Global Information Assurance Certification Paper

Securing Enterprise Internal Network (A Case Study)

Jia Cherng Lee

December 12, 2003

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b

Option #2

Abstract

While working for a multinational Original Equipment Manufacturer as a network administrator, the internal network degraded during a worm attack, management wanted the network to be assessed. The network team had been assigned to conduct a risk assessment of our company's internal network security. We started prioritizing the risks by classifying them as at high, medium and low. The team then recommended a few solutions to address these risks. After publishing the risk assessment report, the team identified a few areas to be fixed as soon as possible. First, the Wide Area Network (WAN) and Local Area Network (LAN) were not fully secured. Second, there was no separation of network services by function. Third, we audited the office environment and found Rogue Wireless Access Points connecting to the office network. Fourth, we found development labs network having many vulnerable workstations and servers.

To start, we decided to secure our WAN and deploy IPSec VPN technology on top of a frame-relay PVC network with Quality of Service (QoS)[5]. Second, we consolidated multiple server farms from many buildings into 2 data centers and separated them from the office network. Third, we secured all the Rogue Wireless Access Points by segmenting them out from the enterprise network and installing virtual private network (VPN) gateway to guard against malicious access attempts to the enterprise network. Lastly, we segmented out the development labs network from the enterprise network. By implementing recommended solutions, we were able to improve the security of my company's network from future network attacks; specifically Distributed Denial of Service (DDoS) attacks.

Before

The enterprise had a good defense-in-depth strategy with the required perimeter in place for the ISP connection and DMZ network. All clients needed to connect to proxy servers before accessing the Internet. The proxy servers located within the DMZ were protected by the inner and outer firewalls, which added an additional layer of security.

Figure 1 below was a simplified version of the private WAN design. It is a hub-to-spoke frame relay network. Please note, all the redundancy connections and devices are excluded from this simplified version.

[5] Reference Document. "Configuring Per Site QoS for IPSec VPN using GRE Tunnel" August 13, 2003, http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns109/networking_solutions_white_paper09186a0080189153.shtml

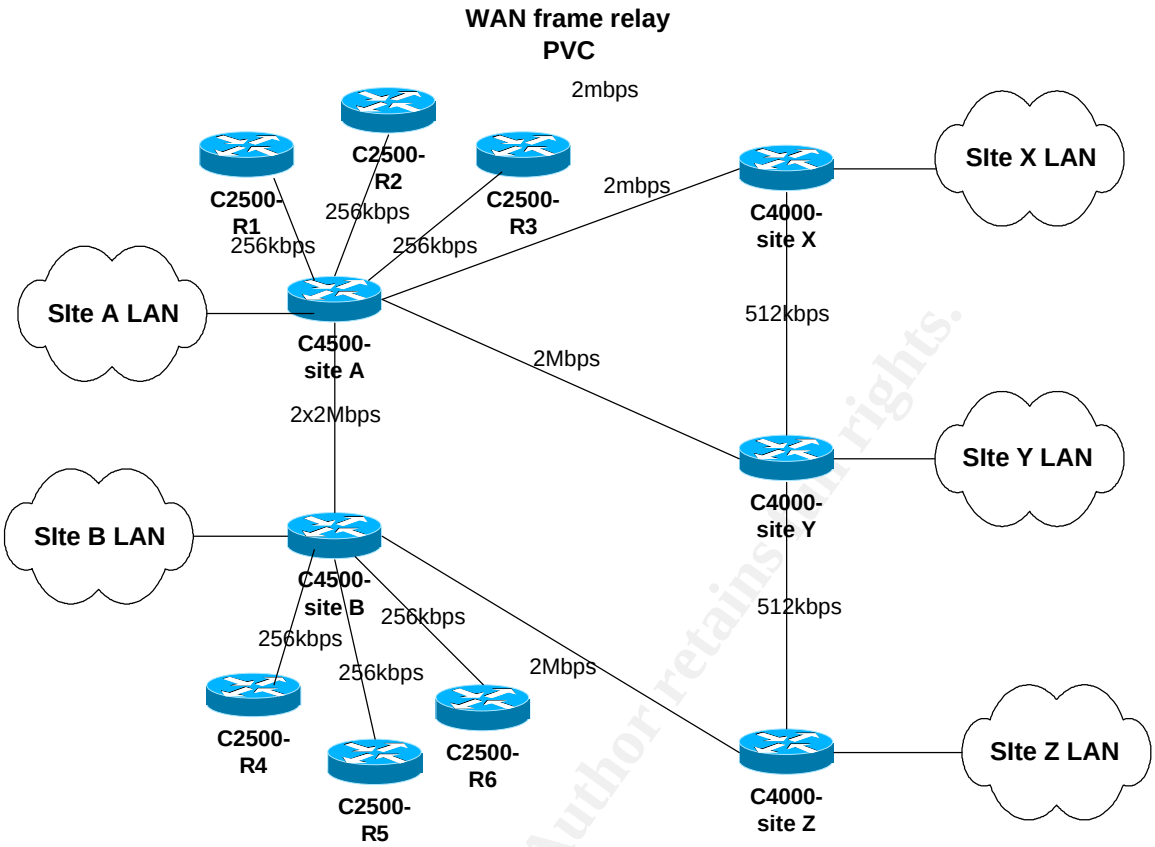

Figure 1: Simplified Private WAN drawing

No encryption for enterprise private Wide Area Network (WAN)

The company did not encrypt the data transverse across the public WAN frame relay connections. This poised a potential threat that someone could listen to our company's confidential information. Though frame-relay does provide network security using traffic separation for data transport security[1], however, it could not protect against eavesdropping, and a malicious person could still intentionally tamper with the information transferred across the public frame-relay network[4]. To ensure information confidentiality and integrity, we needed to improve the WAN security. Looking for better network security tools became a high priority.

