Global Information Assurance Certification Paper

Case Study: Secure Application Deployment Utilizing Terminal Server and VPN Clients

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

By: Greg Croteau
October 1, 2004

Table Of Contents

1.0 Abstract

As companies large and small continue to evolve and embrace technology, it becomes more and more imperative to empower the remote worker. The remote worker may be a permanent telecommuting employee, the CEO at his lakeside retreat or the road warrior salesman. Our company consisted of all three of these types. The problem that companies face – and we faced was securely delivering the tools and applications these remote workers require and demand.

I was faced with the task of taking the current infrastructure that consisted of RAS, OWA and a few other "minimally secure" application deployments and migrating them to a secure infrastructure platform. Utilizing a few technologies new to us, we were able to deliver a fully functional and quite secure desktop. The primary objective of this project was to tighten security, and the secondary objective was to provide a more robust platform that performed better then the current RAS/IIS. In order to accomplish both of these objectives it was decided that we would deploy a terminal server environment along with a VPN device for remote users. Since we are not particularly early adopters of the latest technology, we decided to go with a proven Windows 2000 Terminal server environment and Checkpoint Firewall-1 running on Nokia appliances. Our IS department is fairly small, and I was the primary person responsible for designing, building and implementing the new infrastructure. The only exclusion to this would be our outsourcing of the firewall infrastructure.

2.0 Scenario

2.1 Logical layout

The starting point security posture and functionality was very limited. In order to provide the appropriate application access and reasonable functionality, a combination of several technologies would be utilized. The following table lists the application/resource access importance, performance characteristic and overall security rating:

Function	Crticality	Access Means	Performance Level	Security Level
Email access	High	OWA	Medium	Medium
Application access	High	RAS	Low	Medium
Data access	High	RAS	Low	Medium
Internal Sales Reports	Medium	IIS	High	Low
Corporate Website	Low	IIS	High	Low

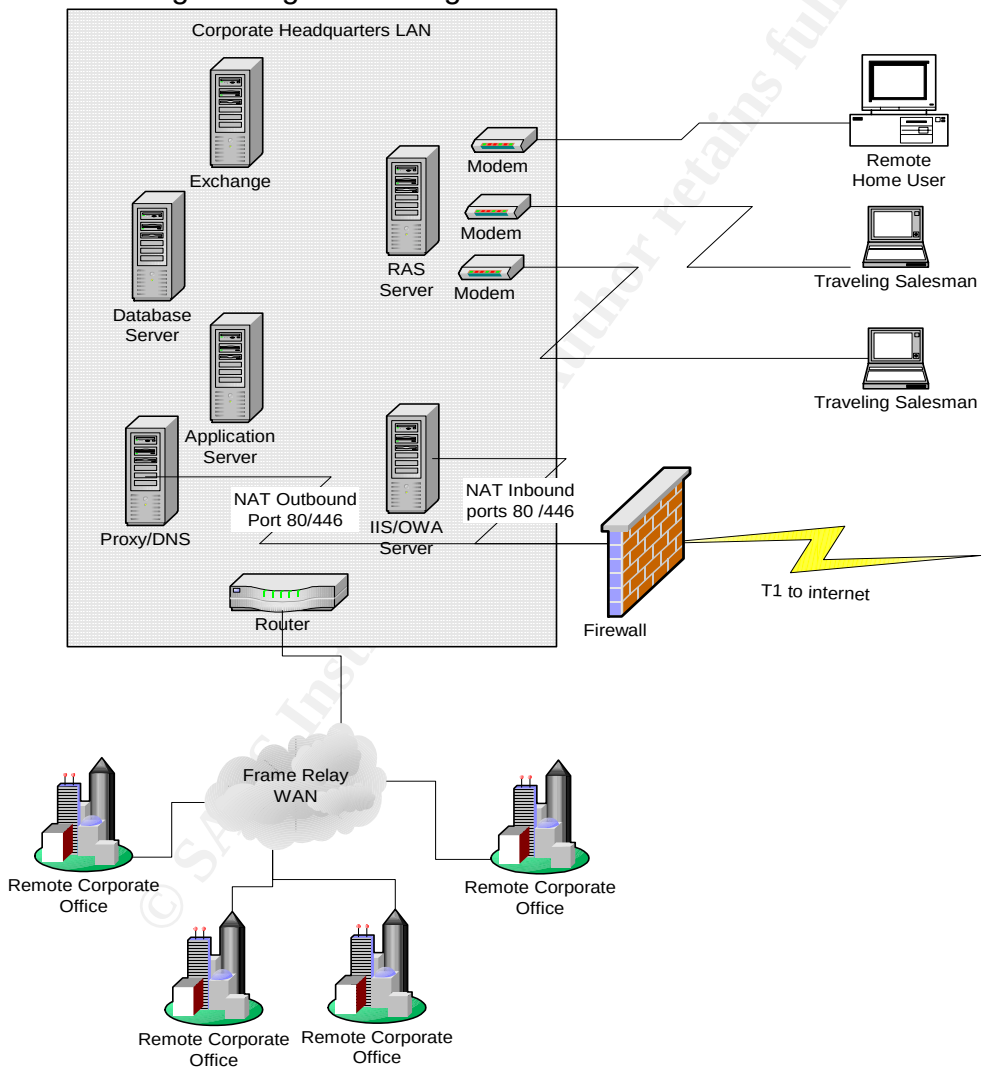
For client access to such things as user directories, shared data directories and FAT client applications RAS direct dial was utilized. There was a modem pool setup at the corporate headquarters site and users would dial directly into this site to access applications/data both at this site and located at the several other WAN sites. This access method proved to be user friendly as all they were required to do was launch the dialer, but performance was severely impacted as

