Global Information Assurance Certification Paper

Network Security for the Small Business:

Hands-On Analysis of a Small Business Firewall / VPN Appliance Implementation

---

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

Submitted By: David H. Hines

September 18th, 2004

Track 1 – SANS Security Essentials and the CISSP 10 Domains
Orlando, FL, April 2004

Table of Contents

Abstract

As competition grows, small businesses are looking for ways to mobilize their work force while maintaining a secure network environment. These businesses face the challenge of securing small and sometimes clumsy networks with no IT professional staff and minimal budgets. Now, with increased media coverage of IT security threats, small businesses are looking for simple but effective network security solutions. In fact, a study by the AMI Group found that while anti-virus software and firewalls are the most common security tools found in small businesses, IDS, VPN, data backup and remote network security management have now captured their attention[1].

This practical will cover the process of mapping out a secure remote access solution for a small business (referred hereto as OrgX for privacy) that needs to mobilize its workforce yet require minimal cost and expertise to maintain. An in-depth look at the challenges involved in choosing the right design and equipment will be described. Last, a full analysis of the successes, trials and tribulations during and after implementation will be performed.

Introduction: Small Businesses and the Need for Network Security

Most small businesses think of network security as protecting themselves from email propagated malware such as viruses, trojans and worms. However, unbeknownst to the small business owner, the security threat is much greater and the challenges difficult to surmount.

Obstacles such as budget, IT expertise, understanding of IT security practices and the need for knowledge of the security threats are some of the challenges a small business must face when developing networks and connecting their staff to the Internet. In addition, business owners can fall into a false sense of security by thinking they are too small to be noticed by interested crackers and script kiddies. Security professionals are all too aware of this mindset and are hoping to entice small business owners to learn about their security needs.

> "Small businesses often feel that because they are small, it is easy for them to hide. They think that there is some kind of safety in numbers. But research says otherwise," explained Geoff Stedman, director of worldwide marketing for Internet security firm SonicWALL[2].

[1] Small Biz Pipeline News, "SMGs Spent 1.8B on Security in 2003, Says Study", URL: http://www.smallbizpipeline.com/news/18200037

[2] Stone, Adam, "Simple Safeguards to Keep Your Small Business Network Secure", URL: http://www.smallbusinesscomputing.com/webmaster/article.php/2107001

This practical focuses on working with OrgX to overcome the common security problems facing small business while utilizing network technology and the Internet to increase workforce productivity. The overall project focused on a well established approach to implementing a truly effective security program regardless of type or scope.

The process consisted of four major areas:

1. Identification of the security need, functional requirements and constraints
2. Evaluation of the proposed infrastructure changes and solutions
3. Implementation of the new security program
4. Post implementation analysis[3]

Each step was followed in order first by identifying the security needs, functionality and constraints (such as budget limitations and limited knowledge base) with respect to OrgX. Then, after a thorough review of several solutions, a decision was made at which time planning and implementation began. The project came to a close and was followed by a complete post implementation review and overall project analysis.

Identifying the Essentials

Identifying the essential security needs, functionality requirements, and constraints is a key step. To ensure that all of the information was used in the proper context, a basic review of the company OrgX as a whole was completed. It was learned that this particular organization functions as a very small private non-profit group of approximately ten individuals (two employees worked remotely by POP email only). The business provides free services for the community thus has no direct income stream. Virtually all revenues are by donation with a small portion being provided by government grants.

By nature of the small non-profit company structure, the budgeting for IT related products is very small and much less so for security specific tools. As well, there is no in-house IT staff and very little understanding of the technology in place by the current staff. Taking into consideration company structure, map of the current network environment and budget constraints, the plan for the security implementation was formulated.

Existing Network Environment

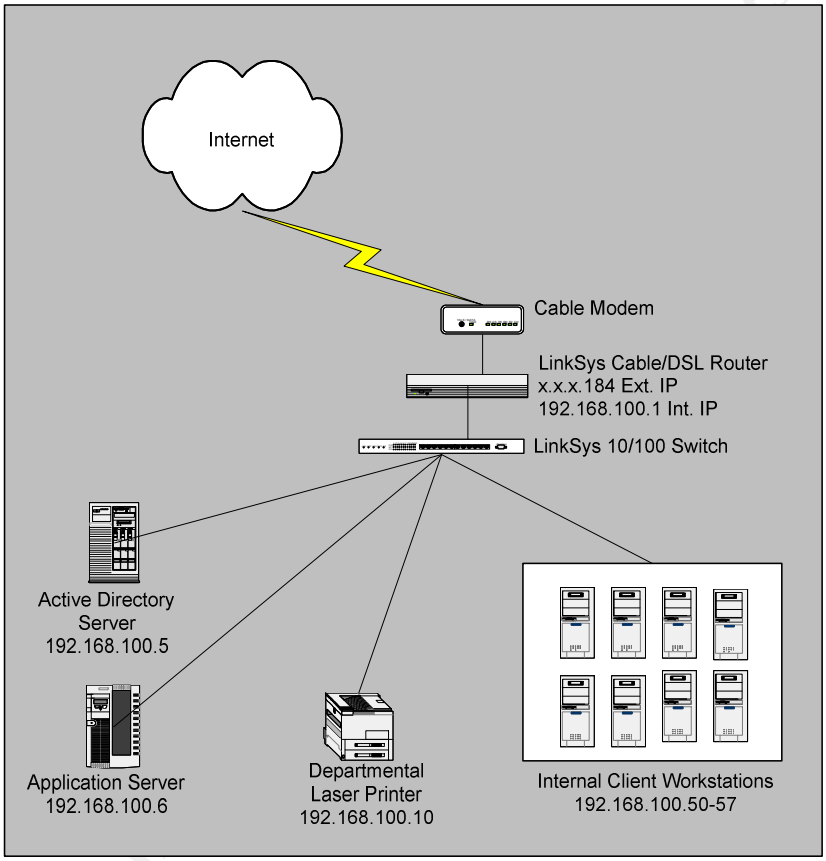
Note – the system names and IP addresses throughout this document have been changed for privacy