[1] Reference Document. "From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task" September 5, 2003 http://www.cisco.com/en/US/netsol/ns341/ns121/ns193/networking_solutions_audience_business_benefit09186a00801ba90f.html

[4] Reference Document. "Data Privacy Solution – Introduction" http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns54/networking_solutions_package.html

WAN Congestion during Nimda[15] Worm Attack

When the Nimda worm attack was seen in the network, the infected clients and servers continuously sent out a lot of packets to scan for the vulnerable systems. Once there were multiple infected systems, it created a Distribution Denial of Service (DDoS) attack, which caused the WAN links to be congested. The disproportionate traffic would cause the routers to run out of resources and drop packets because the links between peering routers could not handle immerse volume of packets. Unfortunately, the important data and critical information to business operations became impacted as well. Critical applications vital to an Enterprise Organization, such as Enterprise Resource Planning (ERP) transactions for finance, accounting, and shipping were all affected when excessive traffic hit the network.

No Access Control List Applied To WAN Routers

Since there was no access control list (ACL) at the border WAN routers, all the clients could send and receive traffic from any clients and servers from any part of the enterprise network. Moreover, there was no access control list (ACL) to filter out the traffic destine to invalid destinations. Therefore, DDoS traffic poised a serious threat to the enterprise network allowing WAN to be flooded during the Nimda worm attack.

Limited Server Farm Protection

The routers could not route the packets properly when the CPU utilization hit 99% during worm attacks. These attacks were coming primary from within the company. They were infected PCs and servers throughout the company. Unfortunately the office network and server farms shared the same routers. Because of the lack of segmentation, the critical server farms were impacted when the routers could not process or route packets quickly taking down the entire network. Lack of network separation was a major issue at the distribution layer, causing all corporate network traffic to fail. During the attack, the worm caused a loss of communication between all client and servers over the LAN and WAN. Sales personal could not update orders and the corporate warehouses could not ship product. Essentially, all the electronic transactions came to a halt. Upper management decided to kick off a business continuity process, which was needed to keep the business running by providing a manual work around for the organization.

Furthermore, physical security for some of the server farms needed to be addressed, as there was lack of good security policy. The IT department did not enforce device owners to register their products before placing them on the network. Therefore, patches and server hardening did not occur as standard operating procedures. Moreover, almost anyone could have compromised the company's data because of lack of security policy and standardization. This was

[15] Reference Document. "CERT® Advisory CA-2001-26 Nimda Worm" September 18, 2001, http://www.cert.org/advisories/CA-2001-26.html

due to poor management of the network. Some of the more obvious threats were: server rooms were not secure; there were no fire-rated-walls, there were no emergency exit door, CCTV was not available, a UPS system and a power generator were not installed.

