOIS?* Retrieved August 19, 2009 from http://www.wisegeek.com/what-is-whois.htm

dlaverty, (2009, Feburary 20). *WPA vs WEP: How your choice affects your wireless network security.* Retrieved August 19, 2009 from http://www.openxtra.co.uk/articles/wpa-vs-wep

dlaverty, (2009, Feburary 20). *WPA vs WPA2 (802.11i): How your choice affects your wireless network security.* Retrieved August 19, 2009 from http://www.openxtra.co.uk/articles/wpa-vs-80211i

Skoll, D. F. (2009, April 5). *Outbound mail filtering — the other half of the problem*. Retrieved September 16, 2009 from http://www.theglobeandmail.com/news/technology/article816375.ece

Cobb, M. (2009, February 5). *What are common (and uncommon) unified threat management features?* Retrieved September 16, 2009 from http://searchmidmarketsecurity.techtarget.com/tip/0,289483,sid198_gci1347014,00.html

Conry-Murray, A. (2005, March 1). *Overview: Cisco NAC vs. Microsoft NAP*. Retrieved September 17, 2009 from http://www.informationweek.com/news/showArticle.jhtml?articleID=159902085

Messmer, E. (2009, September 21). *Sticker shock over data-loss prevention products could be short-lived*. Retrieved October 15, 2009 from http://www.computerworld.com/s/article/9138309/Sticker_shock_over_data_loss_prevention_products_could_be_short_lived?taxonomyId=82

Ouellet, E., & Proctor, P. E. (2009). Magic Quadrant for Content-Aware Data Loss Prevention. *Gartner RAS Core Research Note g00168012*. Retrieved November 4, 2009 from http://www.websense.com/site/docs/whitepapers/en/Gartner_Websense3107.pdf

Howard, A. B. (2009, October 15). *Data loss prevention technology matures but is still no cure-all*. Retrieved November 4, 2009 from http://searchcompliance.techtarget.com/tip/0,289483,sid195_gci1371455,00.html

Chee, B., & Franklin Jr., C. (2009, May 27). *Review: malware-fighting firewalls miss the mark*. Retrieved November 7, 2009 from http://www.computerworld.com/s/article/print/9133533/Review_Malware_fighting_firewalls_miss_the_mark?taxonomyName=Security&taxonomyId=17

Perry, C. (2007, April 13). NAC technologies join forces. *Processor Editorial Article*, Retrieved November 7, 2009 from http://www.processor.com/editorial/article.asp?article=articles/P2915/22p15/22p15.asp

Jabbusch, J. (2009, September 18). Catching the unicorn: a technical exploration of why nac is failing. *Whitepaper.* Retrieved November 7, 2009 from http://securityuncorked.com/docs/CatchingtheUnicorn_NAC_FirstRelease.pdf

Herzog, P. (2009). OSSTMM 3 Lite. *ISECOM - Institute for Security and Open Methodologies*. Retrieved November 8, 2009 from http://www.isecom.org/mirror/OSSTMM_3.0_LITE.pdf

Shinder, D. (2006, November 13). *Tips for bringing e-mail, web site hosting in-house*. Retrieved November 8, 2009 from http://articles.techrepublic.com.com/5100-10878_11-6134430.html

Shinder, T. (2008). *The best Damn firewall book period* [Second Edition]. Retrieved November 8, 2009 from http://books.google.com/books?id=mZEds6I2J_AC&lpg=PA795&ots=T7_Hbrd37N&dq=ICMP%20firewall%20rules%20IPSec%20PPTP&pg=PA795#v=onepage&q=ICMP%20firewall%20rules%20IPSec%20PPTP&f=false

Tyson, J. (n.d.). *How OSI Works*. Retrieved November 9, 2009 from http://computer.howstuffworks.com/osi.htm

Tools Appearing in this Paper

Nmap	http://nmap.org/
Nessus	http://www.nessus.org/nessus/
OpenVAS	http://www.openvas.org/
Kismet	http://www.kismetwireless.net/
Aircrack-ng	http://www.aircrack-ng.org/
Wireshark	http://www.wireshark.org/
Tcpdump	http://www.tcpdump.org/
Metasploit	http://www.metasploit.com/
QualysGuard	http://www.qualys.com/products/qg_suite/
McAfee Foundstone	http://www.foundstone.com/
eEye Retina	http://www.eeye.com/html/Products/Retina/index.html
ISS Internet Scanner	http://www.iss.net/
Core Impact	http://www.coresecurity.com/content/core-impact-overview
Immunity Canvas	http://www.immunitysec.com/products-canvas.shtml
Open Source Security Testing Methodology Manual (OSSTMM)	http://www.isecom.org/osstmm/
Microsoft Baseline Security Analyzer (MBSA)	http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=f32921af-9dbe-4dce-889e-ecf997eb18e9