Small Business Network Upgrade

By

Brian Weber

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Engineering Technology

University of Cincinnati
College of Applied Science

May 2007

Small Business Network Upgrade

By

Brian Weber

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Engineering Technology

University of Cincinnati
College of Applied Science

May 2007

Brian Weber	Date
Professor Mark Stockman	Date
Hazem Said, Ph.D. Department Head	Date

Table of Contents

Table of Figures

Abstract

The *Small Business Network Upgrade* is a total network overhaul for Truck Cab MFG and its subsidiaries. This project was aimed at raising the level of efficiency and stability of the network while also allowing for quick and easy administration on a day to day basis. The former network ran on Novell Netware 5.0, which was outdated and beginning to have stability issues, and the company had outgrown the current servers that it resided on. The upgraded network resides on Microsoft Small Business Server 2003 with Exchange, and also features an open source VPN and firewall known as m0n0wall to allow employees to connect from the road. The major tools used in this project include: Microsoft Small Business Server 2003 with Exchange, Windows XP, Macintosh OSX, and m0n0wall. This new system was chosen for its flexibility, easy of use and overall efficiency in both day to day use and overall total cost of ownership.

Network Upgrade for a Small Business

Introduction

There formerly where two Novell 5.0 servers in place at our small family business. Both of these servers where aging, and have begun to exhibit signs of having software based issues. Also, these servers are running a now outdated version of Novell Netware that lacks some of the newer advanced features available in Small Business Server 2003. To compound this, the business is growing and needs more hard drive space for storage of CAD/CAM files as well as information pertaining to orders and inventory tracking.

Beyond the server situation, this small business had a mixed environment of Macintosh 9.0, Macintosh OSX and Windows XP Pro. This environment causes numerous issues as Macintosh 9.0 is no longer supported and also does not network with newer systems as gracefully as Macintosh OS X does. Our business was also looking to update all our software to the newest version of AutoCAD, and Macintosh OS 9.0 does not support this software. Also playing into this is the difficulty of locking down Macintosh based systems via E-Directory or Active Directory.

After a discussion with the company president, it was been determined that a new network solution was needed for our small family business. (1) The proposed solution is to move all users except the company President, Vice President and President of Human Resources to Windows XP Pro computers with AutoCAD 2007, and to move the servers over to Windows Small Business Server 2003 with Exchange. Also, it was brought up that the company wishes to have VPN type connectivity into the network, but wishes to

do it on a somewhat tight budget as they will be spending a large sum of money on Microsoft products.

Options for Network Upgrade

There were three viable options available for the network:

1. Upgrade to Windows Small Business Server 2003 on a new server and desktop machines to XP Pro, implement an Open Source VPN
2. Upgrade to the newest version of Novell Netware on a new server and desktop machines to XP Pro, implement an Open Source VPN
3. Leave the current server system in place, and only upgrade workstations to XP Pro, implement an Open Source VPN

The first option above is the most advanced, all inclusive option available today to a small business type environment. It includes Exchange server with the license, and also allows for up to 75 users before it requires you to move to the full bore version of Windows Server. The second option, while viable, does not include the advanced email options and security features that Small Business Server would. Novell also uses a very different licensing scheme that involves paying every year for a renewal of the licenses, where as Windows is a one time license. The third option is by far the easiest and least effective, as it would only take care of a few of the company's issues. While upgrading the end user machines is necessary, it would not solve the issues of server storage space and it would not bring the server software back into support from their vendors.

Proposal for the Network Upgrade

The proposal was to move the small business network over to Windows Small Business Server 2003 with Exchange. The primary emphasis on this project was networking and systems administration. The primary applications used in this project where Windows Small Business Server 2003 Standard Edition, Exchange Server, Active Directory, Windows XP Pro, Apple OS X and m0n0wall. The abilities of these software components will allow our small business to grow into the future, and will allot us the necessary additional hard drive space, network access, and flexibility that we need. Not only where there be new pieces added to the network, but older portions such as the anti-spam server where integrated with the new system.

The "Small Business Network Upgrade" project encompassed the following as its deliverables:

- Developed multiple servers to cover our multiple sites,
- Developed a backup strategy,
- Roll our network from Novell 5.0 to Small Business Server 2003
- Managed a Active Directory role out,
- Moved our Macintosh OS 9.0 users to Windows XP Pro and accommodated OS X users on the new server,
- Created a new security policy for all users with customized permissions that assume a policy of minimum necessary permission,
- Developed help/training documents,
- Implement an Open Source VPN via m0n0wall.

Design Protocols

This project's main elements are the following:

- Active Directory- This portion of the project will be used by all employees to validate their logins to their PC's and to provide authentication to the file shares.
- Exchange E-mail Server- This element will provide email services for all employees.
- m0n0wall- This application will allow employees to dial into the corporate network and authenticate to Active Directory.

Technical Details

This project will be created using primarily Microsoft based software and server class hardware which includes the following:

Hardware

- New Server
  This newer server is be the basis of the new network and is be running Small Business Server 2003 with Exchange.

- Second Server
  A second server that was already in place will be modified to handle the authentication at the remote site. This server also contains the anti-spam filter.

- Third Server
  A third server was rolled out in conjunction with this project to accommodate a new shop control program called E2.

- Spare PC
  A spare PC was used to run an Open Source VPN and firewall known as m0n0wall.

Software

This project will be using the following software:

- **Windows Server 2003 Small Business Edition**
  Operating system is packaged with Exchange Server.

- **Windows Server 2003**
  Operating system used for second sites server as well as for the E2 shop control program.

- **Microsoft SQL Server**
  SQL Server will be used to run the E2 shop control software rolled out in conjunction with this project.

- **SonicWall MailFrontier**
  This application will server as our E-Mail filter and Anti-Spam measure.

- **Windows XP Pro**
  Operating system used for desktop machines.

- **Apple OS X**
  Operating system used for select desktop machines.

- **m0nowall**
  FreeBSD based Open Source firewall and VPN gateway.