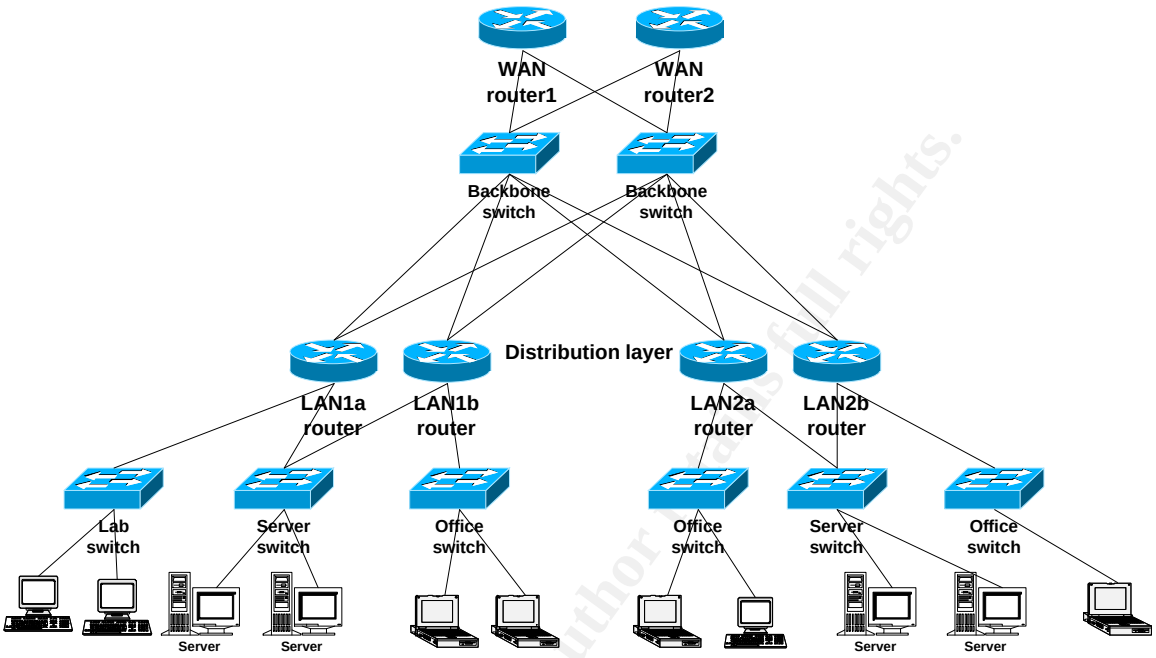

Figure 2: Local Area Network drawing

No Intrusion Detection System Installed

Without network base and host base intrusion detection systems installed, it had become a major problem when there was an intrusion or worm outbreak within the internal network. When a DDoS attack started, it was not immediately detected in the most critical early hours. By the time the network team realized there was a problem, services became degraded. The network administrators depended on the Sniffer traces to analyze network traffic as well as identify the characteristics of an attack. I quickly realized that distributed Sniffer could not be used remotely because the network had been badly degraded during DDoS attack. Therefore, I used the portable Sniffers to capture the traces and reacted accordingly. For instance, I used access control list (ACL) to filter out the DDoS traffic and log the infected systems that hit the access list. Lacking centralize logging mechanism to combat the attack caused a tremendous strain on the network administrators. There was not a method, to identify the source of infected machines. Having a Syslog server for logging events and hits captured by the WAN and LAN routers, would have allowed the network team to catch the infection much quicker with much less resources.

No Intrusion Prevention System

Critical servers did not have an Intrusion Prevention Systems or protection software installed, and any new exploit could potentially infected these servers through a software vulnerability. Missing this important piece of protection

software caused major disruption of service to the enterprise when a worm or malicious code brought down critical enterprise applications.

Rogue Wireless Access Points

Wireless Local Area Network (WLAN) can be set up easily by users to expand their office network. Users purchased these wireless access points and asked vendors to install the access points and connected them directly to the office network outlets. However, this was becoming a major threat for the company's information because no security was put in place. Users did not even turn Wired Equivalent Privacy (WEP) on because they were not aware of the security weakness of a wireless LAN. Walls only reduced the wireless access points' signal strength in most buildings, which allowed people to find and access the corporate network using a simple program like Netstumbler[8]. This was especially true for our remote small offices located in multi-storey buildings with more than one company. Intruders could have hijacked the communication session and gained access to our enterprise network easily by standing outside of an office with a notebook or hand held device processing a wireless access card. To address this issue management published a new security policy prohibiting any rogue wireless access points from connecting to the network. However, ignorant users tend to violate the security policy and make the network vulnerable to hackers[6]. Therefore, having a security policy, educating users and enforcing the security policy is vital to ensure corporate information remains safe from captured stray signals.

Development Labs - Poised A Risk

Normally, lab owners did not have an information security policy for development labs. Lab owners set up servers, workstations and network infrastructure according to their own requirements. These labs located within different buildings at each sites where use by software developers. However, the labs' servers and workstations set-up as workgroup did not comply with the IT security policy. For example, these servers and clients did not follow the strong password policy; the systems were not in a centralized IT asset inventory database. Most of the time, labs systems did not have the latest software patches installed.

Occasionally when the software developers performed testing their newly developed codes they would unintentionally cause a denial of service attack to the network. This would bring down a portion of the corporate enterprise network. This justified a need to segment the network.

[8] Percoco, Nicholas J. "Wireless Security: Detecting Wireless Networks from the Wire" http://www.ambiron.com/downloads/wireless.pdf

[6] Bogue, Robert L. "Stumble across rogue wireless access points" November 26, 2002, http://insight.zdnet.co.uk/hardware/servers/0,39020445,2126559,00.htm

During

After management reviewed the risk assessment reports and began to understand the impact and the risks associated with our business operations, project teams were formed to address and mitigate all high and medium risk vulnerabilities.

End-of-Life Old WAN Routers

Cisco routers 4000/4500 and 2500 routers had been end-of-sale and may have no longer been supported by Cisco[2]. The old hardware and IOS could not support the new services we intended to implement on the network. To upgrade the network, management approved the funding for replacing all the Cisco 4000/4500 and 2500, to Cisco 7200VXR and Cisco 1751. With the new and more powerful routers, we redesigned the WAN with Quality of Service (QoS) on secured frame-relay PVC. After replacing the small office routers from Cisco 2500 to Cisco 1751 routers, I created IPSec GRE tunnels to connect the small offices.

Deployed GRE Tunnels with IPSec Encryption

From network security standpoint, Frame Relay relies on traffic separation for data transport security. Someone could still potentially access our information illegally as Frame Relay data is sent in clear text mode.