the maximum speed was limited by the 56k modems. At best the access via RAS was sluggish but bearable since it was the only means of accessing these resources. Although RAS appears to be a simple technology to implement and secure, if not administered safely it can be a significant security hole [1].

Access to web enabled resources such as Outlook Web Access for email, custom reports via IIS and the corporate website were all handled by a single IIS server running behind a NAT firewall. This provided sufficient performance, limited functionality (especially OWA) and very low security.

2.2 Physical Layout

The following is a high level diagram of the before state infrastructure.



[1] Federal Office for Information Security (BSI). "Improper administration of the RAS system" IT Baseline Protection Manual October 2003 http://www.bsi.bund.de/gshb/english/t/t03039.html (15 July 2004)

From the initial discussions during the GSEC course it was obvious that this design offered very poor security and was very vulnerable to not only WORM propagation but also script kiddies. With the IIS server sitting directly on the corporate LAN with only a simple NAT firewall separating it from the internet, the chances of an exploit were very good. This is not to say that the current IIS server was poorly maintained, but the odds of not keeping right up to date with new patches due to the testing process left windows of opportunity for exploitation.

2.3 Vulnerabilities

IIS Server: Since there wasn't an official build guide to review from the initial implementation, the actual state of the IIS/OWA server was a bit unknown. Running tools such as the Microsoft Baseline Security Analyzer [2] provided a bit of comfort knowing that the glaringly obvious vulnerabilities did not exist, but the state of the websites it housed and the security of their code was still unknown. Since the websites were built in house and the resources didn't currently exist to migrate the pages or rewrite the code, it was decided that external access to it should be cut.

Firewall: The firewall currently deployed was a fairly basic device – something probably more targeted to home use rather then corporate high volume usage [3]. The firewall provided basic NATing service for the IIS server and Proxy server. The firewall also offered basic port blocking functionality so for the most part seemed to be secure, but reliability was an unknown.
WAN Infrastructure: The WAN to the remaining corporate sites was via a managed frame relay network, so the security and reliability of these connections was fairly high.
RAS Infrastructure: The RAS modem pool was direct dial, and only users that actually had a requirement to dial in had it enabled in their NT profile so this means of connecting was fairly secure, but also fairly slow.

