Building and securing a corporate DMZ in preparation for a Data Center Migration

By Kevin Keay
Master of Science in Information Security
Lewis University

May 2008

Abstract

The migration of a data center provides a rare opportunity to completely rethink security and disaster recovery strategies, to rebuild network infrastructure, to devise more efficient work procedures and to upgrade aging equipment. The Information Technology staff faced with this challenge needs to take advantage of the opportunity to compare their system against best practice examples. This thesis is a case study of a data center migration with a special focus on increasing the security protection afforded to the core "De-Militarized Zone" (DMZ) where the corporation's most secure data is kept.

Table of Contents

Introduction

This thesis project describes the migration of a data center, with special attention paid to the protected core of the system known as the DeMilitarized Zone (DMZ) and the secure data it protects. This paper will give insight to the work that was needed to plan and migrate a corporate DMZ network. This paper will give the reader a perspective on the amount of work it took to build an entire data center infrastructure and to move the old to the new.

Company Overview

Company-X is an American multinational corporation with 2007 net sales in excess of $11 billion. Company-X's corporate IT headquarters is located in Location-A. This data center houses 95% of all corporate servers and applications and is the main Internet link for incoming/outgoing data. Location-A is also the central hub for all remote wide area network circuits supporting many locations, including plants, warehouses, and shipping/distribution centers.

In 2007, the decision was made to move the data center from Location-A to Location-B, about 10 miles to the south. The decision to move the data center was based on several factors. The top three being (1) the data center was close to maximum capacity (2) the data center was not able to expand quickly if an acquisition occurred and (3) the Location-A data center was at risk to total catastrophic loss in that it was located directly underneath the landing path for O'Hare airport. It was decided that it was best to move to a new data center rather than attempt any upgrade of the existing Location-A data center.

This project was by no means an easy task. The data center consists of over 150 Unix and NT servers, several large databases, backup networks, storage area networks (SANs), infrastructure hardware, security hardware and miles of network cable. This project would take the coordination of numerous people and several departments company wide. Not only would there be a heavy requirement on the part of the employees but this new data center would be a significant investment by the company. The new data center would require all new network hardware, servers, racks, cabling (copper and fiber), HVAC, fire controls, monitoring systems, Internet Service Provider (ISP) demarcation and an operations center.

DMZ

A Demilitarized Zone or Demarcation Zone (DMZ) in military terms, is an area, usually the frontier or boundary between two or more military powers (or alliances), where military activity is not permitted, usually by peace treaty, armistice or other bilateral or multilateral agreement [1]. This idea applies to corporate networks as well. In general terms, a DMZ is a network that serves as a buffer between the vulnerable protected internal network and the Internet. A DMZ is just an isolated network that is usually protected by a firewall and allows access to servers only over specific ports or services.

Unfortunately, it's neither safe nor smart to just put a server on the Internet and hope nobody does anything bad to that server. Odds are that server will be compromised in a very short time. Any company that will allow access to their servers from the Internet will have to protect those servers on a DMZ. A DMZ will only allow access to the server that the administrator deems necessary.

It is a common fallacy that a carelessly designed DMZ is sufficient to protect servers. The DMZ firewall only restricts access to the server on specific port numbers or services. If a hacker can get past the firewall, all the security is reliant upon server security such as patches, updates, host firewalls, etc. So if firewalls are used and properly maintained, the DMZ will allow an external hacker access only to the DMZ equipment rather than the entire internal network.

DMZ History

The term DMZ originated from the Korean War back in the 1950's [8] and was incorporated into the computer world during the mid 1980's when the Internet was a fairly new technology. The DMZ is synonymous with firewalls, since the firewall is the appliance that really creates and defines a DMZ. There have been three generations of firewalls or packet filters.

First Generation: In 1988, the first paper on firewall technology was published by engineers from Digital Equipment Corp (DEC). These engineers developed the first packet filter which was a fairly basic system but would evolve into much more sophisticated systems. In these early days, the packet filters basically had no intelligence but only allowed packets to pass if they met a set of basic criteria. There was no concern given to whether the packet was part of an existing connection (stateful), which is why these first firewalls were stateless firewalls [2].

Second Generation: This generation covered 1980 to 1990 which were also known as circuit level firewalls. This generation firewall had more intelligence than did the first generation. What set the second generation apart from the first generation is that the second generation firewall did more than just inspect the packet on an individual basis within the context of their connection, they also track the key connection transitions that are expected to take place during a session involving trusted database packets. This technology is referred to as stateful firewall and has the intelligence to update and maintain a state table that has a record of all connections traversing the firewall. The state table allows the firewall to determine whether the connection is part of an existing connection or the start of a new one. This technology helps to thwart off denial-of-service (DOS) attacks [2].

Third Generation: This third generation firewall is known as application layer firewall, it is also known as proxy-based firewalls. This new generation was released by DEC and was given the name DEC SEAL. The first sale of DECs SEAL was on June 13th 1991to an East coast chemical company. The benefit of using an application layer firewall is that it understands certain application layer protocols such as File Transfer Protocol (FTP), Domain Naming Service (DNS) and Hypertext Transfer Protocol (HTTP). This allows the firewall to see an unwanted protocol trying to be sneaked through a non-standard port or whether a protocol is being abused. This ability gave the firewall more intelligence than previous generations thereby making the DMZ more secure [2].