> When information must be protected from eavesdropping, the ability to provide authenticated, confidential communication on demand is crucial. Sometimes, data separation using tunneling technologies, such as generic routing encapsulation (GRE) or Layer 2 Tunneling Protocol (L2TP) provides effective data privacy. Often, however, additional privacy requirements call for the use of digital encryption technology and protocols such as IPSec. This added protection is especially important when implementing VPNs. [4]

IP VPN uses of strong encryption standards in IPSec, such as Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES)[1], this type of encryption will make it very difficult for someone to access and view information passing through the public network. The network team requested to encrypt the traffic carried over the public frame-relay cloud. Although the cost of

---

[2] Reference Document. "Cisco Routers." http://www.cisco.com/en/US/products/hw/routers/index.html

[4] Reference Document. "Data Privacy Solution – Introduction" http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns54/networking_solutions_package.html

[1] Reference Document. "From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task" September 5, 2003, http://www.cisco.com/en/US/netsol/ns341/ns121/ns193/networking_solutions_audience_business_benefit09186a00801ba90f.html

frame-relay services is higher than Internet VPN services, it added a layer of defense while providing better services. Therefore, the team decided to continue using public frame-relay services for business critical traffic between the larger corporate locations. To further improve the security on the WAN frame-relay connections, we used Cisco IPSec VPN encryption technology to secure the WAN. Although there is overhead when using IPSec VPN on top of a frame-relay PVC, this decision was made after careful evaluations and studies.

"Generic routing encapsulation (GRE) is best suited for site-to-site VPNs because it supports routing updates, multiprotocol, and multicast traffic." [7] And it is a good tunneling technology, in terms of configuration and management. Finally, our effort and investment paid off as we secured all the major sites frame-relay PVC connections with GRE Tunnels protected with IPSec. This feature provided the security of encryption protection against eavesdropping on our confidential communication and kept the corporate data confidential.

The network team did some more research on service providers offering VPN services, especially on availability, network security, quality of service and manageability[1]. After getting information from a few companies that used VPN services for their WAN, we received good feedback on this type of service. The input helped our group made the decisions that it would be safe to use this technology. I was assigned by the team to migrate our remote small office connections to VPN over the Internet. The company now had an inexpensive secure solution to transfer data between the core sites and it's remote offices.

I started by increasing the ISP connection from 2Mbps at the hubs sites to 4Mbps. Then, I set up the VPN routers within the DMZ at the hub sites and installed the ISP connection at the remote small offices. Every small offices network had 2 GRE tunnels with IPSec set up for redundancy purposes. I tested the connection for 1 month before terminating the existing frame relay PVC to the remote offices. The team was expecting it would have a ROI (Return of Investment) from the initial investment for the small offices by 9 months[3].

---

[7] Reference Document. "Network Design Consideration" http://www.cisco.com/en/US/products/hw/vpndevc/ps333/products_configuration_guide_chapter09186a008007dcea.html - 1023171

[1] Reference Document. "From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task" September 5, 2003, http://www.cisco.com/en/US/netsol/ns341/ns121/ns193/networking_solutions_audience_business_benefit09186a00801ba90f.html

[3] Reference Document. "VPN Solution Overview: The Advantages of Migrating from Frame Relay to VPN" July 8, 2003, http://www.cisco.com/en/US/netsol/ns110/ns5/ns6/networking_solutions_audience_business_benefit09186a008019cd5c.html