[3] Kadel, Lee A., "Designing and Implementing an Effective Information Security Program: Protecting the data assets of Individuals, Small and Large Businesses", URL: http://www.sans.org/rr/papers/26/1398.pdf

The network infrastructure that existed was fairly simple. The whole system was comprised of an internal LAN hosting eight client workstations, an Active Directory server, an Application server and a LinkSys router and switch with a cable broadband connection to the Internet (see figure 1.0). Virtually all network management was outsourced with plans to maintain that model in the future.

Figure 1.0

OrgX Initial Network Infrastructure



The LAN was structured with a network address of 192.168.100.x of which all internal systems were a part. A LinkSys 10/100 switch was the core of the internal LAN with respect to the Ethernet infrastructure. The Active Directory server played the core roles of user authentication, DNS resolution, group policy distribution, data storage and central backup server. The Application server hosted programs such as Symantec Corporate Antivirus 8.0 for client security, a financial software package and a customer relationship management application. These two systems comprised the majority of the computer technology utilized by the organization though there was one essential service hosted externally. Due to the lack of an internal mail server, the employees of OrgX used POP3 mail through their web site hosting provider. The client workstations were fairly new

Windows 2000 Professional systems all with exactly the same hardware and software configurations.

The Internet connection for OrgX was a business level cable broadband service that provided one dynamic IP address with 1.5Mb/s downstream and 384Kb/s upstream bandwidth. The Internet connection was hooked into the company LAN by way of an inexpensive LinkSys Cable/DSL Router. At the time, the router was also providing the DHCP service for automatic addressing of the LAN workstations.

As for the existing security infrastructure, there was only a very basic setup for both the LAN and Internet devices. The client workstations relied exclusively on Symantec Corporate Antivirus 8.0 for local security though advantageously the virus definitions were centrally managed by the Application server to ensure they were always up to date. The only other security measure was the NAT functionality of the router and the fact that the router blocked all incoming traffic from the Internet by default.

Needs Assessment

As the productivity needs of OrgX grew, so did their need for remote accessibility of system data. The need for a remote workforce was a driving point in developing and implementing the soon to be defined security solution. To make the remote access useful, it not only had to be secure to protect company data but it had to be simple to use and had to work with the limitations of the small office network and varying personal computers. It was decided that in order to provide a secure method of remote access, a simple and cost effective VPN solution needed to be implemented. For a workforce of ten, the firewall functionality must support no less than fifteen concurrent outbound connections and a minimum of ten concurrent connections for the VPN functionality. These minimums would reserve plenty of overhead in place for future company growth. Also, since about half of the workforce would be using dial-up connections, the remote access solution needed to provide reasonably responsive access to company programs and data at fairly low bandwidth.

In addition to the remote access need, it was determined that additional security measures shall be put in place to compliment the existing antivirus system. One such security requirement was the addition of a SPI capable firewall that not only could control incoming traffic but allowed the tight control of outbound traffic on a host by host basis. The main task of the firewall is generally to protect the organization from external threats such as intrusion by crackers, but it can also be used to restrict the way in which staff and their computers are able to communicate with the outside world[4]. At the time, all workstations had full

[4] Symantec, "Preventing Unwanted Access from Intruders: IT Security for Small Businesses", URL: http://www.symantec.com/region/reg_eu/euresc/download/Sym_SB_book_ENG_20040907.pdf

outbound access to the Internet and it was determined that the only outbound traffic every employee required was TCP port 110 (POP3 mail) and 25 (SMTP). The outbound access controls would not only prevent wasteful Internet browsing but could potentially prevent the propagation of a virus, worm or trojan to the Internet via restricted ports.

Another security need was antivirus policy enforcement. The remote workforce would be using personal computers to access any VPN implementation. To ensure that these systems were as secure as possible, guaranteeing that an approved and up to date antivirus client and virus definitions were active was essential to maintaining a high level of network security. The policy enforcement would enable the VPN to reject unprotected clients and thus prevent tunneling a virus, worm or trojans directly into the internal LAN. A VPN solution's security functionality is limited by the security of the clients connected.

One very important aspect of the requirements that came up many times was ease of use. Since OrgX had no internal IT staff and would be relying heavily on expensive outsourcing, the solution had to be as simple and reliable as possible. Systems requiring heavy networking experience, scripting or excessive custom configuration were simply not acceptable.

Budget Constraints

Finally, a budget was provided by OrgX that was defined in terms of cost over the first year. Given that OrgX had very little disposable income for technology spending, they chose to budget over the entire year understanding that technologies represent an ongoing cost. Thus after careful review of their finances it was determined that they needed a solution that met the above requirements while staying within a $3000 cap for the first year.

These requirements definitely presented a challenge but one that certainly could be solved.

Making the Right Choice

With the requirements definition and budget constraints in mind, it was time to design a remote access infrastructure. To meet the needs of OrgX, the following key components would be needed:

- Low cost all-in-one VPN/Firewall appliance
- Remote access software and licensing
- Dynamic DNS service
- Antivirus client software for home computers
- Outsourced implementation expertise

With the rise of the network security industry has come a new generation of security appliances aimed at the small business. Many of the new hardware appliances provide VPN, Firewall, IDS and other security functions in an all-in-one device at a fairly low cost. With low cost comes limitations but given the small size of the organization and limited application base it was believed that some limitations were acceptable. Examples of the limitations that low cost all-in-one VPN/Firewall appliances exhibit are limited bandwidth capacities, limited concurrent connections by clients, limited logging / alerting capabilities and limited user customization.