Types of Users

The following are the four main user cases for this project:

- **Administrator**
  -Full Administrator Access to all aspects of network
  -Network Administrator security settings
  -Read/Write access to shared drives
  -Access to Exchange
  -Access to VPN

- **President (Upper Administration)**
  -Read/Write access to shared drives
  -Full Access to sensitive information
  -Power User security settings
  -Access to Exchange
  -Access to VPN

- **Engineer/Office Worker**
  -Read/Write access to shared drives
  -Limited Access to sensitive information
  - Standard User accounts
  -Access to VPN

- **Plant Worker**
  -Read Only Access to shared drives
  -No Access to sensitive information
  -No Access to Exchange
  -No Access to VPN

Overview of Active Directory User Groups

Figure 1 is a visual diagram of the User Groups contained within Active Directory with several sample users distributed within the groups.

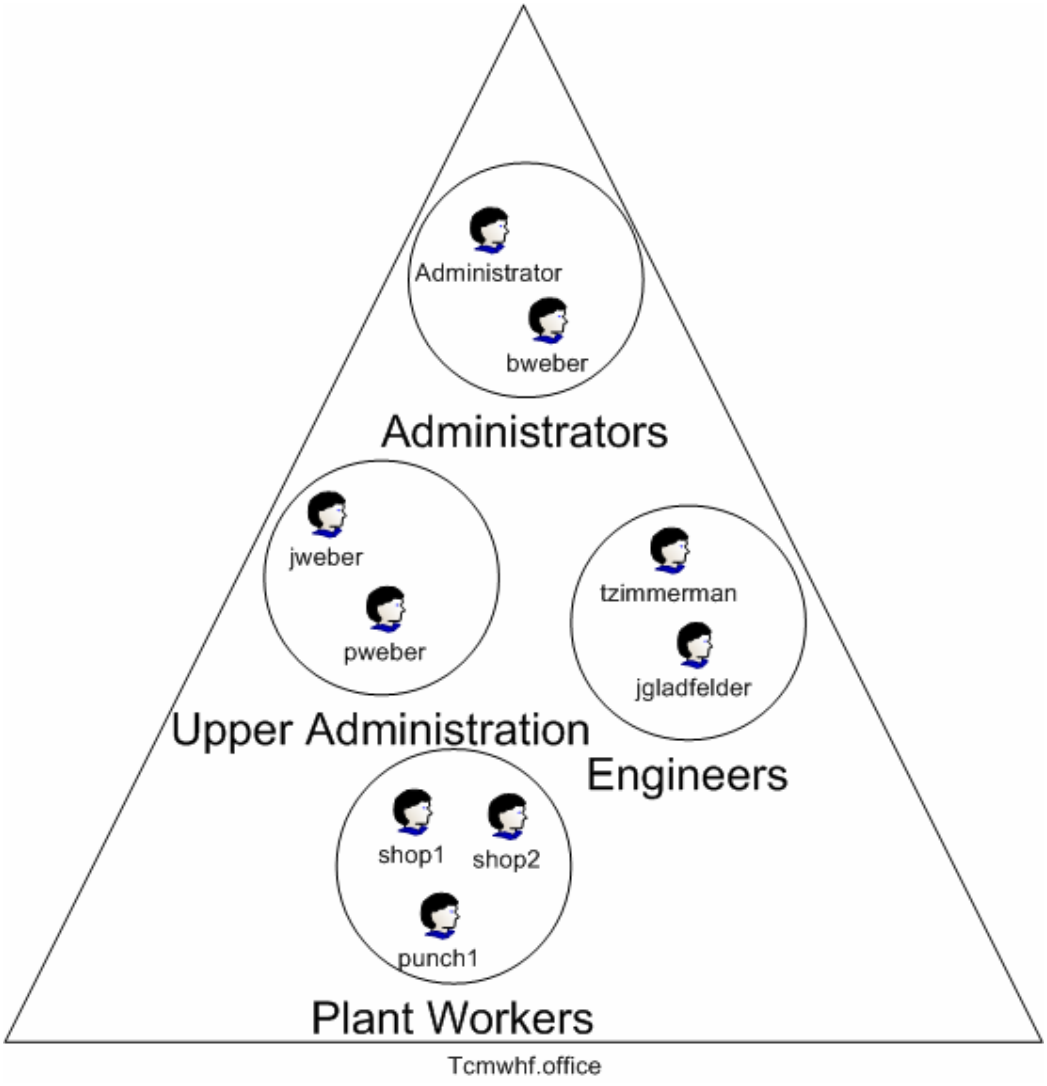

Figure 1 *Active Directory Overview*

Time Line for Project

Figure 2 is the timeline for this project:

ID	Task Name
1	Final Proposal
2	Presentation
3	Research Small Buissness Server
4	Initial Small Buisness Server Load
5	Active Directory Schema Design
6	OpenVPN Server Load
7	Server Testing
8	Server Roll Out
9	User Roll Out
10	Design Complete
11	Design Freeze
12	Create Documentation and Training Materials
13	Write Final Presenation and Report
14	Present Final Presentation
15	Project Complete