Subsequent developments: In 1992, Bob Braden and Annette DeSchon at USC were further refining the firewall concept and developed a product known as "visas". These visas were key to incorporating visual icons into the firewall support model and could be integrated into Microsoft Windows or Apple MAC. In 1994, an Israeli company called Checkpoint built this visual technology into its Firewall-1 software [3].

Why are DMZs effective? DMZ's are effective because they work with the basic fundamentals of Transmission Control Protocol/Internet Protocol (TCP/IP) communications but they maintain their effectiveness only if qualified security professionals keep the environment updated and current. The DMZ is really a fundamental idea that improved over time because the technology for keeping the DMZ safe improved. This technology will always keep improving as the attackers on the Internet will continue to find ways to bypass or manipulate current security trends.

A greater majority of modern day companies have some kind of Internet presence whether it is online sales, a website or both. The Internet is a great tool for companies to use to get their products to the masses that would otherwise not be available to them locally. Websites are also a great tool to use for many purposes such as product support, documentation and to give public or privileged access to online content.

Unfortunately with the good comes the bad. There are many people connected to the Internet who are just looking for a vulnerable web server or system to compromise. These people go by many different names such as hackers, script kiddies, etc. These attackers have different goals in mind but the bottom line is that they want to disrupt service, alter content or steal information.

Any Internet facing server is susceptible to an attacker and is considered a target. Luckily, there are ways to protect these servers and prevent attacker penetration.

Location-A DMZ Architecture

The network in Location-A is considered a three tiered architecture. The three tiers consist of the external or Internet facing network (Tier-1), Tier-2 is the protected middle layer also known as the DMZ and the final Tier is the internal network (Tier-3). (Figure 1) The three layer design is a best practice approach to building a DMZ. This design gives the administrator more flexibility to apply filters at different tiers and it supports a defense-in-depth strategy [9].

Legend:

RT01/RT02 – Router #1 / Router #2

FW1/FW2 – Firewall #1 / Firewall #2

VPN – Virtual Private Network

IDS – Intrusion Detection System

LB – Load Balancer

FW Mngt – Firewall Management Server

FW - Firewall

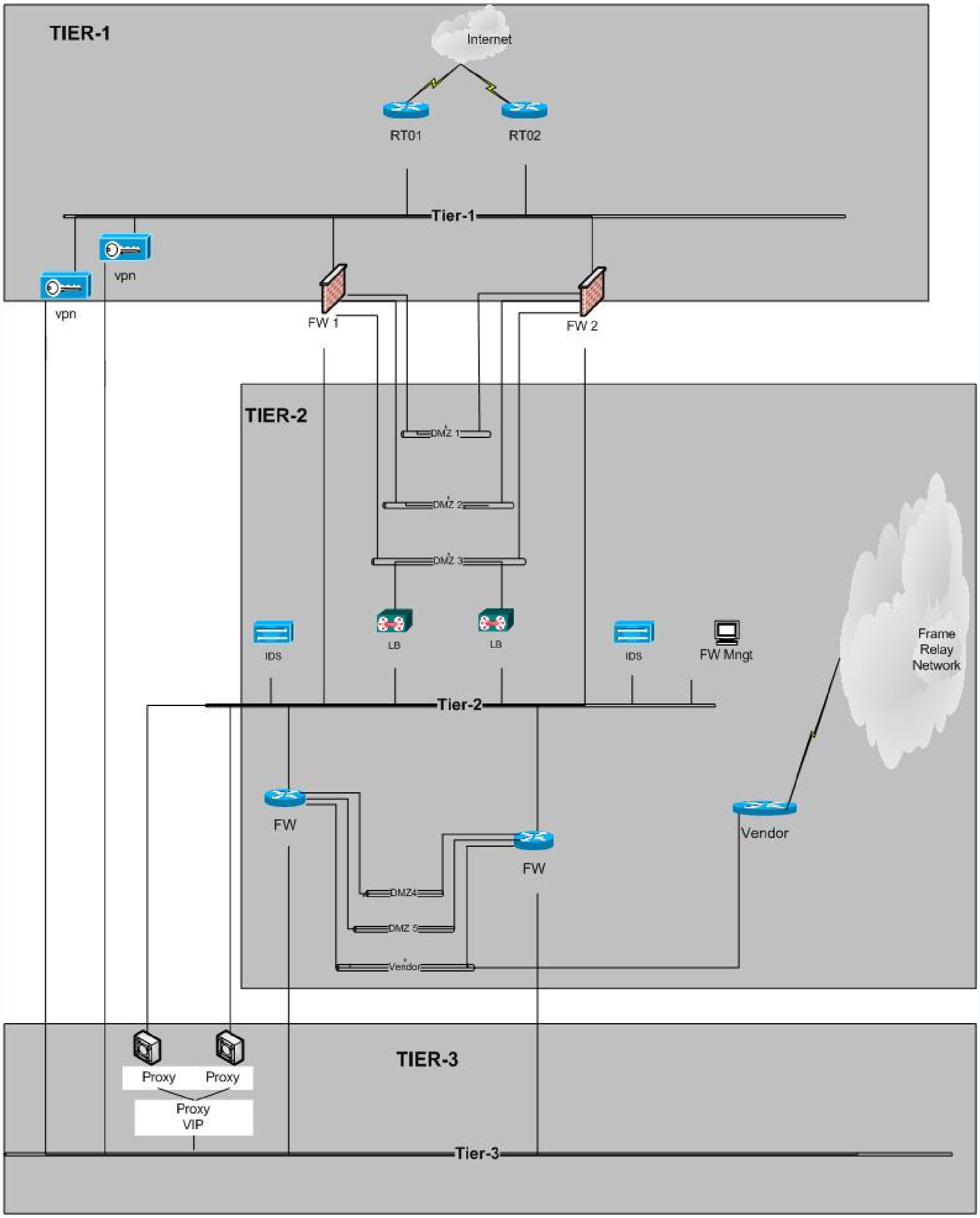

Figure 1. The DMZ architecture at Location-A

Tier-1

The Tier-1 network is the external facing network and this is where all the public facing applications are accessed. The external network basically consists of two Internet facing routers, firewalls and the VPN appliances. The Internet routers run in failover mode using Cisco's Hot Standby Router Protocol (HSRP) failover protocol. The two routers route data over three DS-3 circuits that have a capacity of 45Mbps per circuit. These circuits support many applications including web based traffic, Electronic Data Interchange (EDI), FTP, Instant Messaging (IM) and encrypted VPN traffic.   A Class C network from our ISP which allows us to support 254 public IP addresses. Most of these Internet Protocol (IP) addresses are used to publicly Network Address Translation (NAT) our protected servers in the DMZ Tier-2 protected networks (Figure 1).

Behind the Internet routers are a pair of firewalls that act as the entrance point to the DMZ and accessible Tier-2 applications. All traffic entering and leaving the Tier networks must pass thru the firewalls. The firewalls not only allow, block or drop traffic based on IP address but also based on specific port numbers. This allows for a more granular security policy that will protect vulnerable servers on the DMZ.

Parallel to the firewalls are a pair of VPN appliances. The VPN appliances are used to terminate encrypted secure tunnels from employees, vendors and third party companies. There are two types of encrypted tunnels that we support, client based tunnels and Lan-to-Lan tunnels. Client based tunnels are tunnels initiated from remote users that are typical on a laptop using a VPN client application. These tunnels are usually only temporary and are built and tore down as needed. The other type is the Lan-to-Lan tunnel that is established with another entity and is a permanent tunnel usually terminated on another VPN appliance or firewall.

Tier-2

This part of the network consists of five DMZ networks that exist to isolate and protect all company resources that are accessible from the Internet. Whereas access to the internal Tier-3 network from the Internet is usually forbidden, access to the DMZ is allowed and in most cases promoted. Companies will put services on the DMZ that they want anyone to be able to access, such as a web site or some services will be available but only to certain people. This restriction is in place to allow access to more sensitive data by a smaller group of people. Whatever the service or data that needs to be protected or accessed, the best place to put them is in a well protected DMZ. (Figure 1)

The Location-A DMZ hosts many servers that run a variety of services such as HTTP, Hypertext Transfer Protocol with SSL (HTTPS), Email, FTP and EDI just to name a few. There are a total of five DMZ networks and three of those exist on the outer pair of firewalls and the other two reside on the internal firewalls. The DMZ's are divided into two sets because the more sensitive data/services are housed in the well protected internal firewalls. The other less sensitive services, such as HTTP, are located on the outer set of firewalls (Figure 1).

On DMZ 2, there are pair of load balancers that distribute incoming traffic across multiple servers for a variety of services. These are Cisco Content Switches and they run in redundant (failover) mode, so that if one fails, the other will become active and primary and will also pick up any existing connections. This feature allows a failure with no interruption of service to the client (Figure 1).

Tier-3

This Tier encompasses all internal networks that reside behind the set of internal firewalls. No services exist on the internal networks that are accessible from the Internet. There are internal databases that are accessed by Tier-2 servers but that is the extent of traffic penetrating the internal network. The traffic that does penetrate to the internal network is restricted by source/destination IP address and port number. (Figure 1)

All outbound client traffic is proxied and traverses through a proxy device. Any traffic not proxied and is Internet bound must be explicitly allowed and approved by the network administrator. This constraint insures that data being passed out of this Tier is not secure data, or if it is that the transfer is both authorized and logged. (Figure 1)

Equipment

Below is a list of equipment that is used in the Location-A datacenter.

Tier-1 equipment
- Cisco 7200 XVR Routers (Internet routers)
- Nokia IP 500 series firewalls (external set of firewalls)
- Checkpoint NG FP3 runs on the Nokia appliances
- Cisco VPN Concentrator 3030 (VPN appliances)

Tier-2 equipment
- Cisco 11150 Content Switches (load balancers)
- Cisco PIX 525 firewall (internal set of firewalls)
- Cisco IDS appliances
- Cisco 2811 router (vendor router)

Tier-3 equipment
- Bluecoat 4000 proxy appliance

Vulnerabilities

There are several weaknesses in this architecture that will be addresses with the migration to the new data center. The following is list of these weaknesses including an explanation as to why these issues pose a threat or a risk to the network.

1. VPN Concentrator is connected directly to the Tier-3 network.
   This type of architecture is definitely not a desired type of connection. This is connecting a Tier-1 device to the Tier-3 network. With this type of connection, all security provided by the firewalls is bypassed, putting the vulnerable internal network at risk. The worse case scenario would be to have an attacker compromise one of the VPN Concentrators from the Internet. If this happened, then the attacker would have unrestricted access to any node on the internal Tier-3 network. This is not desirable; it poses a very real threat; and is considered a high risk.

   Desired Change: Create a new DMZ that would be dedicated to the VPN equipment and allow better protection to the interior Tier-3 network.