Determining what to purchase for the remote access solutions was not an easy task. There are many different products offering similar functionality. For the purposes of this project we chose to evaluate only four VPN/Firewall appliances from major manufacturers in the security arena. Name brand recognition and market share can be important factors when trying to reduce the number of choices. The field was narrowed to four main VPN/Firewall appliances due to several factors:

- Vendor familiarity
- Low relative cost
- Feature set

In addition, all of the products selected for evaluation were directly targeted to small businesses.

The four VPN/Firewall appliances and base purchase price[5]:

- CheckPoint Safe@Office 225……..$1099.00
- Nokia IP40 Satellite 16……..$699.00
- Symantec Gateway 360R…….$785.00
- SonicWALL SOHO3……..$639.00

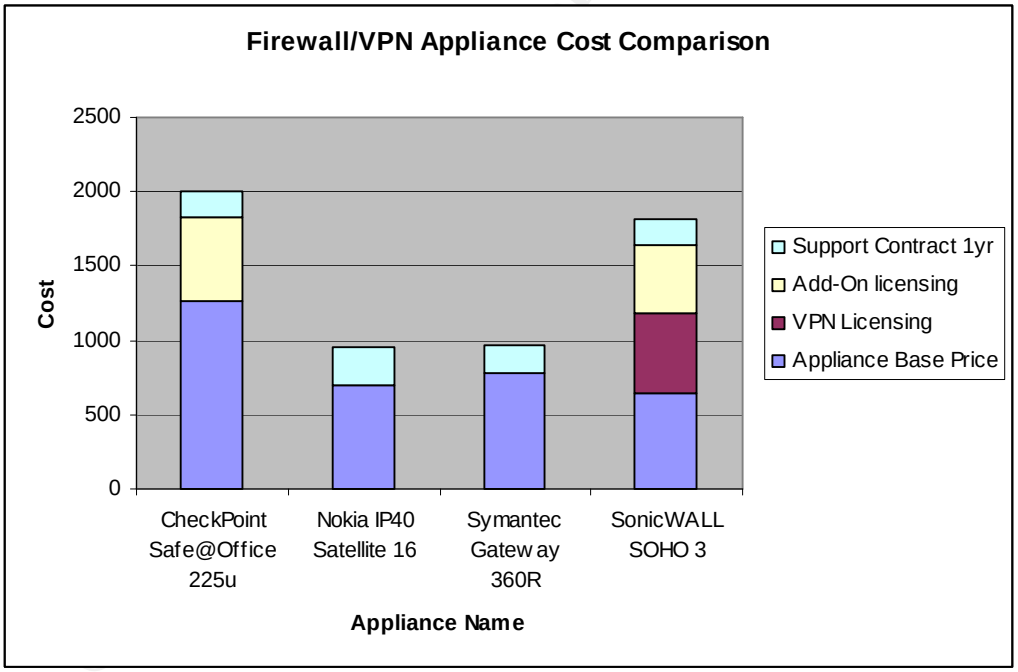
The process of elimination began by removing the Nokia IP40 from consideration. This appliance looked to be a nice and very low cost product. However, the feature set was thin and there were concerns over its compatibility with the broadband cable service. In fact, several calls to the sales department failed to produce any guarantee that this product would work with a dynamic address provided by OrgX's ISP. Knowledgeable sales staff can make the difference between gaining a customer and losing a potential one. Additionally, this product turned out to be focused towards satellite offices of larger enterprises so ease of use was not a primary focus of its engineering.

[5] Pricing obtained May 2004 from http://www.cdw.com, http://www.webfargo.com, http://www.securehq.com and http://www.firewalls.com

The next appliance to be eliminated was the CheckPoint Safe@Office 225. This device was the most expensive and still lacked some of the features OrgX was looking to implement out of the box such as antivirus policy enforcement. However, this product was a very strong player with lots of rich feature and a variety of add-on functionality. Despite the fact that this product would have worked very well, the cost was simply too expensive to qualify as a viable solution. The add-on functionality that would be needed such as virus support would add too much to the bottom line for this particular project. Again, as with the Nokia IP40, it was also fairly difficult to obtain details about the product from sales staff. This appliance was left with unanswered questions about licensing and required product add-ons.

The last appliance to be eliminated was the SonicWall SOHO3 for mainly the same reasons the CheckPoint appliance was rejected. Despite its seemingly low cost, this product required several add-on licenses to meet the requirements for VPN and virus policy enforcement. In fact, the VPN licenses were not built in as with the other products thus making this solution too expensive to implement (see Figure 1.1[6]).

Figure 1.1



The Symantec Gateway 360R was the final option and displayed characteristics that made it a natural fit. First, the Symantec appliance was the second lowest in terms of overall cost in the evaluated group. This was especially evident in that all of the required features and licensing were built right into the appliance. The

[6] Pricing obtained May 2004 from http://www.cdw.com, http://www.webfargo.com, http://www.securehq.com and http://www.firewalls.com

product met all of the feature requirements by providing ten VPN licenses, unlimited concurrent firewall connections, antivirus policy enforcement as well as a host of additional features such as content filtering, intrusion detection and intrusion prevention[7]. An additional benefit was the ability of this appliance to integrate with the existing Symantec Corporate Antivirus application. With the evaluation of the Firewall/VPN appliances complete, the Symantec Gateway 360R was chosen and the rest of the implementation was defined.