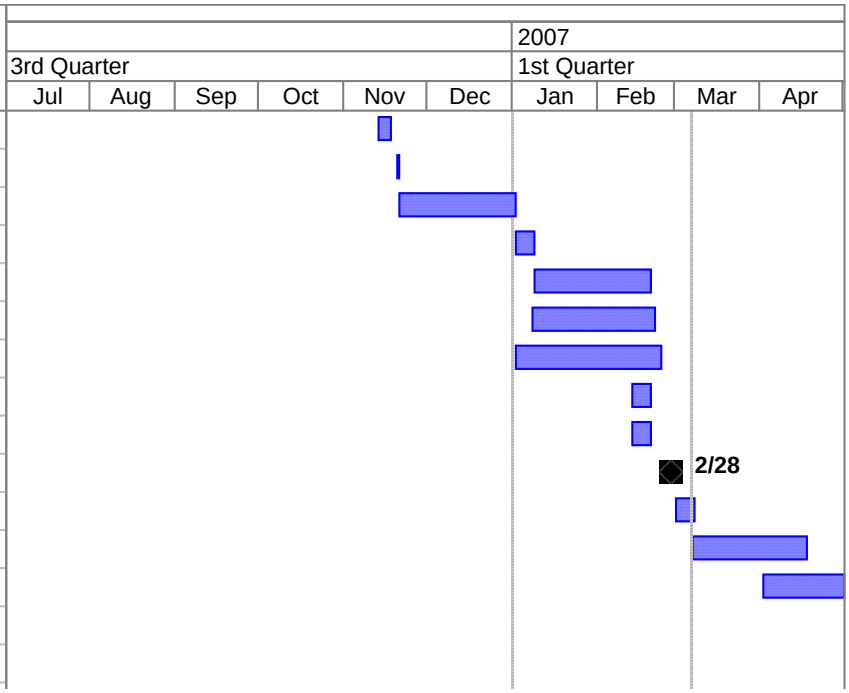

Figure 2 *Project Time Line*

Timeline Milestones

This projects time line lays out the plan for developing, testing and for making the project go live. The development for this project was be done by February 23, 2007, at which point all the major portions of this project where created, and the push to making it go live will begin. The system was completely live once it was rolled out, and only documentation was still necessary to complete the project.

Testing Plan

This project will be throughout its development cycle, and testing will be as comprehensive as possible. Testing will include proving Active Directory is fully functional, that DNS is working properly and being properly pushed out via DHCP and that user profiles are properly being saved to the server.

These modules will all be tested individually at first to prove that they function correctly on their own. After proving each module separately, they will be tested together in a “live” scenario to benchmark and prove the system as a whole.

Project Budget

The budget for this project including the items listed above in the Technical Details section is described below. All items where purchase by the company.

Item	Description	Retail Cost	Cost Incurred
Server	To be purchased by company	$350.00	$350.00
Server	To be purchased by company	$250.00	$250.00
(2) 35gb REV Drive	To be purchased by company	500.00	1000.00
Windows Server 2003 Small Buisness	To be purchased by company	799.00	799.00
Windows Server 2003 Small Buisness Client Access Licenses	To be purchased by company	2800.95	2800.95
Microsoft SQL Server	To be purchased by company	1700.00	1700.00
(5)Microsoft SQL Server Client Access Licenses	To be purchased by company	800.00	800.00
FreeBSD	Open Source Operating System	$0.00	$0.00
m0n0wall	Open Source VPN System	$0.00	$0.00
	Retail Total:	**$7199.95**	**$7199.95**
	My Total:	**$7199.95**	**$7199.95**

Figure 3 *Project Budget*

The project's budget is $7199.95, which is being covered by the company. All of the hardware and software licenses have been purchased and registered with the

company. The FreeBSD based operating system has no cost for the license, as well as the open source VPN solution known as m0n0wall which is free as well.

Project Resources and Logistics

To facilitate this project the resources for it where be provided by the company, and I was also able to work for the company during this time on the project. As for resources Microsoft's TechNet and their dedicated Small Business site will provide the vast majority of documentation necessary to make this project work. Beyond these, I also have additional resources in the staff and faculty of this University.

This project was completed during the course of the Senior Design cycle, and was also my main project at work, as this my family's business. Not only did this project count as my Senior Design Project, but our family business was riding on its success as the company grows.

Proof of Design

This section goes through in detail how deliverables where fulfilled and any challenges encountered where dealt with.

Microsoft Windows Small Business Server 2003 Migration

Microsoft's Small Business Server 2003 is the core of this project, and as so all data from the previous Novell 5.0 servers had to be migrated, cleansed and put back out onto the appropriate shares. While apparently simple in concept, there where issues with the transfer. The previous Novell server had been corrupting files and the metadata on the files was bad which caused issues with applying permissions to the files. In order to

repair the files it was necessary to copy them to a drive formatted as FAT32, which lacks the metadata attributes in the file system, then back over to the appropriately formatted NTFS disks where file permissions could be appropriately set.

User data such as username and passwords were not migrated between systems, as the Novell system was being used for nothing more than file share permissions. It was not handling logon to the local machine, and there was zero data stored to the server about a person's profile. As such, it was quicker and easier to just create new accounts in Active Directory that matched the username of the employees, and create new passwords for everyone.

The company maintains two separate sites, which are several miles apart. Due to this, there was a need to deploy a second server for authentication at the remote site. This server houses the user profiles, and the data shares that the office needs locally, rather than using the T1 connection between the offices for these activities. The secondary domain controller at the remote site also contains a copy of the global catalog, which is a searchable repository for every object with in the domain. This allows for quicker, easier searches for devices on the domain as well as less data moving over the T1.

