Global Information Assurance Certification Paper

Spencer Stewart
GIAC Security Essentials Certification (GSEC) Practical Assignment
Option 2 – Case Study in Information Security
Version 1.4 (amended April 8, 2002)
Defense In Depth Applied To The Small Business

Table of Contents

Abstract

In general, training materials appear to be written for corporate IT managers. While learning about technology from the enterprise level is educational and provides a broad perspective, network managers often find themselves interpreting established design concepts and security practices, in order to scale them down to fit their small business networks - and budgets. Understanding the concepts behind designing a secure network is critical when applying security practices to small business networks. Not every area of security can be met to the degree presented in ant-hacker and certification books. It's important to understand where changes and concessions can be made to security designs to allow for a practical level of security to be created in the small business environment. This paper proves Defense In Depth can be effectively applied to small businesses to protect against the growing threats to inter-network communication from the Internet.

The Unsecured Network: October 2001

Jones Company: Physical Network Equipment and Design

On October 2001, I was originally hired by Jones Company to perform a network documentation project. During my investigation for this project, I noted immediate security risks throughout the network. Other design flaws required a network upgrade or reconfiguration project to correct and these problems were noted. I spent the next nine months correcting problems and addressing a wide range of support issues that had been neglected for some time.

Storage limitations of the existing servers and noticeable network problems, such as servers crashing and slow network connections prompted a network upgrade that facilitated the implementation of new security standards throughout the company. A well-designed network and well-planned upgrade process was critical to creating the several layers of protection that is described in the practice of Defense In Depth.

The Jones Company network was a combination of old and new network hardware. As the company purchased new equipment, the former administrator added it to the hardware rack in the network closet. The old equipment was left in place and running, but performed no function. Figure 1 shows the Jones Company network as it was first documented. The NU FE-700 Switch and Bay Stack Access Node were powered on and connected, but where not used to provide network communications. Since all of the equipment was stored in an unlocked closet, this was a physical security risk. Someone could easily reconfigure this hardware and use it for malicious purposes without anyone noticing.