2. Checkpoint/Nokia firewalls are running older version of software.
   Both external firewalls are running on older versions of Checkpoint Firewall-1 software and Nokia IPSO software. There are many documented vulnerabilities with both versions of the software. Checkpoint NG FP3 vulnerabilities include Denial-of-service against syslog daemon and remote code execution, just to name a couple. The Nokia IPSO version that is used has known vulnerabilities that include denial-of-service; remote security and script injection but there are others. Patches and updates can be installed on these systems to mitigate or remove the vulnerabilities but Company-X is conservative about changing operational software while it is in use and unless the vulnerability is ranked as a major risk, patches or updates are not immediately applied.

   Desired Change: When building the new firewalls for the new DMZ, ensure that the software installed is a recent release that addresses past vulnerabilities. Develop a process and internal Service Level Agreement (SLA) defining parameters for patching that meets management's requirements [7].

3. The companies old mindset was, "If it's not broken then don't fix it."
   There was no formal patch management process in place for Tier-1 or Tier-2 hardware, which is not a good practice. This hardware is close to the Internet making it among the most vulnerable. The old mindset was that production was king and since patching or updating could possibly cause an outage, it wasn't looked at as a high priority.

   Desired Change: Develop, maintain and enforce a strict patch management process for all security hardware and appliances [7].

   This was the mindset of the old management structure and with the new management structure in place, it appears that a formal patch management process will be in place and strictly enforced. Security of all company assets is paramount and any vulnerability needs to be communicated to management immediately, followed-up with a change control request being issued via the change management process.

4. The Location-A VPN environment has all VPN's concentrated on a single pair of appliances. These tunnels include employee client tunnel, vendor client tunnel, company remote site tunnel and vendor remote site tunnel. From a security perspective, this is a relatively safe approach but can be improved upon. Most documentation on the Internet suggests that vendor and company tunnels should be separated and isolated from each other

   Desired Change: Separate Company owned VPN tunnels from vendor VPN tunnels and ensure that both are separated by a different DMZ, Virtual Local Area Network (VLAN) or networks. This will ensure that there is no risk of a vendor compromising company assets.

Location-B DMZ

Building this new network and data center in Location-B was truly a great opportunity. Not too many people get the chance in their careers to participate in a huge effort like this. Migration of a data center takes excellent project management skills and the combined effort of many talented employees. This also provided me the opportunity to build a DMZ from the ground up using current equipment and software. This would give me the chance to reduce our risks by strengthening our weaknesses and develop processes that would maintain that level of security.

The Location-B DMZ architecture will be similar to the Location-A DMZ. This was done intentionally because the three tiered network is a very secure design that we wanted incorporated into the new location. It would also make it much easier to migrate the DMZ servers. Since the migration was going to be complicated and complex, it was decided not to further complicate things by introducing an entirely new DMZ design with little to gain by doing so (Figure 2).