To finalize the remote access solution, several other key components were identified and added to the design. For remote client accessibility to the VPN at all times, a dynamic DNS service known as TZO and a TZO sub-domain name were chosen (i.e. OrgX.tzo.com). This service would allow clients to resolve the VPN appliance IP address in the event of a dynamic address change by the ISP. To ensure all remote clients were protected, licenses for Symantec Norton Antivirus 2004 were selected. This particular antivirus client was supported by the 360R for antivirus policy enforcement. To help support the low bandwidth clients, it was decided to utilize Microsoft Terminal Server running in application mode. Not only did this option promise better network response, it was more secure than direct file and application access. This choice would also leverage the existing Windows 2000 Application server with little additional cost for Terminal Server Client Access Licenses.

The next steps were to purchase the necessary equipment, software and licenses then start setting up the remote access system.

Implementation

The following list details the order of installation for the key components:

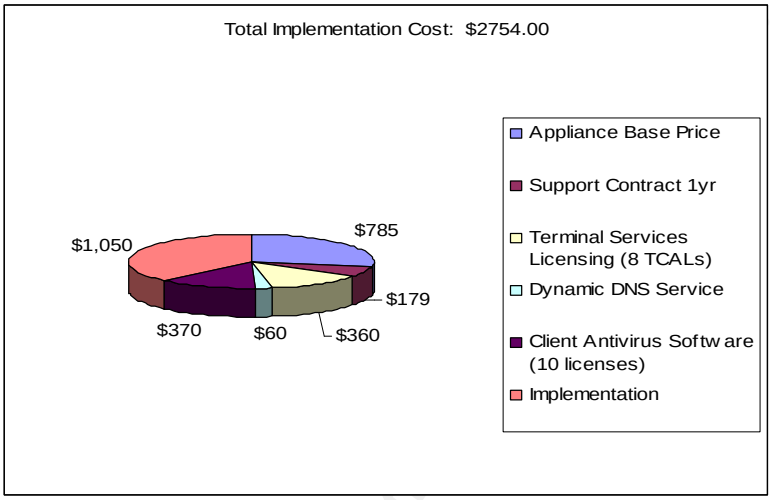
1. Purchase necessary licenses, software and the hardware appliance
2. Install Terminal Services Client Access Licenses (TCALs) and configure Windows Terminal Server
3. Configure roaming profiles for Windows clients
4. Configure TZO dynamic domain name service
5. Install the Symantec Gateway 360R
6. Configure VPN client software and antivirus software on remote clients
7. Testing the functionality
8. Create user documentation and provide training

Purchasing

[7] Symantec, "Symantec Gateway Security 300, 320, 360R Fact Sheet", URL: http://www.symantec.com/smallbiz/gtw/pdf/SGS_300_factsht.pdf

The first order of business was to order the necessary software, equipment and implementation outsourcing. All equipment was purchased through CDW.com due to an existing vendor relationship. Outsourcing was provided by the author of this practical at the rate of $35.00 per hour for a 30 hour contract. The TZO dynamic DNS service and sub-domain name were provided by TZO.com at a total cost of $60.00 (see Figure 1.2 for a cost breakdown).

Figure 1.2



Windows and Terminal Services Configuration

To start, the Windows Terminal Services was installed on the existing Application Server and the Terminal Services Licensing program was installed on the Domain Controller. Per Microsoft documentation, the Terminal Services system could be installed and used by users at no additional cost as long as the connecting client was using the Windows 2000 Pro or Windows XP Pro operating system[8]. For this implementation there were eight remote access clients using Windows XP Home so eight Terminal Services Client Access License (TCALs) tokens were purchased and installed on the Licensing server.

To facilitate easy user transition to the remote access system, roaming profiles were configured for all of the clients. This step allowed the remote access clients to see an emulated desktop environment that closely resembled their personal desktops. In addition, the security policy of the Terminal Server was locked down to protect the server from tampering and user error.

Dynamic DNS

[8] Microsoft Corporation, "Microsoft Windows 2000 Terminal Services – Licensing Technology White Paper", URL: http://download.microsoft.com/download/2/6/e/26ed8bd1-6ab3-49c6-9441-001c794ab79a/tslicensing.doc

The TZO dynamic DNS service was configured on the Windows 2000 Domain controller by installing the TZO software client and entering the activation key. The system was set up to update the DNS name OrgX.tzo.com at an interval of once per day. This service can be invaluable for businesses using cable or DSL Internet access where DHCP is used to assign addresses and there is a need to consistently access the company network remotely.

Installing the Symantec Gateway 360R

The most configuration intensive portion of the implementation was to set up the Symantec Gateway 360R and the remote access clients. The 360R was configured in the following order:

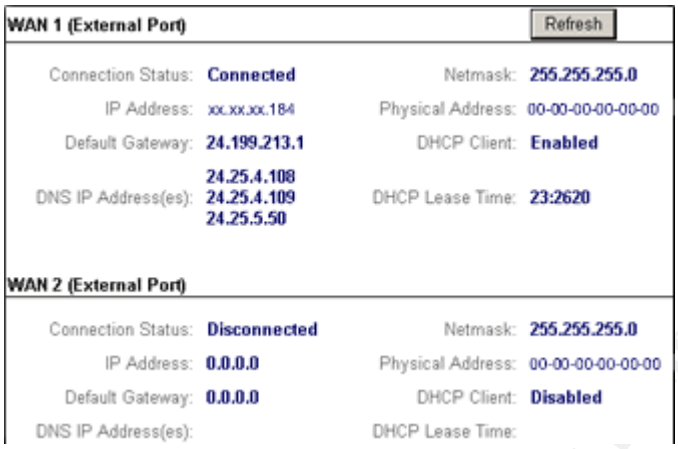
- LAN / WAN networking
- Firewall
- VPN
- Antivirus policy enforcement

The existing LinkSys router was removed from the network environment and the Symantec Gateway 360R was installed in its place. The cable modem connection was made to WAN port 1 (there are two WAN ports for failover and load balancing) of the 360R and a crossover cable was used for connecting the LAN port to the internal LinkSys 10/100 switch.