Jones Company Network Diagram

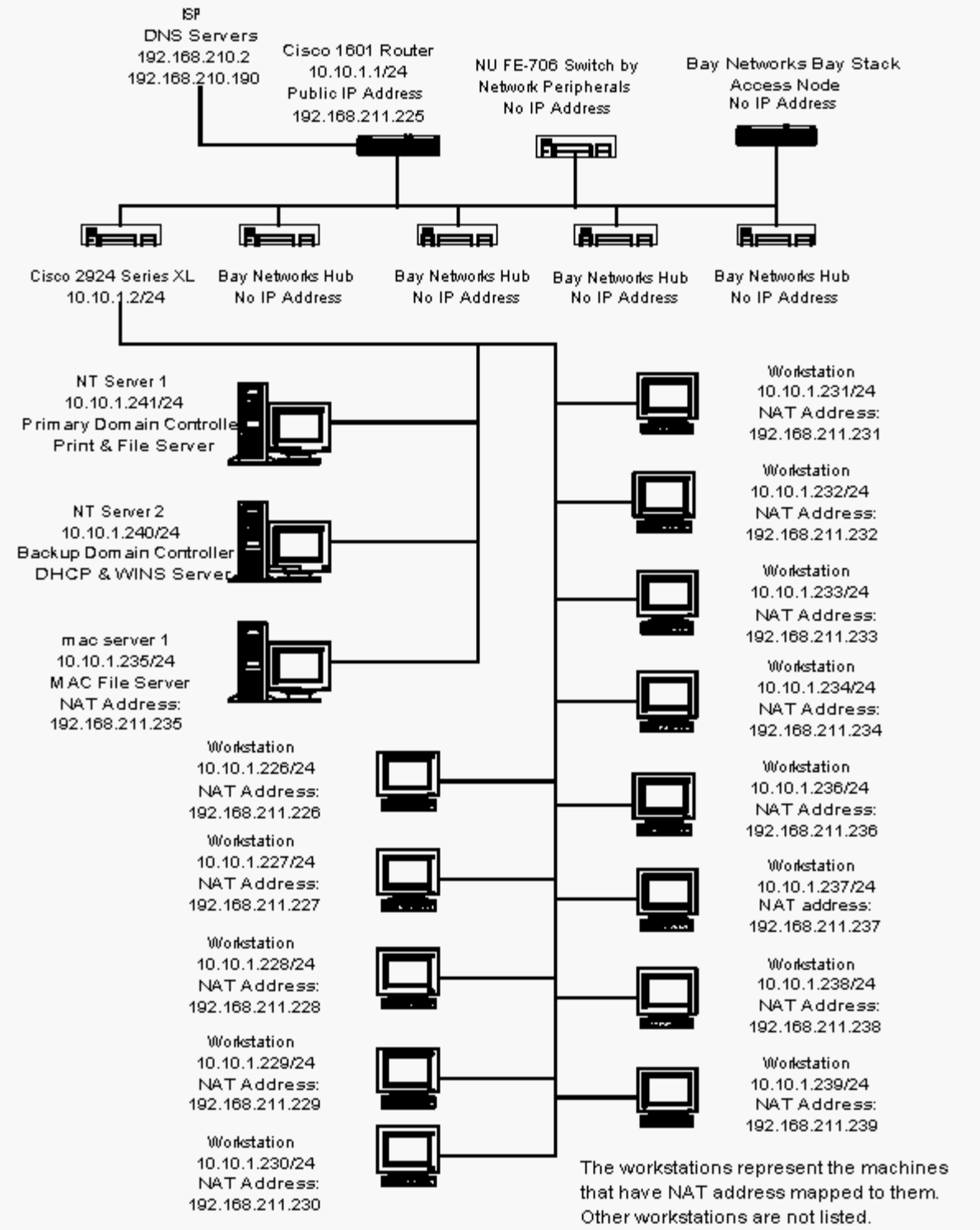

Figure 1

Figure 1 shows the Jones Company network starting at the Cisco 1601 gateway router (Ethernet 10.10.10.1/24 and WAN 192.168.211.225) [1]. Besides unrestricted access to the network closet, the border router had a posted note with the login and enable passwords on it. Access to the router configuration could allow someone to kill the Internet connection, use the router to steal information or use of this router to wage attacks against other networks connected to the Internet. There are many scenarios possible when the border router of a network has been compromised including, the redirection of traffic to other IP addresses or waging attacks from the compromised router.

The router, passed data to a Cisco 2924 Series XL 100 Mbps switch and three Bay Networks Baystack 10BaseT 24-port 10 Mbps hubs and one Baystack 100BaseT 12 port Hub. The Cisco 2924 was a managed switch with a HTTP server running. While this switch did not have an external IP address, the simple password, "jones" left it open to anyone who wanted to investigate the switch configuration. Alteration of the Cisco switch configuration could stop communication to the servers and most network printers.

Data stored locally creates a single point of failure if the local system has problems. At 10 Mbps the Bay Networks switches slowed down traffic throughout the office and caused frustrated users to be more likely to store company data on their workstations. Being in an unlocked closet, was the only security risk associated with the Bay Networks equipment.

The Jones Company server configuration was not secured against accidental data loss or malicious attacks. Users logged onto the Windows NT Domain named Jones.com. The Primary Domain Controller was jones-nt1. This Compaq ProLiant 2500R 6/200 Model 1R had a Pentium Pro running at 200 MHz with 296 MB of RAM. The operating system was Windows NT Server 4.0 with Service Pack 4 and was used as a file server that ran print and backup services. The logical drives D through T had NTFS file systems. The C partition, which held the system files, had a FAT file system. The total storage on this server was 22 GB. The hard drives were setup in a hardware based RAID 5 array to protect data against a hard drive failure.

The jones-nt1 server configuration was vulnerable to known exploits since it was not updated with the latest Windows service pack or security patches. The wasted space made it cumbersome to manage and users storage data in various locations, and at times were not able to remember were data was stored. The use of FAT for the system partition did not allow for access and file level security. Any user with a network account could access the system drive, including system files and logs.

1. All IP addresses have been changed to protect the identity of the organization.

Fixing the security risks was critical. Improper access to the server's system drive could render vital services unavailable to the company.

The Backup Domain Controller for this domain was jones-nt2, a Compaq ProSigna 200 with 233 Mhz processor and 96 MB RAM and running Windows NT Server 4.0 with Service Pack 5. This system had three hard drives in a RAID 5 configuration for redundancy and used an APC UPS for backup power. Data from this server was backed up across the network to a DLT tape drive on the PDC. The RAID configuration and backup were never tested.

There was a high risk of data corruption on the jones-nt2 server. Like the PDC, this server did not have the latest Windows service pack or security patches. The system drive was formatted with FAT. The BDC and PDC servers had the same security vulnerabilities and this doubled the possibility that the servers could be compromised or the taken off line.

The last of the three main servers was a PowerPC G3 with a 300 MHz processor and 192 MB RAM named Mac Server 1. This system was setup for extra network storage. A DLT 4 External Tape Backup was used to backup this system and the server plugged into an APC UPS for backup power. No logon or file level security had been set up on this system. This was not a server class system and did not have the hardware redundancy in place to protect against a hardware failure.

Operating System hardening, hardware redundancy, file level and access level security were major issues for these servers. Data integrity was at risk on these systems. During the network documentation process, I noticed the Windows NT servers were logged onto with the administrator account and all servers were unlocked.

Internet Connectivity and Communication

Jones Company had a fractional T1 at 128kbps that cost more than the price of new WAN connections such as ADSL/SDSL and full even T1 connections. Heavy Email traffic and general web browsing made the Internet connection very slow. A local ISP provided the Internet service, and they had sold the service to the company several years before. No firewall on the Jones network and no intruder detection made the Jones Company network vulnerable to attacks and impossible to determine if internal systems had been compromised. Access control lists were created, but not implemented, on the gateway router. Since ACLs were not applied the router configuration, there was no way this router could stop malicious traffic form entering the network. Jones used NAT to access the Internet with a public IP Addresses range of 192.168.211.224/28 through 192.168.211.240/28. NAT is an excellent way to protect the anonymity of internal systems by allowing them access to the Internet through the same external IP address. Some client machines were using public addresses mapped

to the internal addresses, matching up the last octet of the internal IP addresses to the public addresses. Mapping external IP addresses directly to an internal PC created a risk of outside attacks on these machines. The PCs with mapped external IP addresses were not running personal firewall software. Figure 2 shows the NAT configuration taken from the Cisco router configuration.