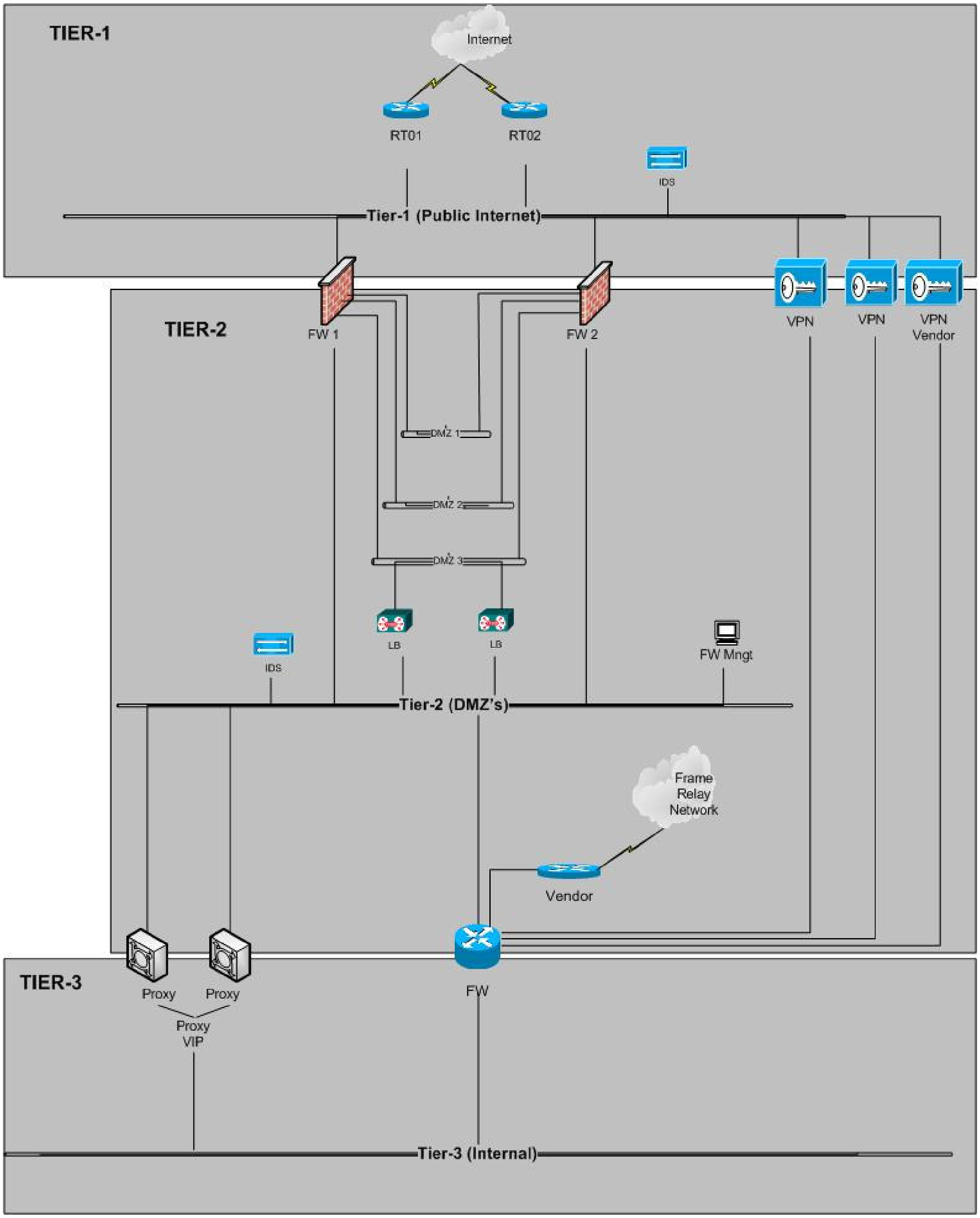

Figure 2. Location-B DMZ architecture

Overview

As you can see this new network design is very similar to the old one. As previously mentioned, this was done intentionally for two reasons: it is a secure design and it would help with the migration. There are a few changes that stand out in this new design. The most apparent change is with the way the VPN appliances are connected to the network. If you recall, the previous diagram had the VPN appliances connected directly to Tier-3, which was a security risk. The new network changed where that connection terminates and the VPN appliances now terminate into a secured DMZ specifically for company user's VPN tunnels. This creates a Tier-1 to Tier-2 connection and further filters access on the DMZ. This one change alone greatly reduced the risk that was associated with this vulnerability and this is the preferred way to connect a VPN appliance (Figure 2).

Another major architectural change is the isolation of the vendor VPN tunnels. In the past, these tunnels were terminated on the same hardware as Company-X tunnels. This created an undesirable situation where company traffic and vendor access coexist and could possibly lead to contamination of data. The goal was to completely separate vendor VPN tunnels from all Company-X tunnels, which was accomplished in this new design. Not only are the tunnels kept isolated but all traffic is further filtered by the VPN router.

One other minor change to mention is that an IDS appliance was put on the external Tier-1 network. This allows visibility to all traffic entering Company-X's network and gives a good view of traffic before being filtered by the firewalls. This gives administrators the ability to compare and analyze traffic on each side of the networks which will assist in troubleshooting and identifying potential attacks.

Aside from the physical improvements, software has also been upgraded on all hardware. Upgrading the software was needed as some of the older software was over four years old with limited patching performed over that time. Some of the new software came with the new hardware but there was some minor patching needed to bring the patch level up to current standards. So just from a software perspective, this new DMZ is much more secure just by upgrading the software and reducing many outstanding vulnerabilities residing in the older versions of software.

With all the many improvements resulting from this migration, one of the most beneficial was the opportunity to review each firewall rule and access list to ensure that each one is still applicable and pertinent. One of the hardest duties of an administrator is to keep track of temporary access and ensure that access gets disabled or deleted upon expiration date. This migration allowed me to review each and every access entry and carry over only the ones that are needed, while deleting any unused rules.

Together, all of these changes resulted in a vast improvement in network security and allowed us to reduce our risk. This gave us the confidence to put corporate services out on the new DMZ and be assured that we took the appropriate measures to secure the vulnerable hardware.

Build-Out

Building the new DMZ required a lot of work and time. I thought it may be helpful to list the high-level steps I used to build each piece or pair of hardware. These will not be detailed steps but rather a general overview of major steps.

Internet routers (Cisco 7200 XR) – These routers connect Company-X to the Internet, they are the first line of defense. Even though these routers will perform only very high level filtering, they are very critical to business and need to be protected. If these are ever compromised or hacked, then everything is at risk. Below are the steps I used to harden my Cisco router for Internet use [4].

Cisco Routers

1. Chose my make/model of router
2. Select the appropriate IOS (software) to use on the router
3. Configure IP and routing requirements on router
4. Select a secure access method (preferably Secure Shell (SSH)
5. Configure the enable password (enable secret) feature
6. Disable any unneeded services (chargen, daytime, echo) most new versions of IOS have these services disabled but it's always good to double check.
7. Set a management sessions time-out so idle sessions are terminated
8. Set up Simple Network Management Protocol (SNMP) notifications to monitor CPU, memory, access, etc. SNMP should be configured very carefully by experienced people.
9. Create an initial access list to restrict access and Internet Control Messaging Protocol (ICMP) to routers and other nodes
10. Restrict console/aux port access and or services if needed
11. Restrict VTY/TTY port access and or services if needed
12. Implement a warning banner for access sessions. This is not really a deterrent to hacking the router but rather a legal requirement. There have been many cases in the past that hackers could not be prosecuted because no warning banner was in place.
13. Configure logging if needed. I always configure logging so that I know who accesses the router and when. I also want to be able to view any past events that may be of interest. Centralized logging is the best long term solution. This will allow archiving of daily logs so that operational changes can be easily found with search software and attack patterns can be analyzed.
14. Configure NTP (network time protocol) or SNTP (simple network time protocol). Having accurate time is important for logging, coordinating events and tracking incidents for further analysis.
15. Disable IP Source Routing, ICMP Redirects and IP Broadcasts.

16. Configure anti-spoofing.

These are the steps I used to configure my routers and deemed appropriate for my environment. There are many more security settings which may be appropriate based on individual needs. My settings will not necessarily secure other environments so please prepare your security strategy in accordance with your company's policies.

Checkpoint Firewalls

The firewalls are the "keys to the kingdom", so special care must be taken when configuring these pieces of hardware. I will not attempt to suggest any configuration settings but really give an overview of the steps I used to prepare the firewalls for the configuration [5].

1. Acquire firewall hardware. In this case it was a pair of Nokia IP710s.
2. Establish the Management server.
3. Rack mount all hardware.
4. Download desired Nokia IPSO version and upload it to the Nokia appliances.
5. Download and install any updates/patches to the selected IPSO version.
6. Download desired Checkpoint version and upload it to Nokia appliances.
7. Download and install any updates/patches for the Checkpoint version.
8. Configure global systems parameters.
9. Configure the interfaces and any services that will be used on appliance.
10. Configure routing and/or preferred routing protocol.
11. Configure redundancy protocol (VRRP) if desired or needed.
12. Create initial policy taking extra precaution to safeguard firewalls and management server.
13. Push policy decisions.
14. Test the new system both piecemeal and as it integrates.

This is a very high level install checklist and there are many more sub-tasks that are not listed here. Given the sensitive nature of this equipment and the role it plays in protecting company assets, only professional certified technicians should install and make systems settings.

Cisco PIX/ASA

As with the Checkpoint/Nokia appliances, the PIX's have many settings that can be tweaked based on company policy and needs and should only be configured by a qualified professional who understands the environment. Listed below are the high level steps used to setup the PIX [6].

1. Acquire PIX hardware. In this case it was a pair of Cisco 525s and ASA 5540s.
2. Rack mount the hardware.

3. Establish a console connection.
4. Download and install the latest acceptable IOS/software.
5. Configure network routing.
6. Identify each interface.
7. Let users start connections (enable NAT and test traffic flow).
8. Create a default route.
9. Permit ping access.
10. Save the current configuration and reload it.
11. After reload, check configuration and test network connectivity.
12. Add telnet/SSH access.
13. Configure inbound server access.
14. Configure outbound server access.
15. Add static routes.
16. Enable silo logging.
17. Add AAA authentication (if needed).
18. Recheck the final configuration.

Those listed are the main components of the DMZ. There is some other minor supporting hardware which I have not listed in these configuration steps.

Procedures Followed

Configuring this hardware was done according to manufacturer's recommendations and documentation. The preparation and configuration of each appliance was not done ad-hoc but rather was planned, reviewed and tested many times.

All of the equipment was prepared in a lab environment with a live Internet connection so testing would simulate the actual production environment. At no time during the testing of the equipment did the equipment come in contact with the production environment. This is a requirement of Company-X. Once the equipment was deemed safe and hardened, then the equipment was moved from the lab environment to production. Once in production, further testing was performed to ensure no environmental variables had changed that may cause issues.

Services in DMZ

The services in the new Location-B DMZ are basically identical to the old DMZ. As of this writing, no new services have been added.

List of Equipment

The equipment list for the new DMZ uses the same vendors as the old DMZ but using new models, IOS and software.

Tier-1 equipment
- (2) Cisco 7200 XVR Routers (Internet routers)
- (2) Nokia IP 710 series firewalls (external set of firewalls)
- Checkpoint R60 runs on the Nokia appliances
- (2) Cisco ASA 5540 (VPN appliances)

Tier-2 equipment
- (4) Cisco 11500 Content Switches (load balancers)
- (2) Cisco PIX 525 firewall (internal set of firewalls)
- Cisco IDS appliances
- Cisco 2811 router (vendor router)

Tier-3 equipment
- Bluecoat 8000 proxy appliance

Enhancements

There were several enhancements as a result of the migration. One of the obvious improvements was the upgrading of the hardware and the software. This alone was a huge benefit in that it really brought our environment up to par with the latest versions of software and patch level. At Location-A hardware was getting old and outdated and we were having some issues with available disk space.

Other improvements include eliminating all unused entries in filters, access lists and policies. This migration gave us a great opportunity to review all access entries and really find out what was being used, what was not being used and how it was being used. Anything that was no longer needed was not migrated. This gave us a good baseline to start keeping detailed documentation on all access rights.

Migration

DMZ Migration Strategy – the migration strategy took on a life of its own. There were many options we could've used and all of them were discussed, picked apart and really tested on paper.

The main objectives of this strategy were to migrate the DMZ services with minimal interruption to internal and external clients. We also wanted little or no changes required by our external customer and vendors. This was a crucial requirement in that we have hundreds of external clients. Had we had to contact each one and request them to make changes, it would be a huge task with unacceptable business impacts. Since a lot of our external clients were using static IP addresses to access our services and not DNS names, we had to take that into account when deciding on a migration plan.

The strategy that we selected was to migrate the servers/services over a 12 month period and to keep the existing public IP addresses. As part of the migration, every server and service was evaluated for the risk it possessed by moving it to a new location. The risk evaluation process for each server and service was extensive and very detailed, but from that process, we were able to identify four different risk levels of low, medium, high and critical. The risk level basically helped us determine the way in which the servers would be migrated. Migrating servers is no easy task with risk associated with each move. To make matters worse, it became apparent very quickly that each server move was going to be different and dynamic.

Based on each server's risk level, it was decided to use one of four different migration strategies which incorporated different methodologies. The four options to migrate the servers are "Lift & Shift", "Physical to Virtual" (PTV), "Rebuild", and "Cloning".

"Lift & Shift" is basically what it sounds like…the server is shut down, removed from the rack, packed and moved to the new location and powered on in the same state if was shutdown. Lift and shift was used for low to medium risk servers. These servers were deemed to be running on recent hardware that did not need to be upgraded and that the services running on it did not need much pre-testing.

"Physical to Virtual" transition or PTV was used for low to medium risk servers. This was used to move physical servers and consolidate them into one virtual server. This approach was used for the many servers that only had one or two applications running on them and had minimal CPU and memory requirements. These applications really have no need to be monopolizing an entire server given the amount of usage. Using the PTV method, we were able to do some "housekeeping" on the number of servers and dramatically reduce those numbers.

"Rebuilds" were done on servers that were running on older equipment and needed newer hardware but also needed a dedicated server to run the service or application. This method was used for high risk servers that ran independently of any live internal or external database. This type of migration was perfect for the high risk servers as it allowed us to rebuild the new server in the new environment, install the application and perform pre-migration testing in order to reduce or hopefully eliminate any migration day issues. Once the testing was completed and successful, the migration basically consisted on powering down the original server, migrate the IP information to the new server and reboot. This was a very successful approach and worked well for us.

"Cloning" was the last method. This was similar to a Rebuild but with Cloning, the data transfer was done the day of the migration. This was used primarily on servers that had live databases running on the servers that required an up-to-date transfer of data. This process basically shut down the services so no new data would be accepted during the cloning. Once the services were shutdown and all users logged off the system, transferring an exact replica of the server image to a new awaiting server at the new data center. This ensured the state that the data was in when services stopped was what was transferred over to the new server. Once cloning was completed, testing was performed; services started and final testing was started with the application.

DNS

DNS was not a huge issue with the migration but it had to be accounted for. Once issue we discovered immediately was that many of our external vendors were using static IP addresses configure in their application to access our services. This was the reason we decided not to change our public IP addresses during the migration. Our thought process was that if we ever had to migrate data centers in the future or change ISP's (resulting in a new public IP subnet) then ideally we would only want to have to make changes to our public DNS

The result of this finding was that we requested a zone file from our DNS provider. A zone file is really just a text file listing all DNS information for all and any domains active with that provider. Once we had the zone file, we could see which of our public IP addresses had a DNS entry assigned to them and which ones did not. If an IP address had no DNS entry, then a new DNS entry was required for that IP address. Our thought process here was that if we ever had to migrate data centers in the future or change ISP's (resulting in a new public IP subnet) then ideally we would only want to have to make changes to our public DNS and not burden our external clients to have to change numerous static IP entries.

Once the DNS entries were active for all IP addresses, we then notified our external clients that if they had configured a static IP address in their application to access our services, then they needed to make a one-time edit to that application and replace the IP address with the DNS name. Once this was completed, we felt confident that any future changes to our public IP addresses could be controlled by us by a simple DNS change. This is a more efficient way to handle these changes as our customers do not want to modify their applications every time we move to a new ISP.

Routing

Routing was a very important issue in this project. This topic alone resulted in many internal meetings and meetings with our ISP. We had two options on the table. The first option was to get a new public IP subnet from our ISP and change all of our public facing IP addresses as we migrated the server to the new location. The other option was to keep the existing public IP subnet and have our ISP route only those individual host IP addresses over to the new data center on a per migration wave basis.

We literally ran many simulated scenarios on paper to see how routing would change as we implemented changes with our ISP. We had to ensure that regardless of which option we chose that nothing would be adversely affected. There were many considerations to take into account. First and foremost, could our ISP support us if we decided to keep our existing public IP subnet? Would having the same public IP addresses at both locations affect internal systems? There were many more but as the discussions progressed, it was becoming obvious that we would keep our current public IP addresses and route only what was needed to Location-B.

Another routing issue that surfaced early was how to support the same VLANs (Virtual Local Area Network) at both locations? In order to make this a successful migration, we would need to support not only the new VLANs in Location-B but also the legacy VLANs in Location-A. This was required due to the fact that there were some systems on the network that the IP address could not change. We identified many dependent systems but there were still many older systems, some with no internal support, which could not be identified. So it was decided that we would support a mix of new and legacy VLANs and over time, we would slowly move all systems over to the newer VLANs and decommission the old ones.

This dual VLAN support between the sites was basic in nature. The gigabit links between the sites were only supporting Layer-2 traffic. Layer 2 traffic is based on the physical address of network nodes and not the Layer-3 IP addresses. Having these Layer-2 links allowed us to exchange VLAN information between the sites and we did not have to worry about complex routing schemes. This enable two systems on the same VLAN but at different locations appear to be virtually right next to each other.

At this point, the internal and external routing issues have been addressed and we were ready to start performing some pre-migration testing to confirm our theories would work.

Pre-migration Testing

Before we could even have thoughts of migrating anything to the new location, we had to test the access between the two sites and the Internet routing using the same subnet at each location. To do this required that we have an active Internet circuit and a router to accept the traffic. Both the circuit and router was ready and in place.

Testing the external routing not only focused on the test itself but we wanted to create a process that we would use for each migration wave. Having a process in place that both parties agreed to would reduce any confusion and give us step by step procedures to follow. Testing external routing was not a complicated process. I chose one of our public IP addresses that were not being used and allowed AT&T to put a static host route on their network that would route that IP address to the new Location-B location.

Although simple in theory, my main concern was that the technician who was putting in the static host route, may inadvertently start routing the entire subnet to Location-B as opposed to the one IP address. If that mistake was made all Internet communications to and from Company-X would come to a halt. So needless to say, this routing test was communicated thoroughly and coordinated with a dedicated technician that understood exactly what we were trying to accomplish. Testing was performed successfully with no incidents.

Internal routing was more involved in that it took more equipment and the configuration of this equipment was much more complex. I will not get into the details of the internal testing, but suffice to say that the VLAN support at both locations was a success and that we were able to implement it and maintain it throughout the duration of the migration.

Pre-migration testing was not performed only for the external and internal routing. Pre-migration testing really should be called pre-migration wave testing as this type of testing continued throughout the entire migration. Each individual migration wave contained several services which had to be tested. Testing was done using an isolated VLAN that allowed service owners to test identical production services without running any risk of duplicating services on the production network and causing severe issues. The access to this VLAN was restricted for both inbound and outbound traffic. Access was allowed on a case by case basis and once approved, was open only for a limited time. It was imperative that this testing environment be controlled and documented.

Migration Strategy

As mentioned earlier, migration of an entire data center is no easy task. The migration was looked at as a whole, and broken out into “waves” based on dependencies. In total, there were eight waves defined and each wave consisted of one or more “groups”. These eight waves would take about one year to successfully complete.

Groups consisted of a pre-defined set of services that would be moved on a given date. Preparing for a group move would require the coordination of all service owners, network engineers, project managers and management support. A group move would be planned and scrutinized months ahead of time and would continue until one week prior to the move. The meeting a week prior to any “group” migrating was basically asking each service owner whether they were ready to go or not…which we referred to as a “go, no-go”. I like to think this reminiscent to the Apollo mission control launch sequences where the flight director gets a status from each controller.

In the weeks and months prior to any Wave or Group being migrated, there was a very detailed check list of steps that needed to be completed by each individual group. This list took many staff-hours to complete but was vital to ensuring everything was accounted for and that each step had an owner. This list also identified dependencies that normally would not be noticeable but had surfaced as a result of getting all service owners together to create the check list.

Migrations usually started on Fridays, normally around 5pm, and could continue until Sunday around Noon because the system is under virtually no load during these times.

We placed checkpoints throughout each migration to evaluate how the migration was going and to identify any issues that we may be having. The results of each checkpoint would be communicated to upper management and posted on an internal portal for employees to view. Sunday at Noon was the set time that we would have to start backing out all necessary changes if we encounter issues with the migration. This would allow a 12-hour period to back out changes and still be ready for production on Monday morning. Fortunately we never needed to enforce this back out action.

On migration days, we would designate a single conference room we affectionately referred to as the "War Room", which acted as the central communication point for that weekend's migration. All participants and management were located in this War Room and on one large screen is the checklist showing the current status and on another screen is the overall status of the migration. The participating employees were treated well during each migration as the room was also filled with food, snacks and beverages since this was an around the clock operation.

Post migration testing occurred on a per service basis. As each service was brought on on-line, the service owners would start assessing the state of the server/service to ensure nothing was damaged in the transit to the new data center. After the health of the unit was confirmed, testing the application would start immediately. Testing time varied based on the application but regardless of the amount of time it took to test, the master checklist was always updated on the progress of each application/server pair. Once all testing was completed and positively confirmed, the item's status was changed to completed and the migration progress chart was updated to reflect that completion.

Summary

This cycle of weekend migrations continued throughout 2007 and into 2008. There were many lessons learned throughout this experience. I really considered myself lucky to have participated in such a complex project that required the teamwork of every IT staff. Most people can work in IT for many years and never have the opportunity, not only witness the building of a data center, but to participate. I've gained invaluable knowledge and experience by being allowed to architect and build the new DMZ networks. I'm always amazed at the amount of organization and project management skills that are needed for a project of this size.

It's truly inspiring to see an entire IT department come together and combine their skills and resources to accomplish such a monumental task such as this. As a result of this migration, Company-X now has updated all of it's documentation for every service/application that it owns. This will be valuable information for years to come

References

[1] Demilitarized Zone. Retrieved February 18, 2008 from Wikipedia website: http://en.wikipedia.org/wiki/Demilitarized_zone

[2] Firewall: Retrieved February 19, 2008 from Perpetuastudents website: http://perpetuastudents.wordpress.com/2007/12/05/firewall/

[3] Firewall: Retrieved February 19, 2008 from Wikipedia website: http://en.wikipedia.org/wiki/Firewall_(networking)

[4] Cisco Guide to Harden Cisco IOS Devices: Retrieved March 2, 2008 from Cisco's website. http://www.cisco.com/warp/public/707/21.html

[5] Check Point Press, (2007*). Check Point Security Administration NGX II 1.1*: Northbrook, IL: Forsythe

[6] Frahim, J., & Santos, O. (2006, August) *Cisco ASA: All-in-One Firewall, IPS and VPN Adaptive Security Appliance*: Indianapolis, IN: Cisco Press

[7] A Best Practice Approach to Implementing a Proactive Patch Management Strategy: Retrieved April 1, 2008 from CA website: http://ca.com/files/WhitePapers/patch_mgmt_wp.pdf

[8] DMZ: Retrieved February 18, 2008 from SearchSecurity website: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213891,00.html

[9] The Evolution of Network Security: from DMZ Designs to Devices: Retrieved April 10, 2008 from Juniper's website: http://www.juniper.net/solutions/literature/white_papers/200084.pdf