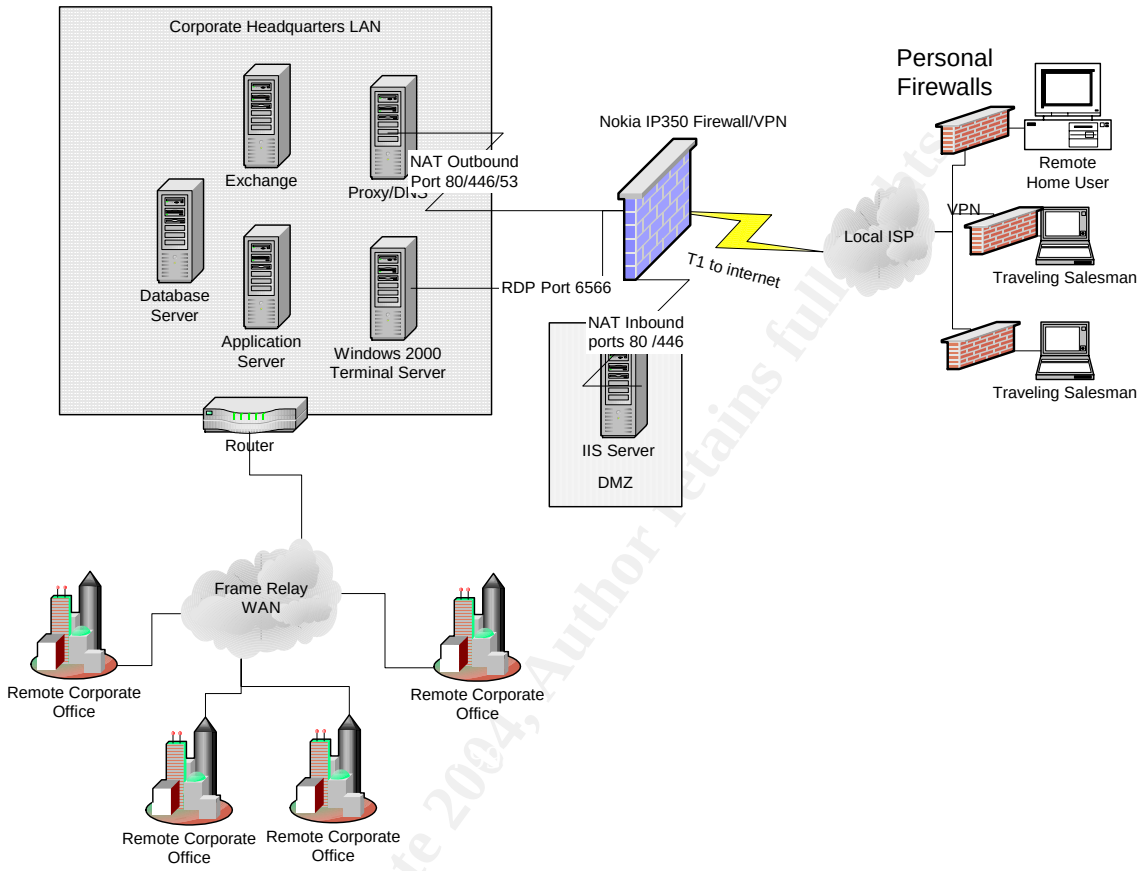
3.0 Solution

The new infrastructure implementation was broken down into three phases. Phase one consisted of the configuration and deployment of the new Firewalls. Phase two was the new Terminal server build and implementation. Phase three was the rollout of the new VPN and RDP clients to the remote users. Applying what I learned during the security essentials course, I designed an infrastructure that met our goals, was reasonable to implement with our limited resources and fit within our budget for this project.

---

[2] Microsoft Baseline Security Analyzer V1.2.1 (August 16, 2004)
http://www.microsoft.com/technet/security/tools/mbsahome.mspx (15 July 2004)
[3] Home Net Help.com "What is a firewall? A simplified explanation" 11-May-2001
http://www.homenethelp.com/web/explain/about-firewalls.asp (15 July 2004)

A high level design was produced and the following diagram depicts our end state goal:



Our design has all access to the corporate network encrypted via VPN, with the only accessible internal system being the new Terminal Server even that runs through the VPN. The Terminal server provides all necessary access to internal systems including Outlook for email access. One of the Nokia DMZ interfaces was designated for the corporate public website running on an IIS server.

3.1 Firewall Implementation

I began my research into firewalls by reviewing Chapter 14 of the SANS Security Essentials and the CISSP 10 Domains course and Guidelines on Firewalls and Firewall Policy published by the National Institute Of Standards and Technology [4]. The review of the SANS material provided a refresher of the general Firewall fundamentals and the NIST paper went further into depth as far as the types of firewalls and the protection they offer.

---

[4] Wack, John, Cutler, Ken, Pole, Jamie "Guidelines on Firewalls and Firewall Policy" January 2002 http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (6 August 2004)

Basically firewalls come in four different categories:

- Packet Filters
- Application Gateways
- Circuit-level Gateways
- Stateful inspection

Since we were interested in eventually getting to a level of security that provides protection down to the content level, we limited our search to the Stateful inspection flavor.

