Global Information Assurance Certification Paper

Upgrading a Windows NT 4.0 Network to a High Security Windows 2003 Network

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4c
Option 2

Kenneth W. Hughes
19 October 2004

Abstract

Upgrading from one version of an operating system to another is never as easy as one might think, especially when network security is involved. The purpose of this paper is to describe the path used to upgrade my departments' secured windows NT 4.0 network to Windows 2003 servers and Windows 2000 workstations. This paper is divided into three sections: Before, During, and After. The "before" section looks at the secured Windows NT 4.0 Network from various aspects and explains why we decided to upgrade. The "during" section looks at the steps taken to identify the appropriate upgrade procedure and the challenges of implementation. The "after" section looks at the upgraded network and at the benefits and consequences of the upgrade and further changes that need to be made.

Before

Our original network came on line in late 1999. The goal was to have a highly secured system of Windows NT 4.0 Workstations with a Windows NT 4.0 Domain and a data server. We defined several objectives in planning for the new network, priority considerations were data integrity, access control, and availability. Since data integrity and availability are ultimately dependent on system security, we approached this from several directions.

Hardware. To maintain high availability, the server was configured using RAID 5 with a hot fail-over drive and a cold spare. The data server was also equipped with a giga-bit fiber optic card. To ensure the users' ability to log on to the system, we included a primary domain controller (PDC) and a backup domain controller (BDC). To handle the client side requirements we chose machines with dual Xeon processors.

Network. The original design was for a standalone network. All servers and workstations were to be directly connected to a single 24 port 100mb switch. However, when relocation of two of the workstation locations created distance issues, two of the connections required 100mb fiber cabling with transceivers on each end to convert back to CAT 5. So, for the first two and a half years of the project the network was completely separate from other LANs in our building. When some users were relocated in the building, it became impossible to reach two of the secured workstations. At that time we decided that these two computers would be connected back to the secure network through our lower security network, by creating a new virtual local area network (vLAN). Two ports in other switches were programmed to communicate with a port in the secured network's switch.

Security. Both physical and software security issues were addressed. On the physical side, the servers were placed in a locked environmentally controlled room. Workstations were placed in secured areas of the office suites in which they were located. On the operating system and application side, the *SANS: Windows NT Security Step by Step* manual was used to help configure the systems. As with any security design some modifications to the SANS configuration was necessary for individual applications and system functions to work. For example, phase 3, Step 3.3 Disabling floppy disk drives[1], could not be applied because this would have made it impossible for users to do their work. Network shares were used on the server to limit and control access to the servers. Users were assigned to specific groups and had restricted rights to the data. An additional layer of protection was added by installing a program that monitored each workstation for unauthorized access or attempts to exceed the user's security level. If users failed three times to successfully login the server would dial my pager and send the event viewer lockout message.

[1] The SANS Institute Windows NT Security Step by Step Version 2.15

We also implemented a disaster recovery plan and a backup plan to protect all central and workstation data. Each night two full backups were performed. One for on-site storage the other for off-site. Even though the network was isolated from other networks and the internet, we ran an antivirus program and routinely updated the virus pattern on the workstation each time the user logged on.

Having provided an overview of our secure network, I will turn to a description of factors that influenced our decision to upgrade the network and its systems. As with any upgrade, we weighed risks against anticipated benefits.

Risks. The first thing we had to ask ourselves is, "what is the risk of not upgrading and, if the system works now, why change?" The answer is," support." Vendors eventually end support for legacy systems. An article dated July 19th, 2001 released by Microsoft entitled, "Update on Windows NT 4.0 Service Pack 7". Stated, "Based on customer feedback, demand for Windows NT 4.0 hot fixes, and the increased stability of NT 4.0 SP6a, Microsoft has decided not to release Windows NT 4.0 Service Pack 7 (SP7), originally scheduled to release third quarter of 2001."[2] This marked the decline in Microsoft's support for the Windows NT 4.0 line. Although Microsoft continues to provide small critical security fixes for Windows NT 4.0 servers. No new service packs were disseminated. Non-security related fixes were no longer available. The risk of this situation is that OS bugs with drivers and application issues would be left unresolved.

Another push to upgrade came from the vendor of our main application who recommended as the OS Windows 2000 or higher. In repeated help calls, the application vendor said that most of our problems with the application were resolved by running on the newer operating systems.

After attending the SANS Security Essentials course, I identified another risk. Although the system was primarily standalone, it was not impervious to attacks and without routine security fixes, the system would become vulnerable. All of these risks combined to make it clear that an upgrade was important to continued reliability of the system.

[2] Microsoft, "Microsoft Update on Windows NT 4.0 Service Pack 7"

During

Early in 2004 we began researching steps required to upgrade our network to Windows Server 2003 Standard Edition and our workstations to Windows 2000 Professional. The process was separated into two phases. Phase 1 was server upgrade. Phase 2 was workstation upgrades.

Phase 1 – Server Upgrade.

Due to Windows 2003 Server's operating system requirements the domain controller's hardware had to be replaced. This turned out to be an advantage, because rather than doing an inline migration, we chose to create a new tree. This enabled us to leave the old system online during the upgrade. The disadvantage was having to recreate all users and groups in the new tree. However, in this instance the number of users and groups was relatively small, so the advantage of remaining on line far outweighed the recreation effort.

The domain controller starts with a standard installation of Windows 2003 Server. Once the server was up and running I added the role of Domain Controller (Active Directory) and the role of DNS (Domain Name System). "Active Directory uses Domain Name System (DNS) to locate domain controllers, enabling computers joining the network to obtain a domain controller, and then begin the process of network authentication."[3] Since the network was standalone and had no access to a DNS, a DNS had to created. To help protect the server, McAfee VirusScan Enterprise 7.0.0 was installed as were all of the Microsoft updates. Since the server normally operates in a standalone environment without internet access, downloading the Microsoft updates necessitated connecting the server to a less secure network with internet access. This required changing the IP address, subnet mask, gateway, and DNS. The downloads generally take about an hour or two. I have learned from experience not to download drivers or unnecessary updates or programs. Once all necessary updates were installed, I reset the IP configuration to the standalone network.

My next step was to review Microsoft's *Windows Server 2003 Security Guide*[4]. It is a 292 page adobe PDF detailing how to harden a Windows Server 2003. Although some of the information was relevant to my department's situation, other parts were pertinent to larger scale networks. It was important to read it all, so that I could make good decisions about the proper configuration of the new network.

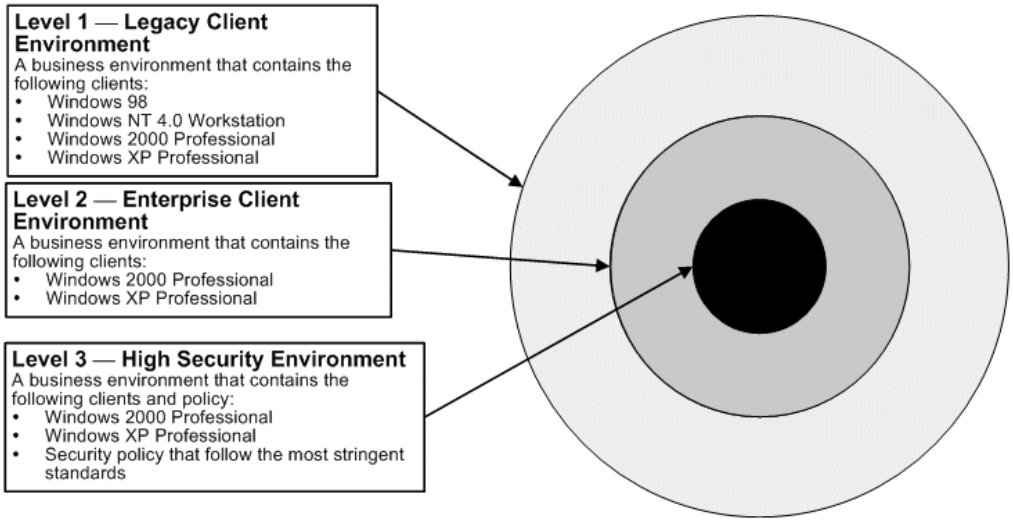
After that review, I focused on the appropriate level of security, each level has its own benefits and consequences. Figure 1.0[4] shows the three levels of security as defined by Microsoft.

---

[3] Microsoft, "DNS requirements for joining an Active Directory domain"

[4] Microsoft, "Windows Server 2003 Security Guide"

Figure 1.0



Since our network requires high security (Level 3), I used the High Security - Domain template provide by Microsoft when you download the *Windows Server 2003 Security Guide* .

Importing the high security template: Start Active Directory Users and Computers, right – click the Domain, and then select Properties. On the Group Policy tab, click New to add a new GPO. Type High Security - Domain Policy, and then press Enter. Right – click High Security - Domain Policy, and then select No Override. Select High Security- Domain Policy, and then click Edit. In the Group Policy window, click Computer Configuration\Windows Settings. Right – click Security Settings, and then select Import Policy. In the Import Policy From dialog box, navigate to Tools and Templates\Security Guide\Security Templates, and then double – click High Security - Domain.inf. When going through the template I change a few of the setting, I prefer to use Authenticated User as apposed to just user in most cases. Close the Group Policy that has been modified. Close the Domain Properties window. The procedure for importing the High Security - Domain Controller is similar to that of the domain except you assign it to the domain controller OU's group policy object (GPO). Run gpupdate.exe /force.

Dealing with the data server's conversion from Windows NT 4.0 to Windows Server 2003 took more time than the domain controller configuration. Upgrading the domain controller had not affected the network or users' ability to access data. Upgrading the server meant users would have to be off the system until the upgrade was complete. In order to avoid a disruption of users' work, I copied all data files from the server to the old domain controller and recreated the network shares the night before the upgrade.

The final step before starting the upgrade was to create a good backup of the data

server and verify it. A good backup of the system is very important because it allows for data recovery should problems be encountered with installing the new operating system. Rather than doing an upgrade on the data server, I reformatted the hard drives and performed a standard installation of Windows Server 2003. Then from the “Mange your Server” application I added the role of file server. I then installed McAfee VirusScan Enterprise 7.0.0 with the most current super DAT. As with the domain controller, I temporarily connected the new data server to a less secure network for internet access in order to get all relevant Microsoft updates. After completing the updates I reset the server to the original standalone network settings. The next step was to join the new domain. Before adding a computer to a Windows 2003 Domain, several new DNS entries are required. The following is a description of the required entries.

"Computers joining an Active Directory domain need the following resource records in DNS to locate an Active Directory domain controller:

• _ldap._tcp.dc._msdcs.DNSDomainName SRV resource record, which identifies the name of the domain controller that hosts the Active Directory domain.

DNSDomainName is the DNS name of the Active Directory domain the computer is attempting to join.

• A corresponding address (A) resource record that identifies the IP address for the domain controller listed in the _ldap._tcp.dc._msdcs.DNSDomainName SRV resource record."[3]

Once the entries were made into the DNS, I ran a test by pinging the new data server from the domain controller using the fully qualified server name and then performed a ping test from the new data server for the domain controller. To add the server to the domain open the system properties dialog box in the control panel and toggle to the computer name tab. Click the Change button. Set the “Member of “ radio button to Domain and then fill in the box with the fully qualified domain name. Click OK. You will be prompted for an account with privileges to add computers to the domain. If successful, a welcome to the domain box will be displayed. Reboot.

Once the data server was in the domain, I added the server role of secondary domain controller. This added redundancy to the Active Directory (AD). After Active Directory was installed, I issued a gpupdate.exe /force from the primary domain controller. This synchronized the secondary domain controller to the primary.

The next step was to copy the files from the old domain controller to the new file server. After data files and directories had been created on the new data server, it was time to install Computer Associates’, BrightStor ARCserve 11 enterprise backup software. To create a complete backup of the system, I also installed the open file and database agents. After obtaining a good backup, I recreated the users and groups. In order to

have a fresh and clean user configuration, but maintain the old users and groups, I carefully checked all user and group settings to insure accuracy.

Once all groups had been created, I recreated the network shares. I like to use the "$" at the end of each network share name, for example "HR$". The "$" will hide the share from the network browser. Network shares add an additional layer of security. Each share has its own permissions and access control. One group may have modify rights, while another has read rights only. These are independent of the rights that are assigned to the directory by the file system.

Phase 2 Workstation Upgrade.

The workstation upgrade started by taking one of the network workstations offline. After copying all relevant user data files to removable media, the hard drive's partitions were deleted. It was important to delete the old partitions, so that Windows 2000 Professional could take full advantage of the entire hard drive capacity. Windows NT 4.0 has a boot partition limitation of 7.8GB. This required the drive to be split into two partitions. While there are advantages to having a two partition configuration, in our case main application occupied almost an entire partition and when combined with the operating system resulted in little useable disk space.

On the blank hard drive, I performed a standard install of Windows 2000 Professional. Once the installation was completed, I temporarily reset the IP configuration to our less secure network with Internet access to obtain all new security patches and updates. I then reset the IP configuration to the secure standalone network.

Raising the workstation's level of security was accomplished in two steps. The first step was to apply the Windows 2000 Professional Gold Standard template. The detailed procedures I use to applying the Gold Standard Template can be found in *Securing Windows 2000 Professional, Using the Gold Standard Security Template*, version 3.0 from SANS Press. This was the manual used in the SANS Securing Windows 2000 Professional training I attended during the fall of 2003. I then installed all applications and copied all default data files to the new workstation. Before joining the workstation to the new domain, I made an image of the hard drive.

There are several reasons for should making an image of the workstation drive before joining the domain. One, it allows a quick redo of the rest of the remaining workstations. The second and most important reason is that an image of a drive, that is already a member of a domain can only be used to restore the workstation from which the image was made. That is because the domain controller will reject subsequent machines created from the image because the new duplicate workstation would have the same unique ID assigned by the domain to the original workstation. This may also temporarily affect the original workstations standing in the domain. So it is better to create a pre-domain image and join subsequently imaged drives to the domain through the standard procedure.

To join the domain you must do two things. First, make sure you have set the preferred DNS to the new Domain Controller running DNS. To check the setting perform follow the steps:

1. Click “Start”.
2. Select Settings.
3. Select Network & Dial-Up Connections.
4. Right click on the “Local Area Connection”.
5. Select Properties.
6. Double click on “Internet Protocol (TCP/IP)”.
7. Now look at the “Preferred DNS server” line.
8. If it is correct just cancel out, other wise, make the change and click “OK” and then “OK” on the Internet Protocol (TCP/IP) properties dialog box.

The second step, from the control panel double click on the System applet. Now click the “Network Identification” tab then click the “Properties” button. Click the radio button from Workgroup to Domain. Type in the fully qualified domain name then click “OK”. You will be prompted for an account with permissions to join the domain. I used the Domain admin account. After a moment or two you should receive a welcome to the Domain message and the click “OK” and you will now be prompted to reboot. Once you have finished rebooting and are about to test the domain connection, make sure the “log on to:” is set to the Domain.

After testing the connection I copied all user data files from each workstation to removable media and off and proceeded to re-image each workstation. On each re-imaged machine the Windows unique Security Identifier (SID) must be changed. Most imaging programs come with a SID changing program. Failure change the SID can create problems down the road. When users look at the machine they just see the computer’s name, but when computers communicate back and forth they use the GUID and SID. If several machines use the same SID, a denial of service could result.

Monitoring. Once all workstations had been upgraded, I installed the new ELM 3.1 enterprise manager software by TNT software. "ELM Enterprise Manager™ gives IT administrators and managers the power to see the health and status of distributed systems with a single glance by combining the following core functions into a feature-packed, reliable, and scalable application."[5]

There are two forms of the ELM agent, the thin agent and the service agent. Each has advantages and disadvantages. The thin client uses fewer resources but increases network traffic with system status information. The service agent produces less

[5] TNT Software, ELM Enterprise Manager 3.1

network traffic but uses system resources. The service agent can also monitor more system functions. I found that it was more effective to use the service agent. When using the thin client the constant stream of responses from all the workstations on this network interfered with user performance.

To install ELM program you must first install the ELM server. Just insert the CD into the server you wish to install the ELM server and from Windows explorer locate the CD and right click on the EEm31_xxx.msi and select install. A Dialog box will appear and will walk you through the installation process. When asked which features to install select all available feature. This will install the server, console and service agent. To install the service agent on other servers and workstations just follow the steps above except just chose the service agent only. The thin client can be installed from the ELM server console if desired. Once the server is up and running and the service agents have been installed on all the systems to be monitored, they must now be registered with the ELM server this is done by logging in to each system with administrative rights and then running the tntagent.exe in the c:\winnt\tntagent. Click “File” then “Register” a box will appear asking for the ELM server and then you will be asked for an account with permissions to connect to the server. Once you have entered the information just click the “Finish” button. The system is now registered with the ELM server and performance and security information can be copied from the service agent to the ELM server. The ELM monitoring software can generate reports and even page an admin if a user account gets locked out.

Updates. Once the workstations were rebuilt and up to date, the next question was, how to maintain high security? Anti-virus updates were a semi-manual process with the prior configuration. I would daily check McAfee’s website, to see if a new superDAT was available. If there was a new superDAT, I would download it to a USB thumb drive then copy it to the netlogon directory on the Domain controller. The superDAT would be installed on each workstation the next time the user logged in. This was done by using a batch file executed by the logon script. When batch file ran it would check the user’s computer for a special file. If the file did not exist the batch file would install the superDAT and the special file would be copied to the workstation . This would keep the batch file from trying to install the superDAT each time a user logged on.

The more challenging task was keeping up with Microsoft security patches and updates because the network did not have direct Internet access. In a standalone network all updates and patches had to be manually downloaded from Microsoft’s website and manually applied to the servers and workstations. This was not a good use of resources and time. The upgrade gave us an opportunity to change that situation.

Since we could not allow the workstations direct access to the Internet, we decided to implement a Windows 2003 Web Server running Microsoft’s Software Update Service (SUS) in a lower security network where Internet access was allowed. The SUS server has access to Microsoft’s website. To get the workstations in the standalone network to

see the SUS server, the network was connected to a port on the main network's CISCO PIX firewall. The firewall's rule for the secure network allowed a connection through the firewall to be established only by computers in the secure network. No inbound traffic would be allowed from any other vLAN on the main network and the out-bound traffic was limited to the SUS server.

To redirect the workstations to look at the SUS server for critical updates instead of Microsoft's Windows update website, in an Active Directory environment the Domain's group policy must be modified. The specific instructions can be found on pages 51 - 61 in *Deploying Microsoft Software Update Services* (SUS_Deployguide_sp1.doc)[6]. This document also covers how to install the SUS server a Windows 2000 or 2003 server.

The SUS server only pulls down Microsoft updates tagged critical. The SUS server has two options for making the critical updates and patches available. The first is automatic, when the SUS server synchronizes with Microsoft's Windows update server, updates and patches are immediately approved for distribution. The second option is an automatic synchronisation with the updates and patches put in a hold directory until they are marked by the administrator as approved for distribution. Using this procedure requires the system administrator to manually download, transfer, and install the recommended and non-critical updates, but this is more acceptable given the relative frequency of critical to recommended updates.

After

Prior to the upgrade to Windows 2003 servers and Windows 2000 Professional workstations, the network was becoming more and more vulnerable to attacks. Windows NT, had not been updated for several years. There are no longer any security patches for it. As more and more NT security vulnerabilities are discovered, the chance of a security breech increases. The upgrade has resulted in improved security. The SUS server allows workstations and servers to get approved critical updates and patches in a more timely fashion than was possible with the manual system employed on the purely standalone network. The new ELM monitor software allows me to better track computer and network problems. I can now quickly be alerted if a machine gets disconnected from the network, shutdown or if someone is attempting unauthorized access. Windows 2000 Professional and Windows 2003 server have improved security over Windows NT 4.0.

The upgrade and increased security controls have yielded some undesired results. The first is that the base high security template imposed new limitations on applications running from a CD. The template set the CD rom drive to run only at the level of the user logged on. This might not sound like a problem, but it created an obstacle to

[6] Microsoft, "Deploying Microsoft Software Update Services".

installing applications even when logged in as the administrator. Several programs, for example, Adobe Acrobat, use Microsoft's installer. When installer is running it uses system level permissions which are restricted by the template. Overcoming this obstacle required a change to the domain's group policy.

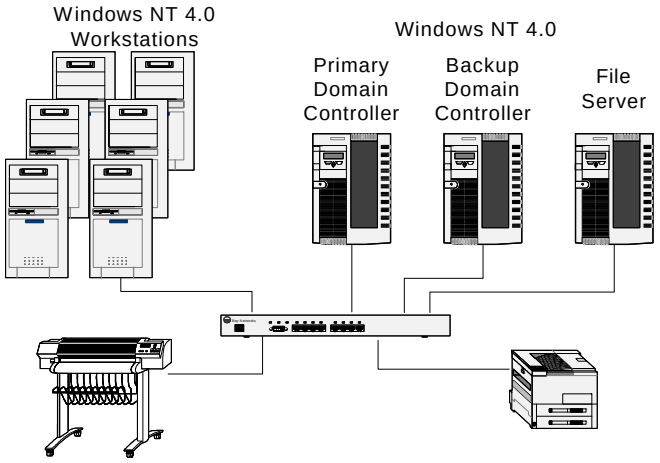
Another problem with the upgrade that is yet to be resolved is forcing user log off after established user hours have expired. Under the old Windows NT 4.0 Domain and workstation configuration, when a users hours had expired the user received a 5 minute warning then were forcibly logged off by the system. Under Windows 2003 Domain the equivalent setting of hours only results in a disconnection of the machine from the server. It does not log the user off from the workstation. I have searched the web for solutions and have found several other administrators in the same situation. Until Microsoft corrects this problem we must routinely check to make sure users are logging off properly and thereby protecting their workstations and access to the network. This is accomplished by reviewing a report generated by the ELM monitoring software.

The upgrade and modification also introduced a new risk. Since the network is now running as a vLAN through the firewall, a device controlled by our third party service provider , any time the firewall is updated or reconfigured there is a chance of an undesired or unintended firewall rule change. If the rule governing the traffic flow is changed or deleted, then the systems running in the secure network may not be able to communicate with the SUS server for updates. Another risk possible via an inappropriate firewall rule modification is that the workstations in the secure network could become directly connected to the internet. At the current time, these risks are mitigated by routinely testing the firewall rules. From one of the servers I open a command prompt window and issue a ping to the secure networks gateway, the SUS server and to an address in each of the other vLANs. I should only see positive results from the gateway and the SUS server. If I get positive results on any of the other test. I immediately contact the firewall administrator and get the problem resolved.

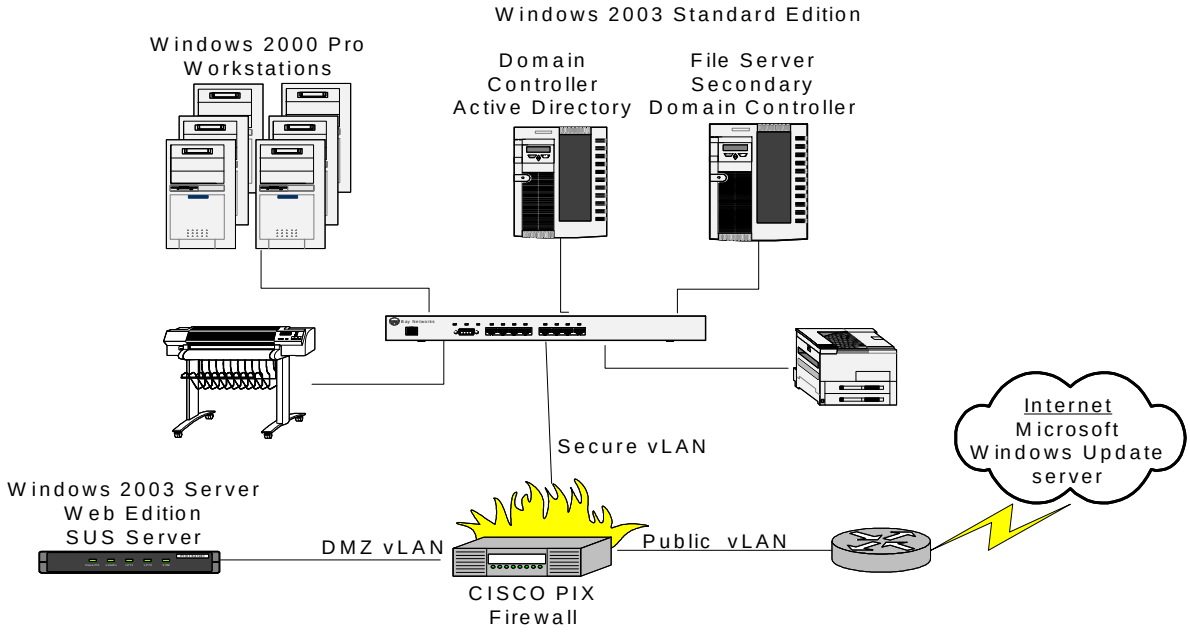
The training that I have received from SANS has played a key role in the decision making process throughout the entire project. It also has reemphasized for me that nothing is static and that maintaining both the security on the network and my knowledge of current security practices and vulnerabilities is critical to good network administration.

Figure 3.0 is a diagram of the network before and after.

The Secure Standalone Network before Upgrade.



The Secure Network After Upgrade.



References:

The SANS Institute. The SANS Institute Windows NT Security Step by Step Version 2.15, The SANS Institute, July 30, 1999.

Microsoft, “Microsoft Update on Windows NT 4.0 Service Pack 7", July 19, 2001
URL: http://www.microsoft.com/ntserver/sp7.asp (15 Oct. 2004)

Microsoft, “DNS requirements for joining an Active Directory domain”
URL:http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_dns_und_ad_join_requirements.mspx (15 Oct. 2004)

Microsoft, “Windows Server 2003 Security Guide”
URL:http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx (15 Oct. 2004)

TNT Software, ELM Enterprise Manager 3.1
URL: http://www.tntsoftware.com/Products/EEM/default.aspx (15 Oct. 2004)

Microsoft, “Deploying Microsoft Software Update Services”,
SUS_Deployguide_sp1.doc. January 19, 2004
URL: http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx (15 Oct. 2004)

Center for Internet Security
http://www.cisecurity.com/

Securing Windows 2000 Professional, Using the Gold Standard Security Template, version 3.0 . SANS Press, 2002.

Securing Windows 2000 Step by Step Version 1.5, SANS Institute, July 1, 2001.