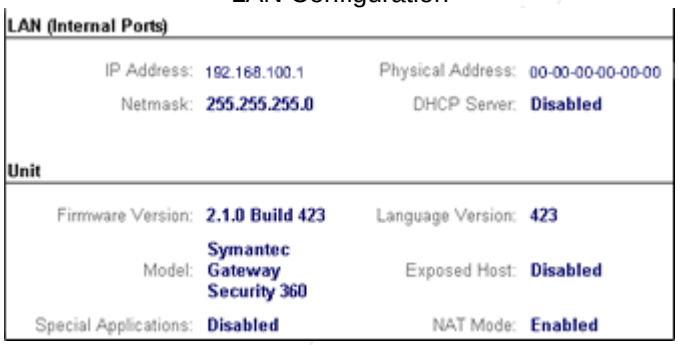
Configuration of the device began by connecting to the Symantec Gateway Management Interface[9] (SGMI) using the Internet Explorer browser. A configuration wizard begins the first time a connection is made to the management interface yet this wizard was exited since more advanced configuration of the device would be required. Before any other network configuration was performed, a strong 16 character password was configured to secure the 360R. The WAN and LAN configurations were configured as follows:

WAN Configuration

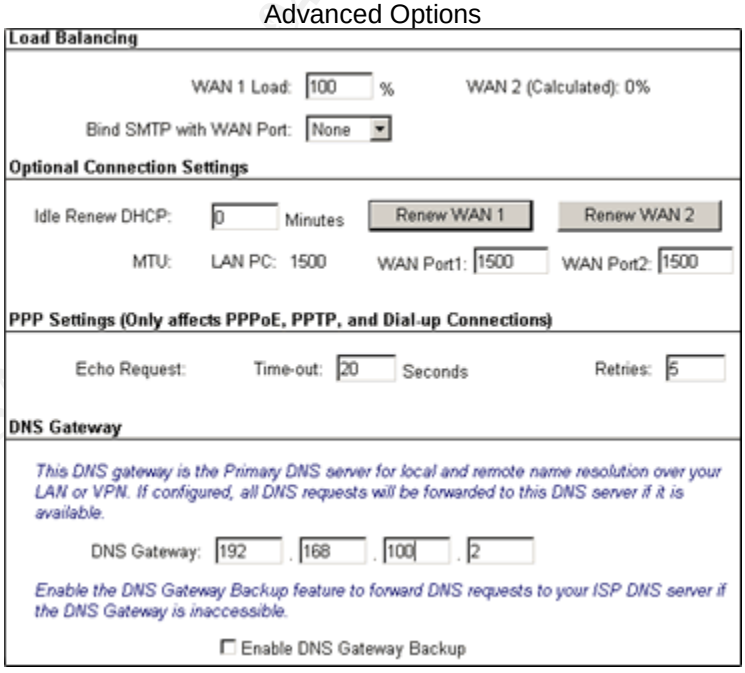
[9] Symantec, "Symantec Gateway Security 300 Series Administrators Guide", URL: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_gateway_security/300-Series_2.0/manuals/SGS300_ADM.pdf



LAN Configuration



Advanced Options



Once the networking parameters and services were configured, the firewall setup began. It should be noted that for the purposes of OrgX, the inbound access

rules were not needed so all inbound traffic was dropped by default. Each LAN system was defined in the firewall as a "Computer" object by system hostname and MAC address. Once all computer objects had been defined, three "Computer Groups" were populated.

Computer Groups:

- **Everyone Group** – Contained all computer objects
- **Computer Group 1** – Contained the Application Server, Domain Controller and five client computer objects
- **Computer Group 2** – Contained the Domain Controller computer object

Finally, four outbound access rules were created and defined in terms of TCP and UDP ports available for outbound Internet traffic.

Outbound Access Rules:

- **SMTPAccess** - contained the "Everyone" group and provided outbound access using TCP port 25
- **POP3Access** – contained the "Everyone" group and provided outbound access using TCP port 110
- **WebAccess** – contained "Computer Group 1" and provided outbound access using TCP port 80 and 443
- **DNSAccess** – contained "Computer Group 2" object and provided outbound traffic using UDP port 53

These few simple access rules allowed OrgX to tightly control the type of network traffic flowing to and from their network and the Internet.

Next, the VPN functionality was enabled and configured for usage by the remote clients. The Symantec Gateway 360R supports several types of VPN connections including static, dynamic, gateway-to-gateway and client-to-gateway VPNs. Interestingly, the 360R supports "dynamic" users with which the authentication takes place by way of an available RADIUS server though this functionality was not enabled. The Symantec Gateway Security 300 Series Administrators Guide recommends that the VPN functionality be configured by way of a seven step process[10].

1. Configure a VPN policy (Phase 2 IKE negotiation)
2. Select a VPN policy that applies to the tunnel
3. Identify remote users and associated VPN Group
4. Enable a client tunnel for the selected VPN Group
5. Configure the VPN network parameters
6. Configure RADIUS authentication for dynamic users (optional)
7. Enable antivirus policy enforcement (optional)

[10] Symantec, "Symantec Gateway Security 300 Series Administrators Guide", URL: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_gateway_security/300-Series_2.0/manuals/SGS300_ADM.pdf

The VPN policy allows for the configuration of standard, reusable policies consisting of data privacy (encryption strength), data integrity and compression algorithms for Phase 2 negotiations. The appliance comes with four default VPN policies but a custom policy was defined to take advantage of the highest level of security the 360R had to offer.