NAT From Cisco Router Configuration
ip nat inside source list 32 interface Serial0 overload
ip nat inside source static 1010.1.238 192.168.211.238
ip nat inside source static 1010.1.237 192.168.211.237
ip nat inside source static 1010.1.236 192.168.211.236
ip nat inside source static 1010.1.235 192.168.211.235
ip nat inside source static 1010.1.234 192.168.211.234
ip nat inside source static 1010.1.233 192.168.211.233
ip nat inside source static 1010.1.232 192.168.211.232
ip nat inside source static 1010.1.231 192.168.211.231
ip nat inside source static 1010.1.230 192.168.211.230
ip nat inside source static 1010.1.229 192.168.211.229
ip nat inside source static 1010.1.228 192.168.211.228
ip nat inside source static 1010.1.227 192.168.211.227
ip nat inside source static 1010.1.226 192.168.211.226
ip nat inside source static 1010.1.225 192.168.211.225
ip nat inside source static 1010.1.224 192.168.211.224

Figure 2

The main security concern was the access from the Internet to internal workstations. On August 22, 2001, the external IP addresses were scanned with Superscan, which is available for download from the Foundstone website at http://www.foundstone.com/knowledge/scanning.html. Figure 3 represents the TCP ports that were detected on this scan.

Outside IP Address	Detected TCP & UDP Ports
192.168.211.226	79/tcp
192.168.211.227	135/tcp139/tcp
192.168.211.228	79/tcp
192.168.211.229	79/tcp135/tcp139/tcp
192.168.211.231	79/tcp135/tcp139/tcp
192.168.211.232	79/tcp135/tcp139/tcp
192.168.211.237	79/tcp139/tcp
192.168.211.238	79/tcp

Figure 3

The addresses with ports 135 and 139 open are Windows machines. The listed ports tell a hacker that it is a mixed environment and allows the intruder to pick his or her exploits accordingly. TCP port 135 is the Windows RPC locator and port 139 is the NETBIOS Session Service. For example, Windows enumeration software or a programs that uses Windows services like "net send" or "net use" to connect to the workstations can be used to gather information or communicate with the workstations. The external to internal IP addresses mappings were originally setup for easy access to internal machines by off site employees, but it created a target on the Internet for Windows attacks.

The Internet Service Provider hosted Jones Company email off site. Employees used Quickmail 2.1 as their Email client over a POP3 connection. In order to check Email, users needed to be logged on locally to their computer. To check Email from home, employees used Timbuktu remote control software and connected to their assigned external IP address from their home PC. There were several problems with the way Email was set up. Passwords were sent using clear text and anyone using network sniffer software could capture passwords and Email traffic. Employees communicated via Email that traveled to the ISP's Email server and back to the Email clients. Many times viruses were spread through the company by Email. Data assurance of Email messages and attachments was a problem with Quickmail. Multiple users had problems with the Quickmail software that were only fixed with a reinstall of Quickmail on the affected machine. It was easy to accidentally delete or remove the Email data files from the local systems while reinstalling Quickmail.

Security Policies and Data Assurance

The Jones Company had no written policies regarding use of company computers, they didn't have a password policy. The standard username and password for employees was the user's first name plus first letter of his or her last name. The username and the password matched. These passwords were changed regularly and employees, for the most part, knew each other's passwords. Easily guessed passwords and co-workers who knew other employees' passwords created a false sense of security for employees who believed their information was secure.

None of the systems had the current virus definitions installed on them and the Mac file server and two Compaq servers did not have Antivirus software installed. Because the Jones Company was constantly a victim of viruses, the most important way to create a high level of data assurance is virus protection. The Jones Company had two-licensed copies of Norton Antivirus. None of the Macs had this program installed. Some of the PCs had Norton Antivirus installed from the PC Manufacturers factory installation, but the users were mostly unaware of this software.

Jones Company backup process provided another level of data assurance. No record of the backup process being tested was available and while on a support cal, I realized it was not backing up all of the files. Several directories were not selected for backup and many of the daily backup tapes were useless. These tapes were stored in a file cabinet next to the server. The tapes should have been stored in a secure location off site. Daily backups were full backups – no partial/incremental tape backups were performed. Both the Mac and NT servers utilized a tape rotation that consisted of a Monday through Thursday tape that was reused weekly. The Friday tape was rotated out – a minimum of 6 Friday tapes were kept. A backup tape for the last Friday of the month was kept for at least 5 months. The date of each Friday tape was included on a note within each tape case. The person responsible for changing tapes for the previous days backup took the tapes off site each night. Since the backup process was not properly setup, data loss was a common occurrence and an accepted consequence.

The Process of Securing The Jones Company

Jones Company Network Equipment Upgrade

The number one requirement for the new server design was availability. If employees could not get to their data, they could not perform their jobs. Being able to access data is extremely important to the Jones Company. The hardware upgrade created an excellent opportunity to secure the Jones Company network and remove unused equipment.

The new network design included two servers:
Server 1 - authentication and network services
Server 2 - network storage

Keeping with or goal of data assurance, the SCSI hard disks were selected for speed and RAID (Redundant Arrays of Inexpensive Disks) hardware was ordered for high availability of the data in the event of a hard drive failure.

For Server 1 to perform the required functions, it would need to have a fast processor, plenty of RAM and fast access to hard disks. This server would also have to have dual network cards for load balancing and high data transfer performance. Server 2 would need less CPU speed, RAM and installed services, but it would need more hard disk space for storage and equally as fast data transfer ability.

In an article titled, Network Storage - The Basics, Drew Bird writes about the NAS or Network Area Storage server. He writes, “The beauty of the NAS structure is… storage of data can be centralized, as can the security, management, and backup of the data. NAS also bring an extra level of fault tolerance to the network. Fault tolerant measures such as RAID…can be used to make sure that the NAS device does not become a point

of failure." For this reason The Jones Company agreed that a NAS server running Windows 2000 Powered would be beneficial.

Since Server 1 would control network authentication, a cost effective Operating System for Server 1 was Microsoft Windows 2000 Small Business Server. It was bundled with several other Microsoft server products, including Exchange 2000 and Internet Security and Accelerator Server 2000. This offered local management of Email with Exchange 2000 and a license for Outlook 2000 & 2001 on Jones Company Windows and Mac computers. The Jones Company could protect the internal network and control Internet access with the ISA Server 2000. In The OS Decision, Alan S Key writes, "suppliers have consistently reported that the server versions of Microsoft's Windows NT 4.0--Standard, Enterprise, and Small Business Server (SBS)--have been the OS of choice, particularly for new small business installations." While Small Business Server may seem like it is putting "all of their eggs in one basket", according to Dr. Thomas Shinder of isaserver.org and author of Configuring ISA Server 2000: Building firewalls For Windows 2000, he also recognizes it can configured to perform well. This design offers a much higher level of security and availability then Jones Company had previously.

In order to maximize the benefits of the new servers, we upgraded the Internet connection. The new provider brought in a full T1, moving the external Email from the old ISP to the new ISP's mail servers. This reduced cost and allowed much faster download and upload speeds. The faster Internet access paved the way for Email to be hosted locally.

Creating Security Policies

According to the book Inside Network Perimeter Security, "User accounts with poor passwords are one of the most commonly exploited security weaknesses". After taking over support for Jones Company, the following immediate steps were taken to improve network security:

I changed passwords on the router and servers
I removed posted notes with IP addresses and passwords from the network equipment
I started educating users and suggesting tougher passwords be used

Management did not see the need to enforce password policies and requiring users to change passwords often would create a greater need for administrative support. For this reason the new system would rely on users to create unique passwords with a minimum of seven characters with a mix of numbers and letter not arranged to create words found in a dictionary.

Before the server upgrade, private files were locked by a password in MS Word or MS Excel. With the new servers and domain, I created security groups and new user names. I organized users into groups and gave users access to data based the privileges assigned to their security groups. I reorganized the data structure to keep

sensitive information apart from files accessed by general users. All network drives are configured with NTFS to provide file level security on all data. This was the first time internal security had been applied to data.

The Jones Company servers were never configured to detect unauthorized access attempts. As an added measure of data security, logging was set up on both new servers to log failed and successful network logins. The event log is also monitored weekly. With this policy, a pattern of attempted unauthorized access to the network could be detected and documented.

Securing Jones Company Network Communication

Since Quickmail Email was stored locally on each workstation, if a hard drive failed all Email is lost. Several times in the past, Emails and attachments were deleted when users workstations crashed. I configured MS Exchange 2000 so Email could be stored in an Exchange database on the server. This put everyone's Email in one place and made it easy to back it up daily. Quickmail frequently crashed and this produced corrupted data. In order to connect to the Exchange server, Outlook 2000 for PCs and Outlook 2001 for Macs were installed. This meant added performance and reliability for users who were experiencing problems with Quickmail. By installing the appropriate patches, we protected Outlook 2000 from virus that specifically target Outlook 2000 vulnerabilities. Employees will access Email remotely with Outlook Web Access using Internet Explorer (http://webmail.jones.com). Remote users who want to check Email, no longer use Timbuktu to connect to their workstation. This reduced the number of systems that needed external addressed mapped to their workstation. For the sake of redundancy, POP accounts still reside at the ISP. These accounts collect Email in the event that the local Exchange server loses its network connection. The Exchange POP connector that ships with Microsoft Small Business Server 2000 is set to download POP Email from the ISP to users local mailbox.

After the Exchange 2000 installation and updates (such as Exchange 2000 Service Pack 3) were installed, I configured the Exchange server to protect against open relay exploits and being used to send Spam. SMTP Relaying was blocked on the Small Business Server (as described by Microsoft in figure 4).

Article #	Article Title
304897	XIMS Microsoft SMTP Servers May Seem to Accept and Relay E-Mail Messages in Third-Party Tests
310356	HOW TO Prevent Mail Relay in the IIS 5.0 SMTP Server in Windows 2000
310380	HOW TO Prevent Exchange 2000 from Being Used as a Mail Relay in Windows 2000
313395	HOW TO Examine Relay Restrictions for Anonymous SMTP Connections and Filter Unsolicited E-mail Messages in Exchange 2000

314734	XCON Relay Restrictions on Default Virtual SMTP Server Are Not Working
324958	HOW TO Block Open SMTP Relaying and Clean Up Exchange Server SMTP Queues on SBS 2000

Figure 4

Various web sites test Email servers for open relay exploits and link to site that will test these servers automatically. There are several online tests that will attempt to connect to your SMTP server and send Spam through the open relay.

http://www.abuse.net/relay.html - Abuse.net
http://www.fabel.dk/relay/test - web site information is in Danish, but test is English

It is important to segregate network services to prevent an outage or failure of one service from taking down others. A separate proxy server/firewall or security appliance (such as a PIX 506E) is the preferred way to secure a small network from the Internet. In the case of the Jones Company, since cost was a major factor and when ordering Microsoft Small Business Server, the Internet Security and Acceleration Server was included, ISA was selected as the firewall.

According to Microsoft, ISA Server 2000 provides "secure, fast, and manageable Internet connectivity. ISA Server integrates an extensible, multilayer enterprise firewall and a scalable high-performance Web cache. It builds on Microsoft Windows® 2000 security and directory for policy-based security, acceleration, and management of internetworking." A firewall is essential to a network with inbound and outbound Internet access and ISA gave Jones Company added security.

In an "enterprise" design, the domain controller would be its own server behind the firewall. In the small business environment, when non-technical managers set limits in IT spending, enterprise level designs must be scaled down. Since the Domain Controller is also the Exchange server, it has an external interface on the Internet. ISA is used to secure the Domain Controller/Exchange server from attacks on the Internet. Intruder Detection reports attempted attacks and port scans to the event log sending Email alerts to the network administrator who reviews the log weekly. This log is reviewed weekly. ICMP is turned off and the sever will not reply to pings of trace routes initiated from the Internet. Only ports needed by for inbound access are open. The few the ports that are open, the few points of attack exist from the Internet. This theory was explained to management at the Jones Company as a brick wall with only a few small doors built in to allow access to the other side of this brick wall. These doors are locked and only opened when the proper identification is presented to the guard. This explanation made the concept of a firewall easy for them to understand. This also illustrated the need for secure passwords.

Data Assurance

As part of the up grade documentation, I created a schedule for Jones Company data backup. All backups consist of the MS Exchange Mailboxes and the MS Exchange Information Store along with the system state and all data from the storage server. This type of backup assures that data will not be lost in the event of s system crash. Monday through Thursday differential backups are performed. On Friday a full backup is scheduled. To prevent data loss in the event of a natural disaster, the previous days tapes are taken off site. For another level of assurance, data from closed projects is burned onto CD and stored permanently at a remote location.

To help reduce IT costs I presented the need for Antivirus on all the PCs in the office. With the money spent on reinstalling software on these systems and the time wasted on lost data, I was able to prove a business need for Antivirus software. I installed Norton Antivirus Corporate Edition on the two new servers and all Windows based workstations.

Norton Antivirus Corporate Edition software is a certified anti-virus scanner by ICSA Labs for both the On Demand and On Access categories. Listed below in figure 5 are the criteria for this certification:

ICSA Labs Criteria
ON DEMAND Module: Products to receive the ICSA Labs Certified mark must:
Detect 100% viruses listed in the current In The Wild List Detect 100% viruses listed in the ICSA Labs Common Infectors Test Suite Detect 100% of ICSA Labs Polymorphic Test Suite Detect 90% of the ICSA Labs Virus Collection Products achieving ICSA Labs certification will not cause any false alarms. The False Alarm tests will be conducted against the ICSA Labs False Positive Test Suite.
ON-ACCESS Module: Products to receive the ICSA Labs Certified mark must
Detect 100% viruses listed in the current In The Wild List Detect 100% viruses listed in the ICSA Labs Common Infectors Test Suite Detect 90% of macro viruses in the ICSA Labs Macro Virus Collection

Figure 5

Products achieving ICSA Labs certification will not cause any false alarms. The False Alarm tests will be conducted against the ICSA Labs False Positive Test Suite.

Secured Network: October 2002

With the network upgrade finished and support standards in place, the Jones Company can enjoy the freedom of enterprise level services without many of the security pitfalls that small businesses face when they implement on site Email and Internet access.

Network Infrastructure Diagram

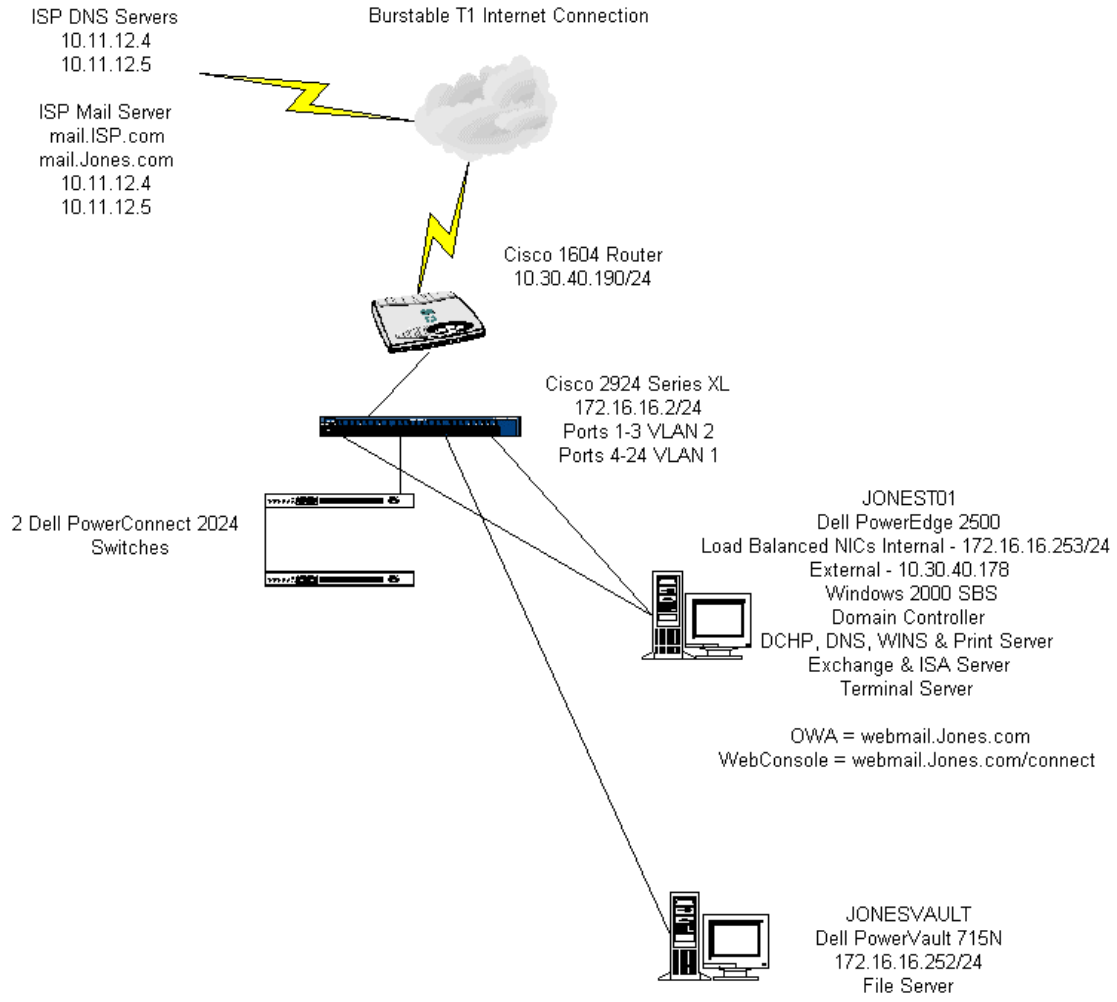

Figure 6

Jones Network Equipment

Jonesnt01 - Domain Controller Server Hardware:
Sever Model: Dell PowerEdge 2500
Operating System: MS Windows 2000 Small Business Server - SP 3
Processor: 1.1 GHz
Memory: 1 GB RAM
Fault Tolerance: RAID 1 Mirrored Across Both Drives
Hard Drives: 2 - 16.95 GB Drives
Network Cards: 1- Intel 8255x 10/100 (External Interface) & 2- Intel PRO/100+ Duel Port (Internal Interface)
Tape Drive: Internal Dell PowerVault 110T LTO Drive
Backup Tapes: Fuji 100/200GB Ultrium Tape Cartridge – two rotated daily and two rotated weekly

Jonesnt01 - Domain Controller Services:
Active Directory
Print Server – Allows local computers to print to queue based printers
DHCP Server – Assigns IP addresses to local computers
DNS Server – Provides Local Name Resolution
Exchange Mail Server – Email Server
Primary Norton Antivirus Server – Protects clients' PCs from viruses
ISA Firewall – Monitors Internet traffic and blocks local systems from attacks
ADP Server – Financial software for accounting
Terminal Services Administration
Tapscan Server – Media software for radio/TV commercial reporting
Backup Exec 8.6 with Exchange Backup Agent

Jonesvault - Storage Server Hardware:
Sever Model: Dell PowerVault 715N
Operating System: MS Windows 2000 Powered - SP 3
Processor: 1.0 GHz
Memory: 512 MB
Fault Tolerance: RAID 5 across all drives & RAID 1 Across Disks 0-1 and 2-3
Hard Drives: 4 - 111.74GB drives
Network Cards: 2 - Intel 8255x 10/100

Jonesvault - Storage Server Services:
Active Directory
Terminal Services Administration
Backup Exec 8.6 Remote Agent

Data Assurance

Since the Jones Company has not had problems with viruses on the Macs, Antivirus software has not been purchased for them. Norton Antivirus Corporate Edition is running on both server and Windows workstations.

Norton Antivirus Corporate Edition Version 7.51 configuration:
Primary Server: JONESNT01
Secondary Server: JONESVAULT
Managed Installation on clients
Weekly Live Update Packages at 12:00 am Saturday – updates pushed to clients
Weekly Virus Scans on servers and PCs are at 12:00 am Sunday
Real Time scanning is set on all systems.

Data stored on Jonesnt01 is protected by hardware based RAID 1 mirrored across both drives. With hot-swap hard drives, hot-swap redundant fans, hot-swap redundant

power supplies, any one of these devices can fail and the other redundant device continues to operate without interfering with normal server operations. When the replacement device is obtained, it can be replaced reinstalled without having to power off the server. This creates reliability by allowing for a quick change of disabled or failed components. This server also has an internal SCSI tape drive that backs up data from both servers.

Jonesvault data is protected by redundant operating system images, hot swap drives, dual fail over Ethernet controllers and the ActiveArchivesTM snapshot utility with hardware RAID 5 across all four.

Secured Communications

Internet access is a T1 line that is provided by a local ISP. There are 14 usable external network addresses. The external IP address range from 10.30.40.177 to 10.30.40.189.

The DMZ is designed for a future FTP server that may host files available for Jones Company customers to download. It is a true DMZ located outside of the firewall and between the border router and the Small Business Server 2000. Since the ISA server performs NAT, I chose not to perform NAT on the router to limit connection problems that can occur with an ISA server behind a NAT router. This also allows the ISA server to perform VPN (Virtual Private Networking).

Exchange 2000 SP3 provides Email services for Jones Company allowing users to exchange Email internally and share calendars. Jones can control Email access of employees and add and remove users at will. The primary method for incoming and outgoing Email is SMTP provided by an SMTP Connector on the JONESNT01 Exchange server. The POP3 connector on the JONESNT01 Exchange server provides the secondary method for incoming Email. The POP3 connector provides for a receipt of Email, if the server JONESNT01 server goes down or if Internet access is lost. When the server or Internet becomes available, the POP3 connector retrieves Email from the ISP mail servers. Remote Email access is granted according to Windows username and password. Outlook Web Access is part of the Exchange 2000 server and provides the Webmail service. Webmail can be accessed at http://webmail.Jones.com and can be access anywhere on the Internet. Figure 7 shoes the MX file hosted on the ISP's DNS servers. It shows that Email is directed to the jonesnt01 server first, and then the ISP's Email server second. This also shows the URL for webmail.

Jones MX Records
Preference 10, mail exchanger = webmail.Jones.com
Preference 20, mail exchanger = mx1.ISP.com
Preference 30, mail exchanger = mx2.ISP.com

Figure 7

A test for open relay was performed on the Exchange 2000 server from http://www.abuse.net/relay.html. Figure 8 shows the results of this test.

Abuse.net Open Relay Test Results
Connecting to 10.30.40.178 for anonymous test ... <<< 220 simnt01.simantel.local Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at Mon, 2 Dec 2002 09:53:56 -0600 >>> HELO www.abuse.net <<< 250 jonesnt01.jones.local Hello [208.31.42.77]

Relay test 1
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<spamtest@abuse.net>
<<< 250 2.1.0 spamtest@abuse.net....Sender OK
>>> RCPT TO:<relaytest@abuse.net>
<<< 550 5.7.1 Unable to relay for relaytest@abuse.net

Relay test 2
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<spamtest>
<<< 250 2.1.0 spamtest@simantel.com....Sender OK
>>> RCPT TO:<relaytest@abuse.net>
<<< 550 5.7.1 Unable to relay for relaytest@abuse.net

Relay test 3
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<>
<<< 250 2.1.0 <>....Sender OK
>>> RCPT TO:<relaytest@abuse.net>
<<< 550 5.7.1 Unable to relay for relaytest@abuse.net

Relay test 4
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<spamtest@[10.30.40.178]>
<<< 250 2.1.0 spamtest@[10.30.40.178]....Sender OK
>>> RCPT TO:<relaytest@abuse.net>
<<< 550 5.7.1 Unable to relay for relaytest@abuse.net

Relay test 5
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<spamtest@hansoninfosys.com>

<<< 250 2.1.0 spamtest@isp.com....Sender OK >>> RCPT TO:<relaytest@abuse.net> <<< 550 5.7.1 Unable to relay for relaytest@abuse.net

Relay test 6
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<spamtest@[10.30.40.178]>
<<< 250 2.1.0 spamtest@[10.30.40.178]....Sender OK
>>> RCPT TO:<relaytest%abuse.net@[10.30.40.178]>
<<< 550 5.7.1 Unable to relay for relaytest%abuse.net@[10.30.40.178]

Relay test 7
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<spamtest@[10.30.40.178]>
<<< 250 2.1.0 spamtest@[10.30.40.178]....Sender OK
>>> RCPT TO:<relaytest%abuse.net@isp.com>
<<< 550 5.7.1 Unable to relay for relaytest%abuse.net@ISP.com

Relay test 8
>>> RSET
<<< 250 2.0.0 Resetting
>>> MAIL FROM:<spamtest@[10.30.40.178]>
<<< 250 2.1.0 spamtest@[10.30.40.178]....Sender OK
>>> RCPT TO:<"relaytest@abuse.net">
<<< 250 2.1.5 "relaytest@abuse.net"@jones.com

Figure 8

In figure 8, Relay test 8 appears to be successful, but the Exchange Virtual server queue shows no mail waiting for from this test.

Remote network administration will save the client time and money. It reduces the need for support personnel to come on site. Terminal Service Administrator is installed on both servers and external access to Terminal Services from the Internet is obtained by making a VPN connection with the Microsoft VPN client to Microsoft VPN and RAS on the Small Business Server. The Terminal Services Client connects to the internal address of the either server. Since port 3389 is not published to the Internet, a potential hacker cannot exploit Terminal Services.

HTTP Administration and Telnet for the Jonesvault server is enabled on the internal network. https://JONESVAULT:1279 is the PowerVault NAS Manager, and both a user name and a password are required to login. Telnet on port 23 to JONESVAULT will allow access to disk drives.

Internal name resolution for Active Directory is done through DNS running on JONESNT01, the domain controller. JONESNT01 has forwarders pointing to external servers at 10.11.12.4 and 10.11.12.5, the ISP's DNS servers. DNS services are only available to internal clients on the network.

Figure 9 lists the ISA server settings that block outside access and detect attacks.

Firewall and Intruder Detection settings:
Traffic to all destinations is allowed IP Packet Filtering is enabled Intrusion detection is enabled IP routing is enabled
Enable filtering of IP fragments: True Enable filtering IP options: True Log packets from 'Allow' Filters: True
Enable detection of the selected attacks: Windows out-of-band (WinNuke): True Land: True Ping of Death: True IP Half Scan: True UDP Bomb: True Port Scan: True Detect after attacks on 10 well-known ports Detect after attacks on 20 ports

Figure 9

Figure 10 shows the server publishing rules that allow three employees remote access to their workstations. The external NIC on the ISA server is multi-homed with several external IP addresses.

Server Publishing Rules:
Server Publishing Rule Name: Timbuktu Control – User1 Enabled: True IP Address of Internal Server: 172.16.16.231 External IP Address on ISA Server: 10.30.40.179 Protocol Used: Timbuktu Control Primary Port Used by Protocol: 1417 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Control – User2 Enabled: True IP Address of Internal Server: 172.16.16.220

External IP Address on ISA Server: 10.30.40.178 Protocol Used: Timbuktu Control Primary Port Used by Protocol: 1417 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Control – User3 Enabled: True IP Address of Internal Server: 172.16.16.232 External IP Address on ISA Server: 10.30.40.180 Protocol Used: Timbuktu Control Primary Port Used by Protocol: 1417 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Exchange – User1 Enabled: True IP Address of Internal Server: 172.16.16.231 External IP Address on ISA Server: 10.30.40.179 Protocol Used: Timbuktu Exchange Primary Port Used by Protocol: 1420 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Exchange – User2 Enabled: True IP Address of Internal Server: 172.16.16.220 External IP Address on ISA Server: 10.30.40.178 Protocol Used: Timbuktu Exchange Primary Port Used by Protocol: 1420 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Exchange – User3 Enabled: True IP Address of Internal Server: 172.16.16.232 External IP Address on ISA Server: 10.30.40.180 Protocol Used: Timbuktu Exchange Primary Port Used by Protocol: 1420 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Handshake – User1 Enabled: True IP Address of Internal Server: 172.16.16.231 External IP Address on ISA Server: 10.30.40.179 Protocol Used: Timbuktu Handshake Primary Port Used by Protocol: 407 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Handshake – User2 Enabled: True

IP Address of Internal Server: 172.16.16.220 External IP Address on ISA Server: 10.30.40.178 Protocol Used: Timbuktu Handshake Primary Port Used by Protocol: 407 Rule Applies to: Any Request
Server Publishing Rule Name: Timbuktu Handshake – User3 Enabled: True IP Address of Internal Server: 172.16.16.232 External IP Address on ISA Server: 10.30.40.180 Protocol Used: Timbuktu Handshake Primary Port Used by Protocol: 407 Rule Applies to: Any Request

Figure 10

Figure 11 shows the custom protocol definitions that tell the ISA server what ports will be open from the Internet.

Custom Protocol Definitions:
Protocol Definition Name: HTTP Server Initial Connection Port Number: 80 Initial Protocol Type: TCP Initial Direction: Inbound
Protocol Definition Name: HTTPS Server Initial Connection Port Number: 443 Initial Protocol Type: TCP Initial Direction: Inbound
Protocol Definition Name: Timbuktu Control Initial Connection Port Number: 1417 Initial Protocol Type: TCP Initial Direction: Inbound
Protocol Definition Name: Timbuktu Exchange Initial Connection Port Number: 1420 Initial Protocol Type: TCP Initial Direction: Inbound
Protocol Definition Name: Timbuktu Handshake Initial Connection Port Number: 407 Initial Protocol Type: UDP Initial Direction: Receive and then Send

Figure 11

At the end of the server upgrade project, I used Superscan to perform a network scan against the Jones Company. The only address that responds with ports open is 10.30.40.178.

An external port scan of JONESNT01 reported the following open ports:
25 - Simple Mail Transfer – Email Protocol
80 - World Wide Web HTTP - Used for Web mail
443 – HTTPS - Used for Web mail
1417 - Timbuktu Service 1 – Mapped to internal workstation
1420 - Timbuktu Service 4 – Mapped to internal workstation

Figure 12

Applying Defense In Depth to a small business requires the review and possible change to network hardware, services, policies and procedures. It almost always requires the network engineer who is designing the project to work within a strict budget. By purchasing new equipment, reconfiguring existing equipment and providing user education, I was able to bring Jones Company to an acceptable level of security.

References

Bird, Drew. "Network Storage - The Basics." 2 Feb 20 02.
URL: http://www.smallbusinesscomputing.com/buyersguide/article.php/981791 (2 Dec 2002)

Kay, Alan S. "The OS Decision." 1 Jun 2000.
URL: http://www.smallbusinesscomputing.com/biztools/article.php/688121%20 (2 Dec 2002)

Shinder, Thomas. "Installing ISA Server on a Domain Controller." 18 Jan 2002.
URL:
http://www.isaserver.org/tutorials/Installing_ISA_Server_on_a_Domain_Controller.html (2 Dec 2002)

Northcutt, Stephen. Zeltzer, Lenny. Winters, Scott. Frederick, Karen Kent. Ritchey, Ronald W. Inside Network Perimeter Security Indianapolis: New Riders, 28 JUN 2002. 241 – 243.

Microsoft. "Internet Security and Acceleration Product Overview." 3 May 2001.
URL: http://www.microsoft.com/isaserver/evaluation/overview/default.asp (2 Dec 2002)

ICSA Labs. "Certified Products - Anti-Virus Scanner."

URL: http://www.icsalabs.com/html/communities/antivirus/certification/certprod.shtml (2 Dec 2002)

Microsoft TechNet. “HOW TO Prevent Exchange 2000 from Being Used as a Mail Relay in Windows 2000.” 310380.10/26/2002.
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;310380 (2 Dec 2002).

Microsoft TechNet. “HOW TO Block Open SMTP Relaying and Clean Up Exchange Server SMTP Queues on SBS 2000.” 324958. 11/11/2002.
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;324958 (2 Dec 2002)

Network Abuse Clearing House. “Mail Relay Testing.” 3 Mar 2000.
URL: http://www.abuse.net/relay.html (2 Dec 2002)

Fabel Relay Test. “Test Your Relay.” 20 Jan 2002.
URL: http://www.fabel.dk/relay/test (2 Dec 2002)

Last Updated: May 23rd, 2017

Upcoming Training

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