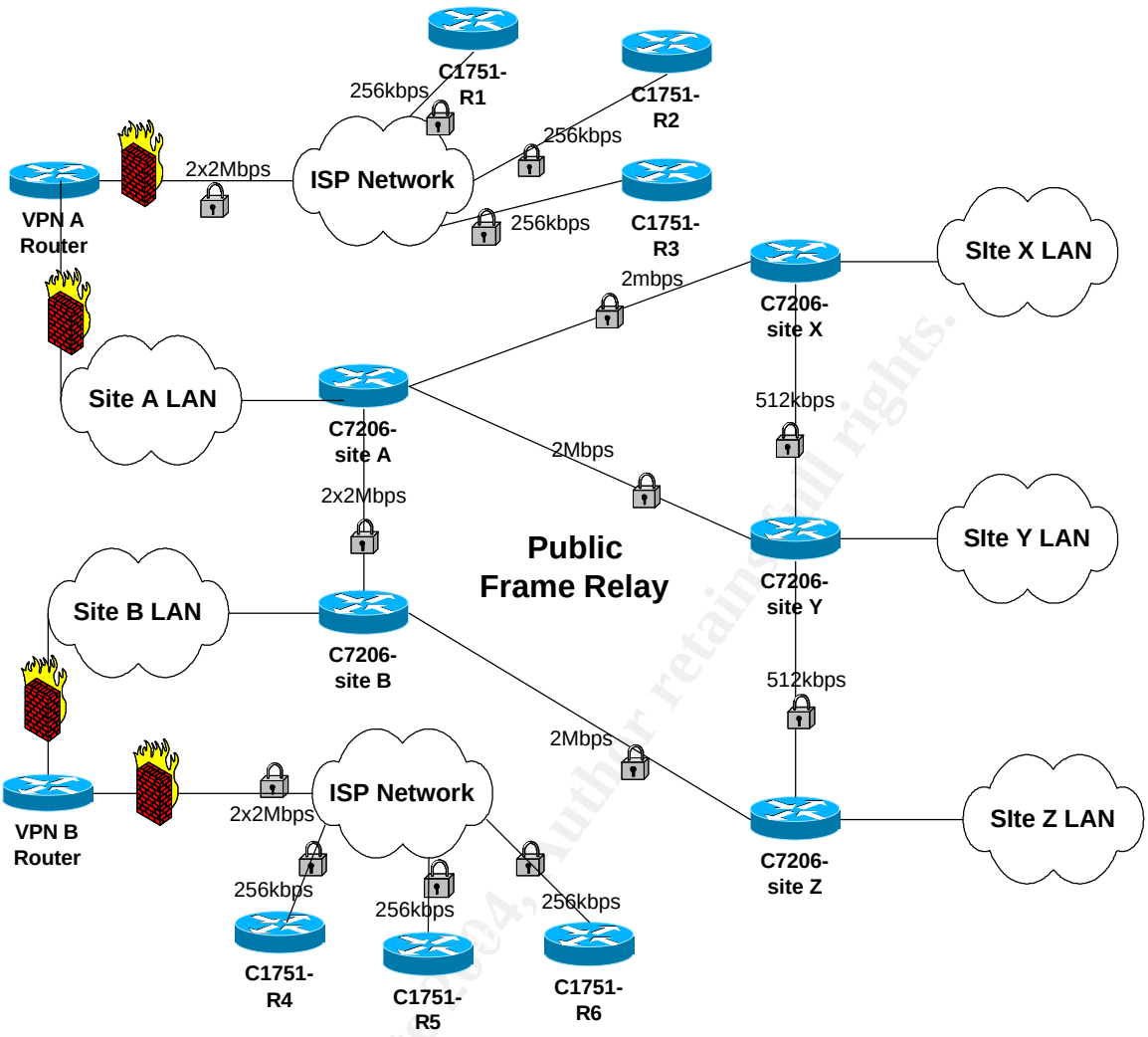

Figure 3: Simplified Secured Private WAN drawing

Enable Quality of Service (QoS) at the WAN

By default, the router did not prioritize the traffic; it routed the packets base on first-in first-out (FIFO) basis. Therefore, we needed Quality of Service (QoS) where encrypted traffic is carried over tunnels between Hub routers and spoke routers[5]. This technique can provide a buffer zone if there is a DDoS attack which floods the WAN. Implementing QoS can also give more priority to the business critical traffic over non-critical applications send across the WAN.

From there, the business critical server-client communication can have a minimum allocation of bandwidth available when the WAN is congested. After performing some analysis on network traffic patterns, we were able to determine

[5] Reference Document. "Configuring Per Site QoS for IPSec VPN using GRE Tunnel" August 13, 2003, http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns109/networking_solutions_white_paper09186a0080189153.shtml

the minimum bandwidth required for all critical business transactions. We then arranged for the data to be sent in clear text format without Graphic Users Interface to maximize the data output in an emergency situation.

Access Control List and Syslog Servers

We configured Access Control List (ACL) on all WAN border routers to drop all packets not destine for the internal network. This can reduce a lot of worm traffic because all the traffic destines to external networks is being dropped, which will reduce the flooding packets on the WAN. Moreover, these dropped packets hit an Access Control List (ACL) and are logged at the WAN border routers.

The group deployed a Syslog server to capture all the events logged by the WAN routers, including weird packets or strange network packets hitting the access control lists. This logging mechanism is good to keep the history of the network health and enable network administrator to look for the details of intrusion events during a DDoS attack. The log is an important source of information to locate the source and target hosts on the corporate network. Further actions can be taken to prevent the network from further deterioration. For instance, I will disconnect the infected systems from the network and inform the system owner to clean and patch them before connecting them back to the network.

Redesigned the Network to Protect the Data Center

Management decided to consolidate all server farms located in multiple buildings into two physically secured data centers located at separate sites. This design would improve the physical security and provide protection against internal and external threats that could cause a major impact to the company's operations. There are four key design criteria for the data centers; these criteria are availability, scalability, security and management.

Separation of the Data Center network with the office network was important. We built two separate network backbones and segmented the network by functionality. In order to do this, we installed two new layer 3 switching devices with routing capabilities at each Hub site. The Data Center network would have redundant layer 3 switches for routing and switching. Segmentation of the networks helps prevent a DDoS attack from the office network to the data center. Access Control Lists are applied at the Data Center routers' interfaces for both ingress and egress filtering to prevent DDoS attack[13]. Malicious and suspicious packets will be filtered. Only legitimate traffic will be allowed to pass through the filter.

[13] Tanase, Matthew. "Closing the Floodgates: DDoS Mitigation Techniques" January 7, 2003, http://www.securityfocus.com/infocus/1655

Intrusion Detection System (IDS)

We deployed Cisco Network IDSs at the data center network to detect any attack on the enterprise network services. Cisco recommends customers to deploy Network IDS at aggregation switch, and configure the network IDS sensors to monitor synchronous traffic flows; this will reduce the amount of false positives and false negative alerts[10]. To protect the enterprise servers operating system and applications, we installed Host IDS agent software on the servers to detect and prevent any worm and intruders to access to the server illegally either from internal or external devices. Worms always open an uncommon port for spreading. The Host IDS are able to detect the malicious code. Additionally, HIDS monitor the file integrity using strong checksum mechanism such as MD5[9]. Any alerts triggered will be sent to master console servers via the network. The network security team would then monitor these alerts that are captured by master console servers. The team analysis of these alerts work to help provide early detection of a new worm or malicious code. This process becomes an important task in order to contain and prevent DDoS attacks.