VPN Policy Configuration

Name:	ike_AES_strong
Encryption Method:	ESP AES_VS SHA1
SA Lifetime:	480 minutes
Data Volume Limit:	2100000 Kbytes
Inactivity Timeout:	60 minutes
Perfect Forward Security (PFS):	5
DH Group:	Enabled

Once the VPN policy was defined, the global settings for the VPN clients were configured to use the ike_AES_strong policy for Phase 2 negotiations. Identifying remote users was performed by creating client IDs and 22 character alphanumeric pre-shared keys for each OrgX remote user. During user creation, one of four predefined VPN groups was selected. Due to the small number of remote users at OrgX, only VPN Group 1 was used.

Example User Configuration

Client ID:	OrgXUser1
Pre-shared Key:	a1zb9xmd50nq1je48c2oh7
VPN Group:	VPN Group 1
Enabled:	Yes

The parameter for enabling antivirus policy enforcement was selected for VPN Group 1. Enabling antivirus policy enforcement would ensure that any VPN connected client had both an active AV program and the most recent virus definitions.

To utilize the antivirus policy enforcement, several parameters had to first be configured on the 360R appliance. The AV policy master parameter was set to the query Symantec Corp. Antivirus Server for the latest virus definitions every 60 minutes to create a virus definition reference. In turn, the 360R would query any connected VPN clients every 480 minutes to determine if an antivirus client was active and had the current or newer antivirus definitions. If either no AV client was found or the virus definitions were not up to date, then the remote user would be prevented from connecting to the VPN.

Installing and Configuring the Remote Access Software

Once the Symantec Gateway 360R was in place and all parameters had been defined, it was time to configure the VPN, antivirus and remote access software on the remote users' computers. The following software was installed on each of the computer systems to be used for remote access:

- Symantec VPN Client 8.0
- Norton Antivirus 2004
- Microsoft Remote Access Software

To make the installation of this software as efficient as possible, each user was provided a personalized CD-ROM that included the necessary software, an OrgX VPN User Guide and a Personal Information document. The OrgX VPN user guide contained a detailed step by step process for installing, configuring and using the software required to utilize the OrgX remote access system. The Personal Information document contained the client ID and pre-shared key that would be needed for VPN negotiation and authentication. It was very clearly stressed to the remote users that the security of their CD was imperative to maintaining secure corporate data. Hands-on user training was also provided to minimize errors and to make sure that the OrgX staff understood how to use and manage the technologies put in place.

Testing the Implementation

Changes to any network environment must be thoroughly tested to verify the critical functionality is available and that the newly implemented functions are working correctly. Since this project had a considerable impact on the network infrastructure of OrgX, unit testing was conducted throughout the project. In addition to the constant unit testing, a quality assurance plan was created that consisted of several key test cases. These test cases were developed to guarantee that the new functionality was performing as expected.

Test Cases:

1. Regression
2. Network Configuration
3. Firewall rule set
4. VPN functionality
5. Remote access connection
6. Antivirus policy enforcement

The following tables provide a list of the tests that were performed for each of the test cases. Each test was described in the table and a result was recorded as either pass or fail. If necessary, details of the test were also provided to describe the reason for a pass or fail result and to elaborate on the details of the test performed.

Regression

Test Performed	Result	Details
Logon to the OrgX Active Directory using an internal LAN client workstation.	**Pass**	Due to the small number of LAN workstations, this test was performed once on all systems. A low authority account was created on the Active Directory server for testing purposes.
Verify drive mappings are present for each user.	**Pass**	This test ensured that the logon script was functioning properly.
Connect to internally distributed applications such as the financial software and customer relationship manager.	**Pass**	A sample of three workstations was used to verify the financial software and CRM software were functioning properly.

Network Configuration

Test Performed	Result	Details
Symantec 360R has obtained a public DHCP address from the ISP	**Pass**	The Symantec SGMI was used to view the status of WAN port 1.
Verify the LAN IP address of 360R is 192.168.100.1	**Pass**	The Symantec SGMI was used to view the status of LAN network configuration.

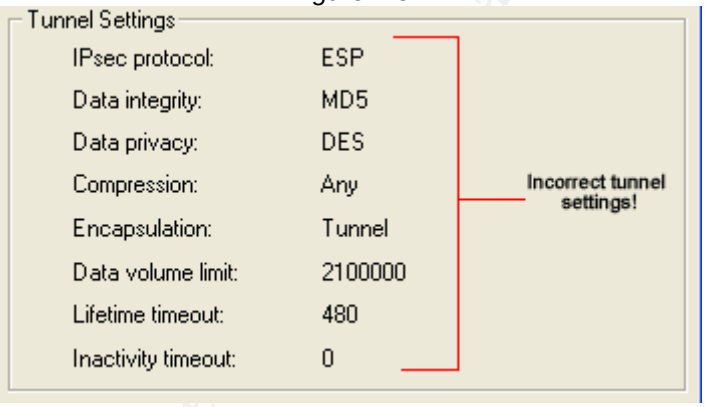
Firewall Rule Set

Test Performed	Result	Details
Clients assigned the WebAccess outbound access rule are able to view websites on the Internet	**Pass**	Three websites were used to test this functionality, **www.symantec.com**, **www.sans.org** and **www.cnn.com**.
Clients not assigned the WebAccess outbound access rule are not able to view websites on the Internet	**Pass**	Three websites were used to test this functionality, **www.symantec.com**, **www.sans.org** and **www.cnn.com**.
Verify the Domain controller is assigned the DNSAccess outbound access rule and verify DNS resolution to the Internet	**Pass**	The access verification was done by using the SGMI console and looking to see what access rules had been assigned. DNS resolution was confirmed by pinging a host on an external domain (www.snoopy.com).
Verify all clients are able to connect to their POP3 mail server and SMTP mail server	**Pass**	Due to the small number of LAN workstations, this test was performed once on all systems. A generic email account was setup on the POP3 mail server for testing purposes. The SMTP service was tested by sending mail to an external Hotmail email account and verifying receipt.
Check Internet access over un-allowed ports to verify the connections are blocked	**Pass**	To test this functionality, attempts were made to connect to an Internet FTP server (ftp.adhtech.com) over TCP port 21 and to an Internet available time server (terrapin.csc.ncsu.edu) over UDP port 123. The testing was performed on a small sample of three LAN clients for the previous services.