A Stateful Inspection firewall can be described as [5] :

"Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. An example of a stateful firewall may examine not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules (as in static packet filtering) but also on context that has been established by prior packets that have passed through the firewall. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested"

Product Selection

All of the major vendors offer a Stateful Inspection firewall in one form or another. Since we did not have adequate spare hardware to deploy for a software based firewall, we decided to limit our search even further to Appliance Firewalls. When we drilled down into our product criteria even further we cam to the conclusion that the Nokia IP line with Checkpoint Firewall-1 best suited our requirements. The Nokia appliance offered a stable platform which was far more secure then configuring a Bastion host from a Windows OS and then installing Checkpoint Firewall-1. The Nokia IP line also offered various sizes of appliances that would allow us to have an appropriately sized box for an office of 10 up to an office with several hundred. Even though our current project only utilizes a single appliance, we have future plans to replace the Frame network with internet VPN so the various sized boxes would allow us to scale accordingly [6].

---

[5] Webopedia Definition: http://www.webopedia.com/TERM/S/stateful_inspection.html (6 August 2004)
[6] Nokia Firewalls and VPN Appliances http://www.nokia.com/downloads/networks/security_products/NOK_FW_VPN_APP.pdf (6 August 2004)

Firewall Configuration

For our initial configuration we analyzed the access we would require from internal sources and also connectivity that would be required from external sources. The following table outlines our initial requirements.

Function	Source	Destination	Service
Web Browsing	Proxy IP address	any	http, https
DNS	Proxy IP address	any	DNS
Terminal server access	VPN Group	Terminal server IP	RDP 6566
Corporate website access	any	DMZ IIS server	http, https

In order to allow web surfing from corporate PCs, we configured a rule to allow all HTTP, HTTPS and DNS traffic outbound from the Proxy server IP address outbound. This would handle all external browsing requirements including the DNS queries. The only unencrypted inbound traffic allowed would be to the Corporate website which we would locate on a DMZ segment. The IIS server located in the DMZ would not contain any corporate information or Data that was no already public in case the box was exploited at some point. Encrypted VPN traffic would be coming from remote clients to the Terminal server. As a best practice recommendation we planned on changing the standard RDP port from 3389 to 6566 on the terminal server and as a result added the appropriate rule to allow users from the VPN group access.

The VPN User group was configured and the only policy that applied to this group was access to the terminal server – thus if the VPN client was some how compromised it would only have access to the terminal server. This could still be disastrous, but provided another layer to our security model.

Firewall Implementation

The actual implementation of the firewall was fairly straight forward once the Nokia appliance was configured and tested. Since we were on a tight schedule we decided to outsource the initial configuration and turn up of the new firewall and VPN appliance. Using our requirements listed above, the firewall was configured and the necessary VPN user accounts created.

Upon receiving the pre-configured Nokia appliance, the installation and turn up was fairly straight forward. There was a brief period of full unprotected exposure to the firewall as it was initially connected to the T1 router and the policies applied since it was done remotely, but to negate this risk the internal interface

and DMZ interface was left disconnected until the firewall was fully tested and operational. In order to test the configuration and verify only the required ports were open, a free ware utility called NMAP [7] was utilized. The results of the scan verified that only the required ports were open and the internal interface to the corporate LAN and DMZ IIS server were connected.

3.2 Terminal Server Build

Server Base Build and Security Tightening

The hardware platform chosen for our new Terminal Server was a HP DL380 G3. Upon completing the Smart Start installation of Windows 2000, basic security changes were implemented. Using Chapters 25 through 30 of the GSEC course as a guide, I began the hardening of the server. Even though this server's only exposure to the internet was from VPN encrypted tunnels, it became our standard policy to harden any server builds. We first installed the latest service pack for Windows 2000 (SP 4) and then installed the Post-SP4 Hotfixes, Updates, and Security Patches. Once the initial updating was completed, we followed the Microsoft guide to conform to a base level of security hardening [8]. . The steps we determined from this list that held the most significance was the disabling of unnecessary accounts, and the enabling and securing of auditing. These two points were also stressed during the GSEC course.

Terminal Server specific security tightening

Once the base OS was hardened sufficiently, we turned our attention to Terminal Server specific settings. Again we referred to the Microsoft guide for Terminal server hardening [9].

---

[7] Network Mapper Open Source Software: http://www.insecure.org/nmap/ (7 Sept 2004)

[8] Windows 2000 Server Baseline Security Checklist
http://www.microsoft.com/technet/security/chklist/w2ksvrcl.mspx (7 Sept 2004)

[9] Mackey, David "Securing Windows 2000 Terminal Services"
http://www.microsoft.com/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.mspx (7 Sept 2004)

We decided on the following configuration:

Terminal Server mode	Application Server Mode
Delete temporary folders on exit	YES
Use temporary folders per session	YES
Internet Connector licensing	DISABLE
Active Desktop	DISABLE
Permission Compatibility	NT 4 Compatible
RDP Configuration Settings	
Encryption level	HIGH
Use client-provided logon information	SELECTED
Override user settings for session limits	YES
End a disconnected session	3 HOURS
Active session limit	NEVER
Idle session limit	3 HOURS
When session limit is reached or connection is broken	END SESSION

We created a local “Terminal Server Users” group and assigned this group permission to Log On Locally. This permission is required to log on from a terminal client. Only the authorized remote users that will be utilizing the Terminal server were added to this group. We also proceeded to tighten the local disk security by assigning the appropriate NTFS permissions for the Terminal Server Group [10].

Terminal Server Implementation

Once the Terminal server configuration was complete, we began the application installation. While we worked through the application installation, we utilized the local group “Terminal Server Users” created previously to control application access. Where required, only the “Terminal Server Users” group was assigned permissions to access the program files, such as the local package installations required for several of our applications. This prevents unauthorized access to these application shares thus adding another layer of protection.

In regards to Data shares, permissions already were applied for the appropriate users. Since the users were accessing the Terminal server with their regular NT Domain accounts the appropriate permissions were already granted.

Once the terminal server was fully configured and all required applications installed, it was moved onto the primary LAN segment and given the IP address specified in the Checkpoint policy.

---

[10] Lewis, Morris “Terminal Server Security” February 2001 http://www.winnetmag.com/WindowsSecurity/Articles/ArticleID/16524/pg/1/1.html (7 September 2004)

3.3 VPN and Terminal Client Rollout

At a high level the rollout consisted of the following steps:

- Local Internet connectivity
- Install and configure VPN client
- Install and configure Terminal Client

Local Internet connectivity

The only Internet connectivity currently in use was that of the home users. Currently all of the home users utilized a high speed connection whether it was cable or ADSL. There were however, no personal firewalls installed. We decided to deploy a basic "home caliber" firewall the Linksys BEFSX41 [11] to provide this protection. For virus protection on the home users we installed Officescan [12] . For the traveling laptop users we configured PC-cillin Internet Security [13] which provided both firewall functionality as well as virus protection. The traveling users would either utilize a dial account we configured for them or the high speed connection offered by most hotels. Having the PC-Cillin Internet Security suite installed offered protection from the many vulnerabilities using high speed at such locations precents.

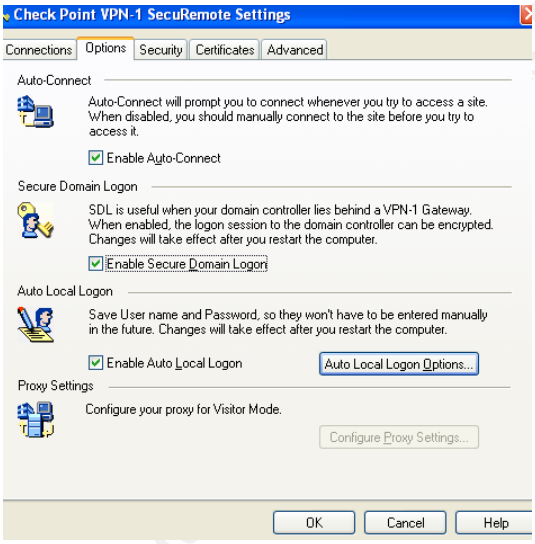
Install and configure VPN client

Due to a tight schedule, secure remote clients were rolled out, but the intention will be to switch these to secure clients which will offer additional desktop security. The vulnerability exists that while using secure remote clients the desktop or laptop could be exploited then that could give the attacker a secure means to penetrate our network. We mitigated this risk by only allowing access to the terminal server from the vpn clients, but to negate this risk completely we would need to enforce desktop policies offered by secure client functionality [14] .

---

[11] Linksys Products http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=433 (7 Sept 2004)
[12] Trend Micro Officescan http://www.trendmicro.com/en/products/desktop/osce/evaluate/overview.htm (10 Sept 2004)
[13] Trend Micro PCCillin http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm (10 Sept 2004)
[14] Checkpoint VPN-1 http://www.checkpoint.com/products/vpn-1_clients/vpn-1_features.html (10 Sept 2004)

The installation was straight forward and the manufactures documentation was followed for the procedure. The only configuration required at the client side was to download a topology map from the Checkpoint firewall and then enter the correct user credentials which we supplied in person. We did however, enable Auto-Connect, Secure Domain Logon and Auto Local Logon. This provided ease of use for the end user, while also allowing them to authenticate during the NT logon process. In the past local profiles were utilized and domain credentials entered when network resources were accessed. The ability to logon to the domain from the onset of login provides seamless authentication for the end user.



Install and configure Terminal Client

The installation of the Terminal client was straight forward. We chose the latest RDP client to install as it offers a single installation source for installation on all windows versions we utilize in our environment. Due to time constraints we chose not to prepackage the installation with server specifics, instead we informed the user of the appropriate server to connect to with the RDP client.

3.4 Testing

Once the installation of the VPN and Terminal clients was completed, the end to end connectivity was tested. Access to the Terminal server through the VPN tunnel performed well as expected. Random testing verified that access through the VPN client was limited to the terminal server only as designed. Once attached to the terminal server, access was limited to the applications defined for the terminal server group. Drive access to directories not intended for terminal server user access was tested and access was denied as expected.

4.0 Concluding Summary

Upon completing this project, we accomplished our goals of significantly increasing remote access to applications and also the secondary objective of increasing performance.

Upon my completion of the Security Essentials course, I was assigned this project. Utilizing the skills I learned in the course I was able to balance a well performing infrastructure with a significantly increased security posture. The application delivery at the end state can be summarized by the following chart which highlights the security and performance characteristics before and after:

Function	Crticality	Access Means	Performance Level	Security Level
Email access	High	Terminal (was RAS)	High (was Medium)	**High** (was Medium)
Application access	High	Terminal (was RAS)	High (was Low)	**High** (was Medium)
Data access	High	Terminal (was RAS)	High (was Low)	**High** (was Medium)
Internal Sales Reports	Medium	IIS	High	**High** (was low)
Corporate Website	Low	IIS	High	**Medium** (was low)

Vulnerabilities that still exist in the environment at the end state consist of typical and ongoing IIS and Nokia/Checkpoint vulnerabilities. This is greatly improved from the beginning state that had vulnerabilities that ranged from RAS, OWA and wide open remote desktops/laptops. Overall, this project was a complete success and greatly reduced our exposure while reducing the number of critical infrastructure pieces that require maintenance and updates.

References

[1] Federal Office for Information Security (BSI). “Improper administration of the RAS system” IT Baseline Protection Manual October 2003
http://www.bsi.bund.de/gshb/english/t/t03039.html (15 July 2004)

[2] Microsoft Baseline Security Analyzer V1.2.1 (August 16, 2004)
http://www.microsoft.com/technet/security/tools/mbsahome.mspx (15 July 2004)

[3] Home Net Help.com “What is a firewall? A simplified explanation” 11-May-2001
http://www.homenethelp.com/web/explain/about-firewalls.asp (15 July 2004)

[4] Wack, John, Cutler, Ken, Pole, Jamie “Guidelines on Firewalls and Firewall Policy” January 2002 http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf (6 August 2004)

[5] Webopedia Definition: http://www.webopedia.com/TERM/S/stateful_inspection.html (6 August 2004)

[6] Nokia Firewalls and VPN Appliances
http://www.nokia.com/downloads/networks/security_products/NOK_FW_VPN_APP.pdf (6 August 2004)

[7] Network Mapper Open Source Software: http://www.insecure.org/nmap/ (7 Sept 2004)

[8] Windows 2000 Server Baseline Security Checklist
http://www.microsoft.com/technet/security/chklist/w2ksvrcl.mspx (7 Sept 2004)

[9] Mackey, David “Securing Windows 2000 Terminal Services”
http://www.microsoft.com/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.mspx (7 Sept 2004)

[10] Lewis, Morris “Terminal Server Security” February 2001
http://www.winnetmag.com/WindowsSecurity/Articles/ArticleID/16524/pg/1/1.html (7 September 2004)

[11] Linksys Products
http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=433 (7 Sept 2004)

[12] Trend Micro Officescan
http://www.trendmicro.com/en/products/desktop/osce/evaluate/overview.htm (10 Sept 2004)

[13] Trend Micro PCCillin
http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm (10 Sept 2004)

[14] Checkpoint VPN-1
http://www.checkpoint.com/products/vpn-1_clients/vpn-1_features.html (10 Sept 2004)