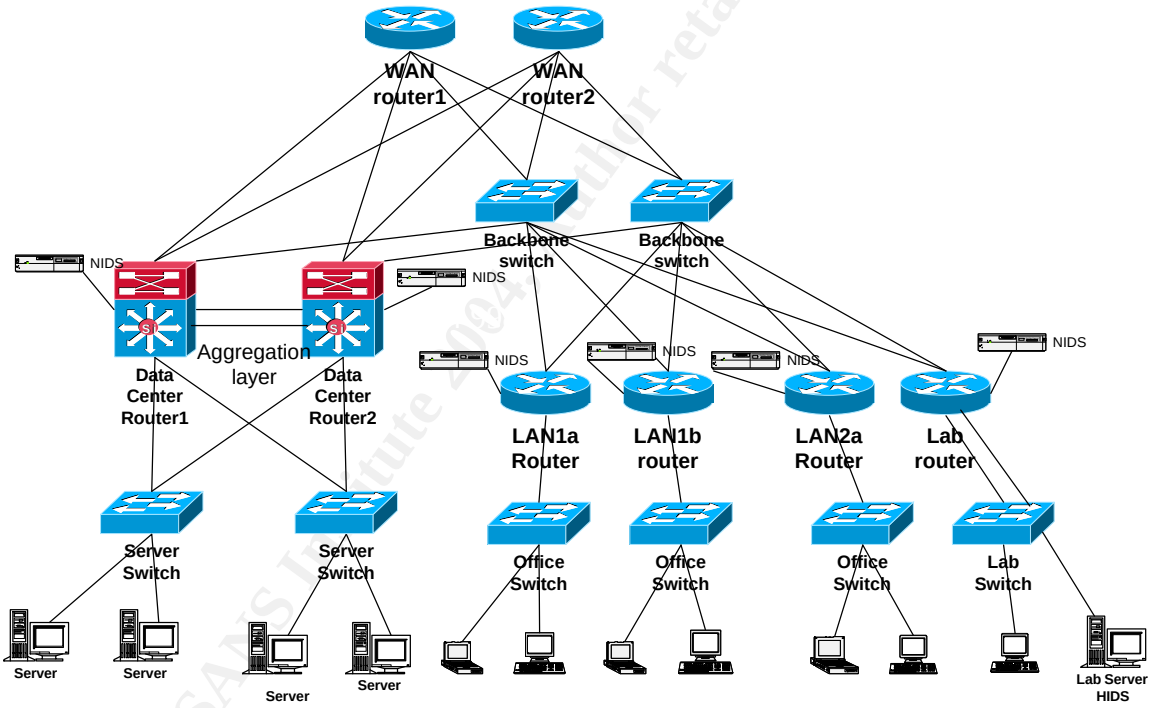

Figure 4: New Local Area Network Design

[10] Reference Document. "Data Center Networking: Securing Servers Farm" http://www.cisco.com/application/pdf/en/us/guest/netsol/ns304/c649/ccmigration_09186a008014edf3.pdf Page 36. Chapter 2-10.

[9] Bussiere, Dick. "Worms – Their Spread and Mitigation" Nov 3, 2003, http://www.ncasia.com/ViewArt.cfm?Magid=3&Artid=21975&Catid=4&subcat=50

Intrusion Prevention System (IPS)

Intrusion Prevention System is a combination of IDS and application firewall, the IPS checks on the API calls, memory management for example buffer overflow, rather than packets at the network layer[14]. Our enterprise systems engineers took the ownership of deploying IPS systems to protect the critical enterprise applications from malicious attacks such as viruses, worms, Trojans or even bad coding. They put a lot of effort to define and customize the policy as well as profile the applications. These measures were important to ensure the IPS works properly.

Network Scanning for Vulnerable and Compromised Devices

A new security policy was implemented to scan the network periodically. Routine network scanning for vulnerable systems lands under the supervision of network security team. This can prevent vulnerable systems in the network from being compromised by the hackers or malicious code. After identifying the vulnerable systems, the system owner would be informed. A tracking database would then be updated with the information found. The system owner then was responsible to fix the identified problem within 3 days. If the identified vulnerable systems remained connected to the network after 3 days, the system would be disconnected.

To Secure the Wireless Network

To protect the enterprise network security from the rogue wireless access points, we worked out a plan to install secure wireless networks for all the remote small offices, campus offices, factory networks, logistic warehouses, and conference rooms. By doing this, we were able to implement 802.11b wireless network to service users while extending the office network without putting our network at risk. I was assigned by the team to deploy the secured wireless network for my home site. I enabled Wired Equivalent Privacy (WEP) for security purpose, changed all the default setting. Moreover, I reduced and tested the signal strength of access points to minimize the chances of intruders of hacking into our wireless network. Furthermore, I changed the Access Point setting to stop sending out the Service Set Identifier (SSID) to the clients[8]. However, WEP is known to be weak in security and cannot protect the network from intruders. Thus, we treated wireless network users same as remote access users, and I deployed the same type of VPN gateway for wireless LAN users. All the remote access users already had VPN client software installed on their notebook. Therefore, minimal effort was needed to secure the wireless network by creating VPN wireless profile for our users. Both remote access and WLAN customers used the RSA SecurID SoftwareToken for login authentication. The RSA ACE servers would then only allow legitimate users to access the enterprise network.

---

[14] Desai, Neil. “Intrusion Prevention Systems: the Next Step in the Evolution of IDS” Feb 27, 2003, http://www.securityfocus.com/infocus/1670

[8] Percoco, Nicholas J. “Wireless Security: Detecting Wireless Networks from the Wire” http://www.ambiron.com/downloads/wireless.pdf

Moreover, we can check the servers' log for any illegal login attempts; this is important to safe guard the enterprise network.

Secure the Development Labs

Meeting end users to understand the different lab requirements was the first step of lab isolation project. From there we defined the requirement of the development labs. The prime objective was to provide a minimum level of connectivity for the labs to the enterprise network. To do this, we consolidated all the labs into a single router with multiple access switches. We applied access lists to block most of the packets, only opened a few TCP ports for the office network. We blocked all the UDP ports and multicasting traffic flow into enterprise network. On the same note, labs servers' were relocated to the same router, Host Intrusion Detection System (HIDS) software was installed on all the labs servers. The HIDS agents will then send the alert to the master console when suspicious or malicious activity is seen on the labs network.

After

The investment for the network security paid off; there were many benefits in having network stability. The remaining challenges were the continuous enhancements on security tools, infrastructure, which were required to face the threat of new cyber attacks and malicious codes.

Secured Private Wide Area Network

After securing the WAN, we ensured our confidential data transverses the Public Frame Relay network without being viewed and modified by intruders. Furthermore, the implementation of Quality of Service limited malicious traffic carried over the WAN when there is a new worm spreading across the network. Moreover, any malicious packets hitting the WAN border routers would be filtered out. The Syslog servers would then capture these hits. By making monitoring scripts to continuously process and parse the log at the Syslog servers, we could receive certain events or hits above a predetermined threshold. Whenever there is a new worm, modification of the script would be needed because new malicious codes will capitalize on new software bugs and the use of different UDP or TCP ports.

Data Center and Local Area Network security

A benefit of having data centers is to allow IT to control the environment and infrastructure, twenty fours hours a day and seven days a week. Additionally, enterprise standard security policies can be implemented and easily controlled in a data center environment. Furthermore, consolidation of multiple server farms located at different buildings located at separate secured data centers, provided redundancy and flexibility to do maintenance and recovery whenever needed.

Furthermore, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) provided surveillance, intrusion prevention and protection to the

enterprise server within the data center. As alerts triggered, Master console servers capture all the logs sent by the IDS and IPS. The Network security team can monitor the alerts all the time using the console clients.

Network security team continues to update the latest IDS signatures into IDS whenever there is a new signature provided by the vendor. These signatures are important to ensure any IDS can detect a new exploit. On the other hand, a lot of works still needed to be done to fine tune the Intrusion Detection Systems for false positive alerts. A challenging but necessary task is to filter out 70-80% of the alerts that are considered noise. These are harmless alerts that can be overwhelming to sift through, while looking for attackers' malicious codes.

A Secured Wireless Network

After IT deployed the secured wireless network services in the office locations and published the Wireless Network security policy, users came forward and turned in their rogue wireless access points illegally installed. We continue to look for wireless security tools to improve the security of wireless network. The team is currently in progress to evaluate whether we should install IDS at the edge of the wireless network; this would detect hackers might come in from the WLAN. Additionally, we are evaluating new generation of encryption technology for wireless network.

For prevention and detection, we worked out a schedule to scan for rogue wireless access points. The network team evaluated Nmap Stealth Scanner for detecting rogue wireless access points at the wired network[8]. Scanning rogue wireless access points is a critical task. All newly identified rogue access points need to be found and removed from the network immediately.

Mitigated Risk from Development Labs

After the R&D labs segmented out from enterprise network, and most vulnerable systems were disconnected from the enterprise network. Access Control Lists were deployed to filter majority of the traffic generated by labs. Then, we worked out a Security Policy for the labs. This ensured information security is taken care by the labs users seriously. IT worked with Lab owners on the security policy, which enhanced the Labs' information security. Finally, an Inventory Management System was developed to track all systems in the environment. This allowed IT to control and manage patches as well as other updates.

Users' Awareness and Security Policy

Upon being hired with the company, a new employee would read and sign the Information Security Policy. The company security policy needs to be updated regularly to keep up with the latest threats. Continuous education is needed to keep the employees updated about the latest amendment of the security policy.

[8] Percoco, Nicholas J. "Wireless Security: Detecting Wireless Networks from the Wire" http://www.ambiron.com/downloads/wireless.pdf

This is too big of a challenge for the information security officers to handle themselves. To make sure employees do not put the enterprise network at risk, management required regularly scheduled classes for employees on updated Security Policies. For instance, a training segment would cover strong password authentication, users' responsibilities on patching their systems when new patches are needed, and do not download application from Internet. Users' awareness and information security training for users are now playing important roles to secure our enterprise network.

Automated Patching Tools

Patching servers and clients in the network is taxing our IT human resources whenever there is a new patch release. Sometimes IT needs to work with software vendors while testing and certifying the patches on different platforms before deploying to the rest of the corporate. The risk of bringing down the enterprise systems due to new patches is always there; thus new patches should always be tested to ensure the patch does not actually break the system. However, the malicious code writers capitalized on the software bug notifications by releasing new worms and viruses within days of notification. Today, one of the major challenges for our server and client engineering teams are to test the patches quickly enough in order to get them installed. Given that there are a few days to months before an exploit comes out, companies have to be ready in case the malicious code is developed within days. Therefore, organizations look for third party vendor tools to speed up the process. If the team can use an automated tool to certify patches and patch 95% of the systems within a week, then, worm and virus will not be able to take down a robust network infrastructure.

Anti-Virus

Update Anti-Virus latest signatures files to corporate servers and clients are crucial to prevent the systems from getting infected by worms and viruses. Normally, users will be informed by mail and web postings requesting them to update their signatures file immediately. However, the management requested an automated process. The server engineering team developed scripts to update the servers' Anti-Virus signatures files. Sub-sequentially, server administrators will then scan all the servers to ensure all patches were updated successfully.

Impact

The security fixes put in place defended our network services effectively and against the recent worm DDOS attack. While the Nachi[11] and Lovsan[12] worms

[11] Reference Document. Network Associates Technology, Inc "W32/Nachi.worm" August 18, 2003, http://vil.nai.com/vil/content/v_100559.htm

[12] Reference Document. Network Associates Technology, Inc "W32/Lovsan.worm.a" August 11, 2003, http://vil.nai.com/vil/content/v_100547.htm

crippled some businesses, our preventative measures stopped them from spreading on our enterprise network. Alerts that were sent out by the IDS to our master console servers and logs that were recorded by Syslog server enabling the network security administrator to react in the early hours during the infection. The access control list that were added at the WAN border routers and data center routers prevented the distributed denial of service attacks caused by Lovsan and Nachi worms. Moreover, we did not see DDoS traffic from the developments labs because they were isolated from the enterprise network.

Since the security upgrades, we have done well in intrusion detection during recent worm attacks. However, manual disconnection for infected clients remained a challenging task for network administrators and client support personnel. Now, we are working on automating a script to auto disconnect the infected clients from the network. However, a lot of legacy network equipment does not support remote management for port disconnection, which is impeding us from deploying the script. Some further investments are needed to upgrade the network equipment and enhance the protection of our environment. A good example, remote access engineering team is evaluating a low cost personal firewall for remote access and VPN users; this is preventing vulnerable remote access and VPN clients from being infected from Internet and spreading the worm into the enterprise network.

Conclusion

To secure the enterprise internal network is an extremely challenging task, and involves every employee to play his or her roles diligently. The return on investment of a secured network environment is essential for the company's survival. An organization's survival cannot be measured by daily operation cost. Our management continues to provide regular security training to educate employees. These classes help to improve overall enterprise information technology security and reduce risks to minimum.

References:

1. Reference Document. “From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task” September 5, 2003, http://www.cisco.com/en/US/netsol/ns341/ns121/ns193/networking_solutions_audience_business_benefit09186a00801ba90f.html

2. Reference Document. “Cisco Routers.” http://www.cisco.com/en/US/products/hw/routers/index.html

3. Reference Document. “VPN Solution Overview: The Advantages of Migrating from Frame Relay to VPN” July 8, 2003, http://www.cisco.com/en/US/netsol/ns110/ns5/ns6/networking_solutions_audience_business_benefit09186a008019cd5c.html

4. Reference Document. “Data Privacy Solution – Introduction” http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns54/networking_solutions_package.html

5. Reference Document. “Configuring Per Site QoS for IPSec VPN using GRE Tunnel” August 13, 2003, http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns109/networking_solutions_white_paper09186a0080189153.shtml

6. Bogue, Robert L. “Stumble across rogue wireless access points” November 26, 2002, http://insight.zdnet.co.uk/hardware/servers/0,39020445,2126559,00.htm

7. Reference Document. “Network Design Consideration” http://www.cisco.com/en/US/products/hw/vpndevc/ps333/products_configuration_guide_chapter09186a008007dcea.html - 1023171

8. Percoco, Nicholas J. “Wireless Security: Detecting Wireless Networks from the Wire” http://www.ambiron.com/downloads/wireless.pdf

9. Bussiere, Dick. “Worms – Their Spread and Mitigation” Nov 3, 2003, http://www.ncasia.com/ViewArt.cfm?Magid=3&Artid=21975&Catid=4&subcat=50

10. Reference Document. “Data Center Networking: Securing Servers Farm” http://www.cisco.com/application/pdf/en/us/guest/netsol/ns304/c649/ccmigration_09186a008014edf3.pdf Page 36. Chapter 2-10.

11. Reference Document. Network Associates Technology, Inc “W32/Nachi.worm” August 11, 2003, http://vil.nai.com/vil/content/v_100559.htm

12. Reference Document. Network Associates Technology, Inc "W32/Lovsan.worm.a" August 11, 2003, http://vil.nai.com/vil/content/v_100547.htm

13. Tanase, Matthew. "Closing the Floodgates: DDoS Mitigation Techniques" January 7, 2003, http://www.securityfocus.com/infocus/1655

14. Desai, Neil. "Intrusion Prevention Systems: the Next Step in the Evolution of IDS" Feb 27, 2003, http://www.securityfocus.com/infocus/1670

15. Reference Document. "CERT® Advisory CA-2001-26 Nimda Worm" September 18, 2001, http://www.cert.org/advisories/CA-2001-26.html

Last Updated: May 23rd, 2017

Upcoming Training

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