VPN Functionality

Test Performed	Result	Details
Client connection to VPN over dial-up Internet connection	**Pass**	A laptop was used to dial-up to the Internet using the Earthlink ISP.
Client connection to VPN over broadband Internet connection	**Pass**	A remote system on the Road Runner cable network was used to connect to the VPN.
Verify IPSEC NAT transversal is functioning properly	**Pass**	The remote system on the Road Runner cable network was placed behind a NAT enabled cable/DSL router.
Verify the custom VPN policy is applied properly to the connected tunnel	**Fail**	The VPN connection was established successfully but when the tunnel status is viewed the wrong VPN policy is active (see page 14 for correct VPN policy). This was an known bug that was being addressed by Symantec support (see Figure 1.3). A live update security patch fixed the issue.

Figure 1.3



Remote Access Connection

Test Performed	Result	Details
Verify that a connection can be made to the Terminal Server from a remote computer	**Pass**	The remote laptop used in VPN testing was again used to connect to the Terminal Server. A test user with standard authority was used to logon.
Confirm that the user's roaming profile is functioning properly	**Pass**	A roaming profile was configured for the test user.
Establish connections to the internal LAN applications such as financial software and customer relationship manager	**Pass**	The test user was provided authority to the financial and CRM software. Only the connection to the software was performed, no other tasks were attempted.
Confirm that the Terminal Server security policy prevents user tampering or accidental shutdown of the server	**Pass**	Having logged on using the test user, attempts were made to change files in the system directory, to change the system time, install Bejeweled game from MSN Game Zone and to shut down the system.

Antivirus Policy Enforcement

Test Performed	Result	Details
Verify that all users are required to use AV policy enforcement	**Pass**	The Symantec SGMI was used to view the status of all users with respect to AV policy enforcement. All users showed "enabled"
Confirm that systems with out of date AV definitions are denied access to VPN	**Pass**	A laptop was configured with a new install of Norton Antivirus 2004 and the definitions were not updated. When attempting to connect to the VPN, the connection is rejected due to antivirus definitions not matching the AV server definition level.

The testing of the implementation went very well except for a small bug in the VPN policy settings. When connecting to the VPN, the tunnel settings would always default to MD5 DES parameters regardless of the settings on the Symantec 360R appliance. After consulting with the Symantec support team, a Live Update patch was applied to the system and the VPN policy bug was resolved.

Post Implementation Analysis

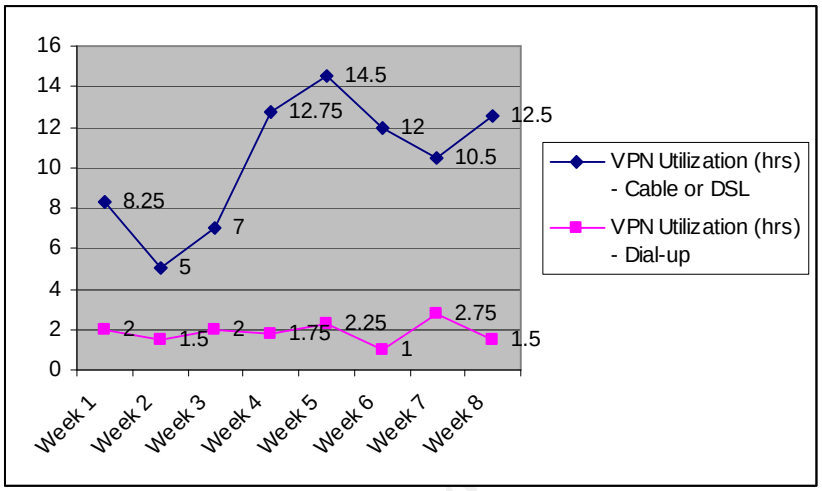
Analysis of the implementation was critical to determining if the project was a success, had ongoing issues or is having a negative impact on the company. The purpose of the project was twofold, to increase the productivity of OrgX by enabling a mobile workforce and to increase the security of OrgX through additional technical security measures. For this practical, the analysis focuses on several key points for determining the success of the implementation. An analysis of the remote access system was used to determine the value of any increase in workforce productivity. A review of the implementation timeframe and any implementation impact on the daily business functions was also performed. Last, a review of the security measures put in place would be used to determine if the security of OrgX had actually improved.

Workforce Productivity

To set the stage for evaluating any increase in workforce productivity, it was decided that an average hourly rate should be established for any time spent utilizing the remote access system. A median rate or $15.00 per hour was established by looking at all of the employee salaries within OrgX. This rate would help in determining the ROI or return on investment for OrgX with respect to the remote access implementation. Next, each employee was asked to keep track of all of their time spent utilizing the remote access system over eight weeks. As seen in Figure 1.4, there was a marked increase in the remote access utilization after the second week. It should be noted that the majority of the utilization hours were accumulated by the five remote users that possess a cable or DSL broadband connection. The Dial-up users experienced acceptable

response but were not inclined to remain on the system any longer than necessary. The cable and DSL users found that the connection was so responsive that all of their tasks, including reading email, could be performed with little delay. In fact, several of the users commented on how it was like sitting right at their internal LAN workstation.