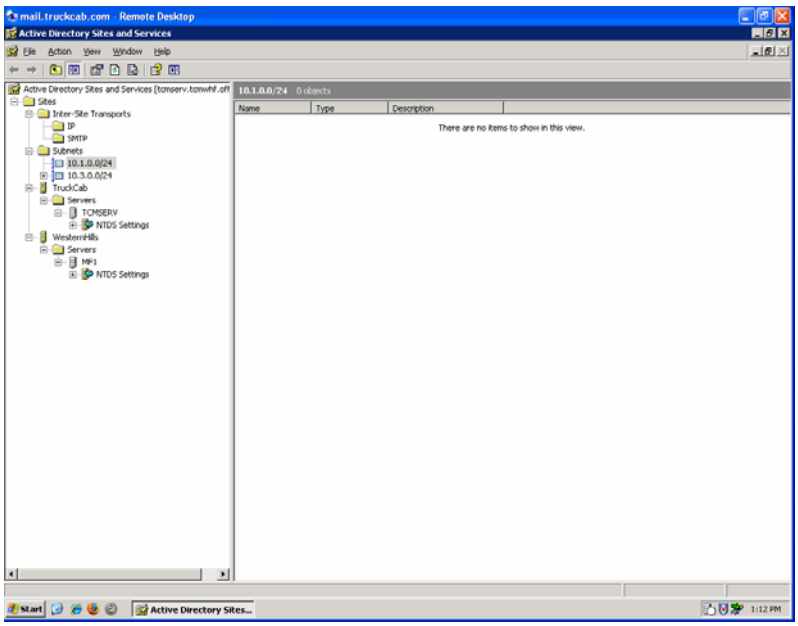

Figure 4 *Active Directory Sites and Services*

Due to the distributed nature of the two offices, the DNS and DHCP setup for the servers is very important as well. DNS is primarily handled by the Small Business Server, which looks at the DNS servers provided by the companies ISP. DHCP is handled per site by each domain controller, with the primary domain controller handling the main site, and the secondary domain controller handling the remote offices DHCP needs. Static routes are set within the network allowing full communication between sites.

Backups are handled on the servers by Brightstore ARCserve, which came bundled with the Iomega Rev drives we use for data backups. Data backups are performed every weeknight, while full system backups including data and operating system are performed every Saturday night. In addition to normal backups, Volume Shadow Copy is also running, which allows access to previous versions of files without running restores from the backups. This is extremely useful if a single file was deleted or somehow was changed incorrectly. Each drive has an identical, dedicated drive for storing Shadow Copies of the data on it.

Active Directory Security Policy and User Groups

Moving from Novell to the new Windows based serve was a huge boost in security and accessibility for the end users. The users themselves went from being local accounts, with local administrator access to being domain users with extremely limited access. This was a significant boost in security as the end user no longer could install applications, make changes to their respective machines and rouge applications (such as spy ware) are much harder to have infect a machine in this environment. Once again, the users where not directly migrated from Novell to Windows. As mentioned above, Novell was acting as nothing more than a file share authentication system and had no data saved per user to the server other than username and password. The previous user groups in Novell where duplicated and then modified to fit into the new system, so that previous file permissions could be appropriately set to match the data access security that the company wished to have.

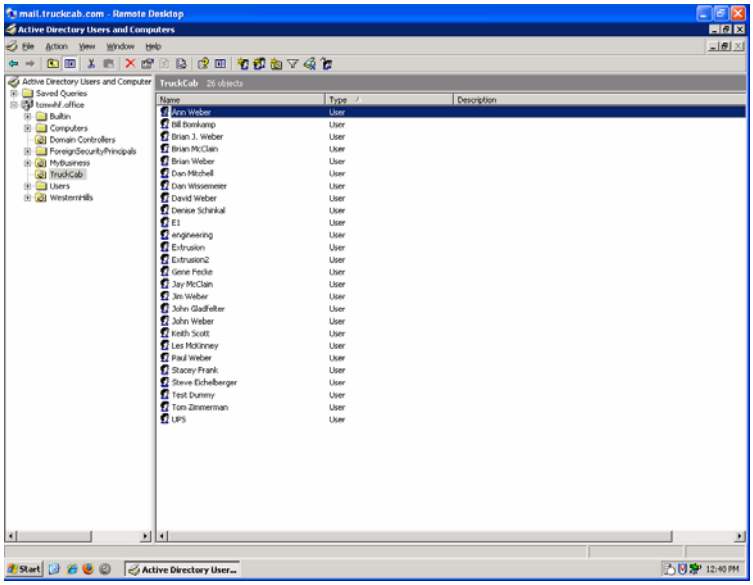

Figure 5 *Active Directory Users and Computers*

User accounts where also significantly improved, both from and end user and administrative standpoint by the use of My Document and Desktop Redirection. As part of the Active Directory Policy, the user's desktop and My Documents folder are redirected to shares on the server. This allows better data security and retention, as even if a desktop machine crashes the data the user thought was stored locally is really being

kept safe on the server. Another equally important benefit of this is the ability for user's data to migrate with them as they move from machine to machine. No longer does each user who sits down at a machine have to have a local account as before, but rather their domain based account works at each station, and their data moves with them. As an administrative benefit, it is now far easier to retrieve data from a users account, even without their password, than it was before. Previously, there where several incidents where this would have proved useful as employees became sick or abruptly left the company.

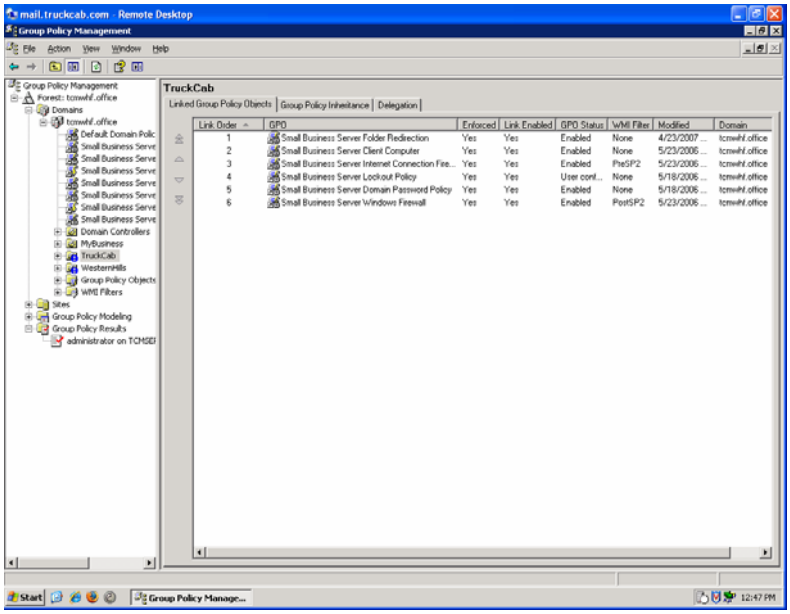

Figure 6 *Active Directory Group Policy*

File share permissions also became much tighter, yet easier to control with Active Directory. The previous user groups in Novell, while quite functional, where never set up to their full potential and left several gaps in security and accessibility.

Windows XP Pro Migration

The migration to Windows XP Pro was two fold, as there where users to migrate from Novell logins to Windows logins, as well as users to migrate from Apple OS 9 to Windows XP Pro.

The migration of users already in Windows from the Novell login, to the Windows login was wholly manual, due to the poor implementation of Novell previously.

The quickest and most effective way was to simply copy all the information in the My Documents folder, all the data on their desktop, and then export their email all into a folder on each user's hard drive. (Previously, each user was only capable of using their machine, so user data was limited to one machine within the network per user) This information was then copied back into their new profiles on the Windows server, which stored all information for the account on the server. From there, email was imported into their Exchange account, and mapped drives where restored.

The users with OS 9 machines where again an ugly process, as much of their information was unable to be copied. Rather, their settings where duplicated as best as possible to a new Windows XP Pro machine, and their data was copied over to the new machine as well. Unfortunately, there was little or no viable way to copy certain parts of their setup. E-mails that where stored in the default Apple application for e-mail where lost, and those that had to be retained were forwarded to a temporary account, then back over to the new accounts.

Due to business constraints, the whole process of converting the company's users to Windows XP Pro was accomplished over a single weekend, and resulted in an extremely minimal downtime for the company. Users where able to log out Friday afternoon from Novell, and then login to the new Windows system by Monday morning.

OS X Integration

The few remaining users (three in total) that remained using Apple's OS X had two major hurdles in their integration into the network. First, they had to be able to see and access the network shares on the new Windows based server system and second they had to be able to connect to Exchange via Entourage. Originally, this was an extremely

difficult task, and was even a major problem for large corporations; resulting in a multi-server configuration with OSX servers and Windows based servers to make this communication possible. However, Microsoft has made this task substantially easier with their release of the Universal Authentication Module or the UAM. The UAM is a tool that installs into the OS X operating system and takes over all authentications with Windows based servers. In addition to the UAM, two select services known as Print Sharing for Macintosh and File Sharing for Macintosh need to be turned on server side, as well as the designation of which shares these services effect.

The setup of Entourage, the Apple E-mail client from Office 2004, is a somewhat tedious exercise, and was extremely hard to find documentation for. Unfortunately, there was no working set of instruction on how to accomplish this. As a result, Entourage's setup with Exchange was forced manually, with zero automation available for it. In the end, the setup was accomplished and now all the functionality of Exchange is available to the Entourage users including calendaring, a global address book, and normal email connectivity.

Exchange Setup

This particular installation of Exchange had to be modified in order to address a unique issue that the company presented. While all essentially one company internally, the company has

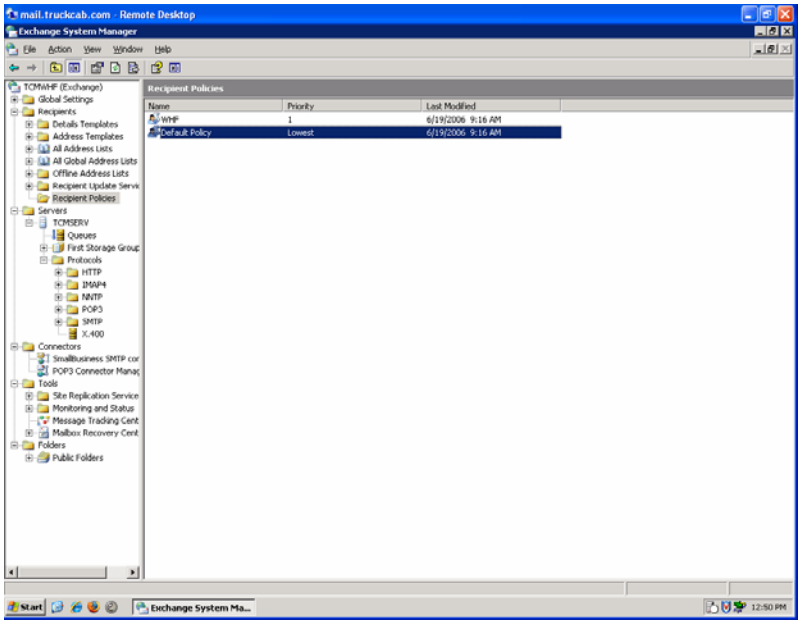

Figure 7 *Exchange Manager*

two names (Truck Cab Manufactures LLC and Western Hills Fabricators LLC respectively) and therefore, two separate email suffixes. While this is typically not an issue with less advanced e-mail services, Exchange was not truly meant to handle such a configuration gracefully, and very little documentation was available specifically for Small Business Server to be used in this setup. In the end, Exchange was correctly configured, with both email suffixes of truckcab.com and westernhillsfab.com being sent and received properly.

m0n0wall

For the VPN connectivity, an open source project known as m0n0wall was chosen. (Please do note, the correct spelling and capitalization is m0n0wall, with the "m" in lower case at all times) This project far exceeds the original call of the project, as it not only gave us VPN connectivity, but also replaced our firewall and gave us more advanced features that allowed for better integration of existing services within our network.

The VPN that m0n0wall uses is known as a Point to Point Tunnel Protocol (PPTP) and is entirely standards based and works with nearly any operating system in existence. The configuration is extremely quick on both the server end and the client

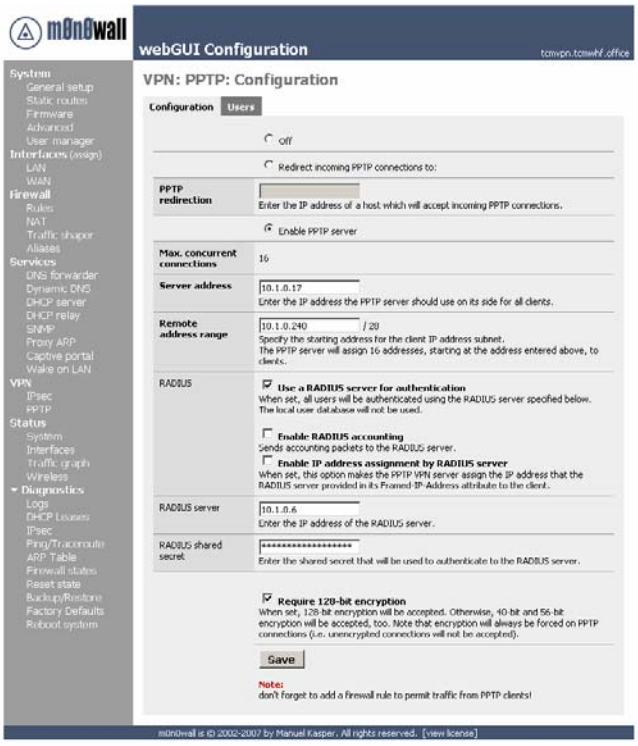

Figure 8 *m0n0wall PPTP Interface*

end, with encryption being mandated on the server side. Any connection that does not adhere to the 128bit encryption being mandated server side is dropped.

For added ease of administration and user convenience authentication via Remote Authentication Dial in User Service (RADIUS) was set up, which the PPTP VPN looks at for authentication. The RADIUS service looks at Active Directory for the username and password, and allows or disallows access to the VPN based on this information. This allows for a single username and password for every person in the company, which means every employee only needs to remember one username and one password.

The firewall built into m0n0wall is relatively complex, and has a great number of features that go above and beyond what this project required. However, these features end up being instrumental in allowing access to several internal resources that the company has, as well as a much tighter set of rules for access into the network. One particular service that the company wished to access was its security camera system from outside the company network. Previously, the firewall system in place did not have the available bandwidth to stream 10 different video feeds at the same time. Now however, due to the traffic shaping and increased processing power of this new firewall the company is able to quickly and easily access the camera system. Another service that can be accessed via the VPN and that was heavily improved by the traffic shaping tool is access to a shop control program known as E2. This allows plant managers to remain in touch with the plant work flow regardless of where they are, so long as they have access to a PC.

Conclusion

The upgrade to this small business network provides updated security, current documentation, fully backed up data and VPN access to the corporate network. These items will allow the company to continue growing, and allow it to be far more efficient and secure in its future. It is plain to see that the former server system was far outdated and there were much more efficient and cost effective solutions available. The upgrade will provide the company a way to safely and effectively continue to grow into the future. This move gave workers the ability to quickly and easily share documents, schedule meetings, and generally be more productive than they used to be. It also gave the administrator greater control over the user environment, and allow for quicker and easier updates and security patches than previously possible in the Novell based environment the company was formerly operating under.

Appendix A

Microsoft Small Business Server 2003 Setup

A1. Domain Name

In order to allow Exchange to receive multiple E-mail suffixes, it is necessary to have your Active Directory domain named differently than any of the email addresses you wish to receive. The easiest way to accomplish this is to use an ".office" domain name, instead of a ".com" or ".net" domain name as your internal Active Directory domain name.

A2. Primary and Secondary Sites

In order for the two sites to communicate and to have Active Directory login and policy apply correctly, two sites had to be created in Active Directory Sites and Services. Below are the instructions on how to set up multiple sites in Active Directory. These instructions start at the point where a secondary domain controller has been brought into Active Directory and now needs to be configured to replicate data between sites.

1) In Active Directory Sites and Services, right click on Sites selecting the option to create a new site
2) Enter the appropriate site name, and select the correct link to the new site. IP is normally the correct type of link for this process. Hit OK once these settings are correct
3) Find the correct server for this site, and move it to the newly created site inside of Sites and Services
4) Right click on the Subnets option, and select New Subnet
5) Create the new subnet, the IP address scheme should match your current network but be a different subnet
6) Assign this new subnet to the appropriate site and select OK once all settings are correct
7) Select Inter-Site Transport/IP and right click on the DEFAULTSITELINK in the menu to the right selecting the Properties option
8) Assign both sites to the link, and choose a replication time that is appropriate (typically once a hour is sufficient)
9) Select OK, Sites and Services should now be properly configured for multiple sites. If more than two sites are needed, simply repeat these steps

A3. DNS/DHCP

DNS and DHCP are two vital services for any network. Setting up a physically disjointed network that contains a bridge to the other site presents some unique issues for DNS and DHCP. In order to provide these services two DHCP servers must be set up and authorized to assign IP address's to machines within the network. DNS can be provided by a single source, but must be exceptionally stable and correctly configured. Below are instructions for both. The instructions for DHCP begin after the DHCP service has been installed onto a server within the second site, and now needs to be set up and authorized to serve addresses.

A3.1 DNS

1) Open the DNS Management tool, and select the DNS server to be configured. This is typically the domain controller.
2) On the Interfaces tab, provide the appropriate IP address that DNS will be running on. This is typically the IP address of the Domain Controller
3) On the Forwarders tab, provide the address of a DNS forwarder. Typically the firewall has the ability to act as a DNS forwarder
4) On the Monitoring tab, select the check boxes for simple query and recursive query then proceeded to test these. If the tests fail, trouble shot as appropriate. Network settings are specific to each environment and change accordingly

A3.2 DHCP

1) Open the DHCP Management tool, and right click on the DHCP service to manage add servers
2) Enter the IP address of the server to be added and authorized and hit OK
3) Right click on the server that was just added, selecting the Authorize option
4) Once authorized, proceed to make any necessary changes to the configuration of the server. Please note that important settings include the Default Gateway and DNS server being served along side the IP address's

A4. Active Directory Policy

As part of the policy for Active Directory, the My Documents and Desktop folders are redirected to a shared drive on the server. The instructions below can be used as a guide to setting this up.

1) Create Folder on an appropriately large drive that you wish to redirect user's information to. One folder for Desktops and one folder for My Documents should be used.

2) To set permissions on the shared network folder where each user's My Documents folder or Desktop is redirected:

   a) Click Start, and then click Windows Explorer.
   b) Right-click the folder to which you want to redirect the user's My Documents folder, and then click Sharing and Security.

   c) On the Sharing tab, choose Share this folder, click Permissions. Add the following users and groups if they are not present, and then assign them Full Control permissions:

      a. Domain Users
      b. Domain Admins
      c. SBS Folder Operators

   d) On the Security tab, click Advanced, and then clear the check box for Allow inheritable permissions from the parent to propagate to this object and all child objects. When prompted for how to assign the permissions, click Remove.

   e) Click Add, add the following users and groups if they are not present, and then assign them Full Control permissions:
      a. Creator Owner
      b. Domain Admins
      c. SBS Folder Operators
      d. SYSTEM

   f) Click Add, and then type Domain Users. In the Permissions Entry for All Users dialog box, click the Apply onto drop down box, click This folder only, and then select the following:
      a. List Folder/Read Data
      b. Read Attributes
      c. Create Folders/Append Data

3) Enter the Group Policy Management tool, and either create a new policy object, or edit the existing “Server Folder Redirection” object.

4) Navigate to User Configuration/Windows Settings/Folder Redirection/My Documents and right click selecting properties to edit. (Select Desktop in place of My Documents for desktop redirection)

5) On the Target tab, Choose the Basic Redirect option, and the for the Root Path browse to the folders previously set up.

6) On the Settings tab, be sure that the following options are set.
7) Uncheck “Grant the user exclusive rights to My Documents” (Or desktop for desktop redirection)
8) Check “Move the contents of My Documents to the new location” (Or desktop for desktop redirection)
9) In the Policy Removal box, select the option to “Redirect the folder back to the local user profile location when policy is removed”

10) The group policy object should be enforced, linked and enabled in the Group Policy Management tool. Apply accordingly to user groups whose data needs to be redirected.

A5. Shadow Copy Setup

Shadow Copy allows for a “live” backup of data to be stored to a separate drive on a regular schedule. This backup copy can be accessed quickly and provides an easy to use alternative to restoring from a standard backup. The instructions below can be used as a guide to setting this up.

1) Right Click on any drive on the machine and select Properties
2) Select the Shadow Copies tab
3) Select the drive to be tracked with Shadow Copy
4) Select enable, then select the settings button
5) Choose the correct storage area for the Shadow Copy to reside on (A empty, dedicated drive is best)
6) Select the option for no size limit
7) Select the Schedule button, and set the appropriate schedule for the copies to be made
8) Hit OK to accept these settings
9) Repeat as necessary

Appendix B

Exchange Setup

B1. Multiple Recipient Policy Setup

Setting up Exchange for the company with multiple E-mail suffixes was highly necessary to provide good business continuity despite the massive internal changes being made. The instructions below detail how to set up Exchange to receive multiple E-mail suffixes. These directions begin after Exchange has been set up and already receive the primary address that was entered during the initial setup.

1) Open the Exchange System Manager and select Domain/Recipients/Recipient Policies
2) Right click New/Recipient Policy to create the new second policy
3) Select both the options for Property Pages and hit OK
4) On the E-Mail Addresses (Policy) tab, create a new SMTP address
5) Enter the correct email suffix and hit OK

It is possible at this point to set the Primary address for the Exchange server. This option alters the default address that ADS accounts are made with.

B2. Adding E-mail addresses to a user via Active Directory Services

1) Open Active Directory Users and Computers, selecting the user account that needs to receive an additional address
2) Right click and select properties of that account, and select the E-Mail Addresses tab
3) Create a new SMTP address, entering the appropriate email address (the address suffix must coincide with a suffix in the recipient policy)

It is possible to alter the primary address at this point, simply be selecting the address and then clicking on the Set as Primary button. This alters the address that E-Mails from this Exchange account appear to originate from. Any address listed for an account is capable of receiving email, so long as it matches up with any of the suffixes entered in the Recipient Policy.

Appendix C

Windows XP Pro Setup

C1. PPTP Client Setup

The PPTP VPN setup within m0n0wall works with the built in Windows VPN connector. Below are the instructions on how to configure this connection.

1) Open Network Connection (Start/Control Panel/ Network Connections) and select the New Connection Wizard and then hit Next
2) Select the second option to Connect to the network at my workplace and then hit Next
3) Select the second option for Virtual Private Network connection, and then hit Next
4) Enter VPN for the name, then hit Next
5) Enter the IP address for the VPN server, and hit Next
6) Select the second option to create this connection for only you, and hit Next
7) Check the box to create a shortcut on your desktop for this connection, and then select Finish
8) Select the Properties button
9) Select the Options tab, and then be sure to check the Dialog options box to include windows logon domain
10) Select the Security tab, and that all options match those shown below. Select OK once you have verified this
11) Enter your username and password (same username and password you use to log into your PC) and fill in the domain. Select Connect to VPN into the target network

Appendix D

m0n0wall Setup

The exact settings of this portion of the project are privileged information due to security risks and therefore general instructions and guidelines on what to look for and use within m0n0wall are provided. The instructions and guide lines below pickup after the installation and initial configuration of m0n0wall. Instructions for which can be found on the projects site. More information on m0n0wall is available at the projects site and detailed information can be had upon request and approval from weberbn@gmail.com.

D1. Firewall Rules

While outside the scope of the project, m0n0wall is a replacement for a large number of small to mid size firewalls. The configuration of the firewall rules allows for a number of services to be hosted with a fair amount of security within the company network. m0n0wall is relatively straight forward in its firewall configuration, and below are some key services to account for on a network running similar services as this one is. Exact settings will vary with each network.

1. Outlook Web Access- Access from port 80 and port 443 to the internal IP
2. x.400 Exchange Protocol- Access from port 103 to the internal IP
3. Remote Desktop- Access from port 3389 to the internal IP

D2. NAT Rules

Network Address Translation (NAT) allows for external IP address and port numbers to be mapped to internal IP address and port numbers. This allows services that run on specific ports access through the firewall. There are two types of NAT, Inbound and 1:1 NAT. Inbound function on a single IP address, and maps ports to internal IP addresses. 1:1 NAT maps one external IP address to one internal IP address with all ports being forwarded on that external address to the internal. Below are some key services to account for on a network running similar services to the one developed for this project. Again, exact setting will depend on the specific network in question.

1. Inbound NAT for port 25 to the internal address of the Exchange server for SMTP

2. Inbound NAT for port 110 to the internal address of the Exchange server for POP3
3. Inbound NAT for port 443 to the internal address of the Exchange server for X.400

D3. Static Routes

Static routes allow two networks to be connected via devices located within each network segment when they are not physically joined together, but rather the only connection between the two is a router type device. In the case of this project, a static route was set up to point all traffic going to the other subnet at the remote site towards a router located within the local network. This router then pushed the traffic over to the other network; much like a default gateway pushes traffic to the internet.

D4. PPTP Setup with RADIUS

The Point to Point Tunnel Protocol (PPTP) VPN configuration within m0n0wall is relatively straight forward, but has to be set up in conjunction with the Remote Authentication Dial in User Service (RADIUS) to provide authentication against the user names and passwords stored in Active Directory. RADIUS authentication is handled by the Internet Authentication Service (IAS), which will need to be installed on the domain controller. Instructions pick up after the initial installation of m0n0wall and IAS has been completed, but neither has been configured yet.

1. Within the Internet Authentication Service control panel, select RADIUS Clients, and create a new client.
2. Enter the friendly name (this can be anything, but it helps to make it actually mean something)
3. Enter the IP address of the client machine (in this case, the IP address of the m0n0wall inside the network)
4. Select Next
5. The Client-Vendor selection should be RADIUS Standard
6. Enter the shared secret, and confirm it again below
7. Hit OK
8. Open Users and Computers in Active Directory, create a new user group known as VPN
9. In the IAS control panel, select Remote Access Policies and create a policy known as VPN. Add the usergroup that was just created to the policy conditions
10. Select the option at the bottom to “Grant remote access permission” and select OK
11. Log into m0n0wall, and select the PPTP configuration page

12. Enable the PPTP server
13. Enter the IP address that the PPTP server should use internally
14. Enter the remote address range that the PPTP server will be assigning
15. Enable RADIUS authentication
16. Enter the IP address for the RADIUS server
17. Enter the shared secret that was used above
18. Force 128-bit encryption to ensure encryption is always being ran
19. Select Save, and then reboot firewall

Appendix C

OS X Setup

Apples OS X is notorious for being difficult to integrate into corporate type networks. However, by using a piece of software from Microsoft known as the Universal Authentication Module connecting to these types of file shares is made much simpler and quicker. Exchange based E-mail for OS X is achieved through Entourage which is part of Microsoft's Office suite for Mac.

C1.1 Entourage Setup

1) From the Tools menu, select Account and click New.
2) Enable the "My Account is on an Exchange Server" checkbox.
3) Click the Configure my account manually button.
4) In the Account ID field, enter the user's logon ID.
5) In the Password field, enter the user's logon password.
6) In the Domain field, enter the domain for the server using either the NetBIOS domain name or the fully-qualified domain name.
7) In the Exchange Server field, enter "https://ServerFQDN/exchange"
8) In the Name field, enter the user's name as it will appear on outgoing messages.
9) In the E-mail address field, enter the user's public reply-to mail address.
10) Click the Directory tab.
11) In the LDAP server field, enter the FQDN of the server.
12) Click the Click here for advanced options button.
13) Enable the "This server requires me to log on" checkbox.
14) Enable the Override default LDAP port checkbox and enter 3268 in the field.
15) Click the Advanced tab.
16) In the Public folder server field, enter "https://ServerFQDN/public"
17) Select the Synchronize all items to server radio button.
18) Enable the DAV service requires secure connection checkbox.
19) Click OK.

C1.2 Universal Authentication Module Setup

1) Enable the “File Server for Macintosh” and the Print Server for Macintosh” services on the server
2) Download and install the Universal Authentication module from Microsoft’s website onto any OS X based machines that require authentication to Windows Server shares. Be sure to use the latest version
3) Open up Computer Management, and browse to Computer Management/System Tools/Shared Folders/Shares. Right click on the Shares folder in the menu on the left, and select New Share
4) Browse to the appropriate folder, and select next
5) If this is a new share, select both check boxes for Microsoft Windows Users and Apple Macintosh Users. If this is a share being modified for Apple users, select the box for Apple Macintosh users only.
6) Select the appropriate share permissions. These setting will vary according to the share
7) Hit close to finish setting up the share

References

1. Burger, Stephen Discussion of Novell Servers 25 October 2006

2. Weber, John Discussion of Company IT Needs 26 October 2006

3. Weber, Jim Discussion of Company Needs 26 October 2006

4. Waddle, Mike Discussion of Company Needs 25 October 2006

5. Raabe, Todd Discussion of Company Needs 27 October 2006

6. Microsoft.com Small Business Server
   2006 Microsoft Corporation
   http://www.microsoft.com/smallbusiness/products/server/detail.mspx

7. Microsoft.com Exchange Server 2003 Product Overview
   2006 Microsoft Corporation
   http://www.microsoft.com/exchange/evaluation/overview/default.mspx

8. Feilner, Markus OpenVPN: Building and Integrating Virtual Private Networks
   Packtpub May 2006

9. "Novell eDirectory vs Microsoft Active Directory"
   2004 Novell Press
   http://www.novell.com/collateral/4621396/4621396.pdf

10. Cisco.com Cisco VPN Client Introduction
    1992-2006 Cisco Systems, Inc
    http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html

11. Micrsoft.com Virtual Private Networks
    2006 Microsoft Corporation
    http://www.microsoft.com/technet/itsolutions/network/vpn/default.mspx

12. Kasper Manuel m0n0wall Handbook
    2005 http://doc.m0n0.ch/handbook/