Figure 1.4



Over the eight week period it was found that a total of 97 hours was spent utilizing the remote access system. In combination with the median hourly rate of $15.00, the estimated ROI for this implementation was $1459.00 over the first eight weeks. This was an outstanding result in that over an eight week period the system had made up for about a half of its initial cost. Looking at this trend over the course of a 52 week period, OrgX could potentially increase their productivity by an estimated net value of $6729.00 (this value takes into account the cost of the implementation).

Implementation Impact

Since the remote access system created considerable changes to the OrgX network infrastructure, it was determined that a look at the impact of the implementation was necessary. This analysis would evaluate the installation and find if it had any negative impact on the daily functions of the OrgX workforce.

Fortunately, most of the implementation was done during off hours so that the workforce would not be dealing with critical system outages thus limiting their productivity. However, there was one caveat that did significantly impact the business operations of OrgX. After about twelve weeks of usage, the Symantec 360R appliance began to lock up every three to four days. The temporary resolution was to have a staff member restart the 360R when a lock up occurred. This still required about 15 minutes of productivity downtime per incident while the workforce waited for Internet functionality (such as POP3 and SMTP mail) to

return. Several calls were made to Symantec support and a beta firmware (version 5.26) was made available for installation. After performing the upgrade to the 360R appliance, the lock up issue appears resolved.

It should be noted that the Symantec support center was not very responsive and thus delayed the final implementation by approximately 4 weeks. This delay did not directly impact the current applications and network functionality but it did delay the use of the remote access system considerably. Overall, the implementation went very smoothly and the employees of OrgX were pleased that there was little impact on their business functions while the process was taking place.

Security Analysis

Finally, the implementation was analyzed with respect to its impact on the security of OrgX and its corporate data. Given the very limited security infrastructure that OrgX started with, a client antivirus system and NAT, it was very clear that this solution did provide them with an enhanced security environment. With the addition of a highly secure VPN, effective SPI firewall and antivirus policy enforcement for remote users, network and data security was greatly improved within the OrgX network.

However, as with any project that allows remote access to corporate data, there are exceptions to these improvements in security. One such exception is the limited client security on the remote user's workstation. Antivirus software is a good start to providing client security though it does nothing about the port scanning, vulnerability scanning and system intrusion that is all too common among systems attached to the Internet. As stated earlier in this document, a security system is only as secure as its weakest link and in this case the remote client workstation is a considerably weak link.

To mitigate the future risk to corporate security by remote clients, a project to resolve this issue was discussed with OrgX. It was determined that a future project would address the remote client security by adding a local firewall to each remote client with restrictive port and application access to and from the Internet. At the time of this analysis no date had been set to implement the remote client firewalls.

Conclusion

The need for corporate security and increased productivity has grown for small and large businesses alike. As discussed in this practical, the small business OrgX recognized these growing priorities and worked to develop an effective system to improve both security and productivity. The challenges facing small companies can sometimes be overwhelming to address but with the proper planning, solution evaluation, and implementation process, a well scaled system

can be put in place. It has been revealed that companies, such as OrgX, that have severely limited technology related budgets can implement relatively simple and cost effective systems to address their functional and security needs.

Overall, this practical demonstrated that the remote access and security implementation for OrgX was very successful. With new security enhancements to protect their corporate data and a now mobile workforce, OrgX is well positioned to experience increased productivity with minimized risk of business interruptions due to malicious network activity. Additionally, this project has been an invaluable learning experience for OrgX with respect to how this company approaches future enhancements to their security and technology infrastructure.

References

Small Biz Pipeline News. "SMGs Spent 1.8B on Security in 2003, Says Study". 24 February 2004. URL: http://www.smallbizpipeline.com/news/18200037

Stone, Adam. "Simple Safeguards to Keep Your Small Business Network Secure". 10 March 2003. URL: http://www.smallbusinesscomputing.com/webmaster/article.php/2107001

Kadel, Lee A.. "Designing and Implementing an Effective Information Security Program: Protecting the data assets of Individuals, Small and Large Businesses". 24 March 2004. URL: http://www.sans.org/rr/papers/26/1398.pdf

Symantec Corporation. "Preventing Unwanted Access from Intruders: IT Security for Small Businesses". 7 September 2004. URL: http://www.symantec.com/region/reg_eu/euresc/download/Sym_SB_book_ENG_20040907.pdf

Symantec Corporation. "Symantec Gateway Security 300, 320, 360R Fact Sheet". February 2004. URL: http://www.symantec.com/smallbiz/gtw/pdf/SGS_300_factsht.pdf

Microsoft Corporation. "Microsoft Windows 2000 Terminal Services – Licensing Technology White Paper". 2004. URL: http://download.microsoft.com/download/2/6/e/26ed8bd1-6ab3-49c6-9441-001c794ab79a/tslicensing.doc

Symantec Corporation. "Symantec Gateway Security 300 Series Administrators Guide". 11 February 2004. URL: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_gateway_security/300-Series_2.0/manuals/SGS300_ADM.pdf

SonicWall, Inc. "SOHO3 Product Data Sheet". URL: http://www.sonicwall.com/products/soho3.html

Nokia Corporation. "Nokia IP Security Solutions – IP40". 2003. URL: http://www.nokia.com/BaseProject/Sites/NOKIA_MAIN_18022/CDA/Categories/Business/LargeBusiness/NetworkIntegrity/IPSecurityPlatforms/DistributedEnterprises/_Content/_Static_Files/sec_ip40_datasheet.pdf

Check Point Software Technologies, Ltd. "Safe@Office for Small Business". 19 July 2004. URL: http://www.checkpoint.com/products/downloads/safe@office_datasheet.pdf

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor