Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Multi-Layered Approach to Small Office Networking

The growth of the internet over the past several years has made it an integral part of many small businesses' daily operations. Small business owners see the internet as a tool to help their business prosper. The internet provides ready access to information, suppliers, and customers via the web and e-mail. The growth of affordable broadband connections such as DSL and cable modems provides small businesses with affordable, always-on connections to the internet. Unfortunately, many business owners do not fully realize ...

Copyright SANS Institute
Author Retains Full Rights

AD

Multi-Layered Approach to Small Office Networking

David S. Taylor
GSEC Practical Version 1.3

Abstract

The growth of the internet over the past several years has made it an integral part of many small businesses' daily operations. Small business owners see the internet as a tool to help their business prosper. The internet provides ready access to information, suppliers, and customers via the web and e-mail. The growth of affordable broadband connections such as DSL and cable modems provides small businesses with affordable, always-on connections to the internet. Unfortunately, many business owners do not fully realize that there are potential downsides to this always-on connection. They are more concerned with growing their business, and securing their network is typically not in their skill set.

This paper will address several areas that small business owners should consider as they deploy and grow their office network. It begins with an overview of network basics, briefly describing two popular network topologies. After the topology overview, the paper will explore several topics that are combined to provide layers of defense against malicious activity directed at their network, either from internal or external sources. These main areas are:

- File Security
- Anti-Virus Protection
- Internet Connectivity
- Remote Access

Network Basics

There are several different topologies available to the small business for constructing their internal network.[1] Ethernet is probably the most popular solution, providing cost effective connectivity at speeds of either 10Mbit or 100Mbit. We will focus on Ethernet for this paper.

Peer to Peer Network

Many small businesses start out with a simple peer to peer network. This configuration, shown in Figure 1, provides simple file and printer sharing capabilities, allowing the members of the network to access files on each others computers and take advantage of pooled printer resources. However, users could have problems if the file or printer they need is located on a computer that is turned off. Typically, the business might designate one of the shared computers as the "server", centralizing its files and printer resources on this workstation.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The peer to peer configuration works fairly well for small businesses with relatively low network activity. However, as the number of users increases they could become frustrated with the performance issues related to using a workstation class computer as the server. Workstations are designed to prioritize foreground processes. Most printer and file sharing processes tend to run in the background, and thus receive lower priority on the workstation.

Figure 1 - Peer to Peer Network Configuration

Dedicated Server Network

The next logical progression for the office network is the installation of a dedicated server, shown in Figure 2. The software that runs on a server is designed to give priority to background tasks. This makes for a much cleaner solution to file and printer sharing on the small network, especially as it grows with the business.

Microsoft offers several flavors of Windows server software, depending on the needs of the business. The most popular choices for small businesses are Windows 2000 Server and Windows 2000 Small Business Server. Small Business Server 2000 provides the functionality of Server 2000 while also adding Exchange 2000, SQL 2000, Internet Security and Acceleration Server, and a shared modem and fax server.[2] The main limitation of Small Business Server is that it supports a maximum of 50 computers.

Figure 2 - Network with Dedicated Server

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Linux and Novell are also possible server software solutions for small businesses. Linux is very affordable and offers lots of functionality. However, installation, configuration, and ongoing support of a Linux server generally requires someone fairly knowledgeable with Linux. While this resource might not be available on the staff of the small business, it is possible to hire a consultant to assist with the installation. Novell's popularity has faded over the past few years and it will not be covered in this paper.

This paper will focus on the multi-layered approach to protecting a small business network that has a dedicated server platform running some flavor of Windows 2000 Server. This configuration is flexible enough to provide a good solution for a wide variety of small business environments. It will not deep dive into the technical nuts and bolts, but rather provide some guidelines for the small business network administrator to consider as he prepares to deploy the network. It will provide references to more in-depth technical papers where applicable.

File Security

The first layer of defense to consider is the protection of the files on the central server. These files could be anything from customer lists to accounting records, and the small business owner might not want everyone in the office to have access to these files. We will look at some issues involving the installation of the server software and involving the configuration of the user account structure on the new system.

Server File System

The initial installation of the Windows 2000 Server software will present the installer with the choice of formatting the drive partitions using either the Fat32 or NTFS file systems. Fat32 is compatible with Windows 98, ME, and XP. It can also be read by various flavors of Linux. Unfortunately, FAT32 does not provide any file security. Thus, a user with access to the disk can read any file on the disk. While this might be acceptable for a home computer, this typically is not the case at a place of business.

NTFS is supported by Windows NT, 2000, and XP. Given the choice, NTFS is almost always the preferred option for server partitions. NTFS supports file level security as well as encryption, allowing the administrator to grant access to particular files and directories on an as needed basis. This follows the principle of least privilege; that is, don't give a user access to more than he needs to do his job. Additional information on the advantages of the NTFS file system is available in Microsoft Knowledge Base Article Q300691.[3]

Workgroup versus Domain

Another decision point will be the choice between setting up the server as part of a workgroup versus a domain. If Windows 2000 Server is configured as part of a workgroup, then the only user accounts it can authenticate are local machine accounts. Microsoft Knowledge Base Article Q299909 [4] documents the steps necessary to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

configure a server to participate in a workgroup. Password synchronization between the various computers in the workgroup is one of the issues that must be addressed.

The recommended option is to configure the new server as part of a domain. If this is the first server on the network, it will be configured as the domain controller. There are several advantages to using a domain on the small network. First, all the users on the network can authenticate using their domain accounts. This allows users to log in from any computer on the network and have the same server access rights regardless of their location. Second, group policies can be distributed using the domain controller to control the policy settings, scripts, and security settings of the network computers.

Microsoft has a full series of articles titled "Windows 2000 Step-by-Step Guides"[5] that walk the small business network administrator through the various steps necessary to install Windows 2000 Server as a domain controller. The Guides are not limited to just domain controller issues, but also cover more advanced topics such as clustering and remote storage that are well beyond the scope of a small business network.

Once the domain accounts are set up, the network administrator can assign users to groups, and the groups are given rights to the resources on the server. Files and directories can be made available to everyone, specific groups, or individual users. The administrator should use the "Domain Users" group instead of the "Everyone" group since the latter group is truly everyone. That is, all users, including anonymous users from the internet, are members of the "Everyone" group.

Internet Information Services (IIS)

One component that is included in the default installation of Windows 2000 Server products is Internet Information Services, or IIS. Unfortunately, the default configuration of IIS is not very secure. The SANS Top 20 List of Vulnerabilities[6] contains three entries that relate to IIS issues. If the small business does not need to host internal web pages on the server then it is recommended that IIS not be installed during the server software installation. If IIS is needed on the server, Microsoft's Lockdown Tool[7] will assist the network administrator in securing the installation to prevent malicious activity.

Anti-Virus Protection

The server should now be configured to segregate directory and file access to the appropriate groups, keeping employees out of unauthorized directories. The next layer of protection to factor in is how to protect the company data files from outside invaders. The first outside invader we will look at is categorized as "malware" (malicious software). Examples include viruses, worms, and trojan horses. A virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.[8] Viruses usually arrive on floppy disks brought in by users or from e-mail messages they receive. Worms are similar to viruses, but they can replicate themselves and spread to other computers without user intervention.[9] Trojan horses are programs

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

that appear to do one thing while actually doing something different, such as granting access to malicious users.[10]

Fortunately, there are several good anti-virus programs that can protect the small business network. These anti-virus programs also protect against worms and trojan horses, so perhaps a better name would be anti-malware programs. A multi-layered approach to virus protection would protect all parts of the small business network. Table 1 lists a few of the more popular anti-virus programs for both workstations and servers.

Product	**Vendor Website**	**Additional Notes**
Norton AntiVirus Corporate Edition 7.6	http://enterprisesecurity.symantec.com	Server and Desktop protection, minimum 10 licenses
Norton AntiVirus Enterprise Edition 8.0	http://enterprisesecurity.symantec.com	Adds E-mail server and gateway, web protection
McAfee VirusScan	http://corporate.mcafee.com	Desktop protection
McAfee NetShield for NT	http://corporate.mcafee.com	Server protection
Trend Micro OfficeScan	http://www.antivirus.com/products/osce/	Server and Desktop
Trend Micro OfficeScan SBS	http://www.antivirus.com/products/ossbs/	Windows 2000 Small Business Server Version

Table 1 - Popular Anti-Virus Programs

The Symantec offering, Norton AntiVirus Corporate Edition, the package the author is most familiar with, offers a very good solution for the small business network. A 10-node network, including the server, can be protected for less than $400, including a year of support and virus definition updates. A similar network running Small Business Server, which includes Microsoft Exchange, can usually be protected for less than $600. There are similar packages available for Lotus Notes, but Notes is not usually found in the small business environment.

Typical Norton Antivirus Installation

Symantec published a document on their web site, "Norton AntiVirus Corporate Edition 7.6 installation walk-through for administrators"[11], which provides a good tutorial on how to successfully install the Norton AntiVirus on your small business network. Figure 3 shows a typical installation of the software. Using the Corporate Version provides several advantages. First, it is possible to download updated virus definitions to the server one time and have the server distribute the updates to each workstation. This occurs transparent to the users, freeing them from having to remember to perform this crucial step. The software is only as good as its latest set of definitions, and new viruses are discovered daily. It is also more bandwidth-efficient to download the definitions

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

from the internet once rather than have each user workstation download them. Second, any virus located on either the server or workstations can be "quarantined" in a central location. This allows the administrator to go to one place to review suspicious files. Finally, it is possible to have the antivirus management console notify the administrator via e-mail or pager when a virus is discovered.

Figure 3 - Norton AntiVirus Corporate Edition Installation

Internet Connectivity

We are building layers of protection into our small business network. We started with the file server and network itself. The next layer of protection is anti-virus software to protect our network from viruses and other malicious software. Another external source that can introduce malicious activity is the internet. The next logical layer of protection to add to our network deals with internet connectivity.

Several years ago most small businesses could only afford a dial up connection to the internet, allowing the transfer of e-mail and some limited web surfing. Faster connections were cost prohibitive and only larger companies could justify them. Today, however, digital subscriber line (DSL) and cable modems have brought the world of always on, broadband connections, to the small business and home user.

The connection options discussed in this section include:

- Router with NAT (Network Address Translation)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Firewall Appliance
- Microsoft Internet Security and Acceleration (ISA) Server

While it is possible to connect the small network server directly to the internet, this is not recommended. Such a connection gives malicious internet users direct access to your files. Also, providing a direct internet connection to the entire network would require that each computer have a public IP address. This is potentially costly since most internet providers charge a monthly fee for public IP addresses. In reality, a public IP address is only necessary if a computer on your network needs to be accessible from the internet. The internet connection from the provider will include one public IP, and that is needed to get the network connected to the internet.

Router with NAT

The first possible technology solution to address network internet connectivity is a router using Network Address Translation (NAT). Network Address Translation is a technology that allows multiple addresses on one interface to hide behind a single, or much smaller group of addresses on a different interface. Internet standards document RFC1631[12] provides a technical overview of NAT, but it goes beyond the scope of our small business network. A key point to remember is that NAT allows the conservation of public, routable IP addresses by hiding the private, non-routable addresses on the internal network.

NAT provides several advantages for the small business network. First, only one public IP address is required to connect up to 253 computers on the LAN to the internet. Second, because the LAN computers have private, non-routable addresses (see RFC1918[13]), the network is afforded a fairly good level of protection from malicious internet users. This stems from the fact that a malicious user cannot initiate a connection to a computer on the LAN that has a private IP address. However, one feature of many NAT routers is the ability to forward ports to particular IP addresses on the LAN, so this level of protection is removed if that feature is used. Figure 3 shows a typical LAN installation of a router using NAT. Some routers provided by service providers connect directly to the broadband connection without the need for a modem.

There are multiple vendors that provide small office routers with NAT capability. Table 2 lists several of the more popular models available. Prices and features vary between models and vendors. Some models have built-in switches, providing a connection point for several computers on the LAN. The author has experience with the Linksys product line and finds they provide good results for a small network.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Product	Vendor Website	Additional Notes
Linksys BEF Series Routers	http://www.linksys.com/Products/group.asp?grid=23	1, 4, and 8 port switches, wireless access point
Netgear RT Series	http://www.netgear.com/routers_main.asp	1 and 4 port models
D-Link DI Series	http://www.dlink.com/products/DigitalHome/CableDsl/	1, 4, and 7 port models

Table 2 - Some Popular Broadband NAT Routers

Most of these products provide simple web interfaces that allow the network administrator to easily configure the router. If the broadband provider is using PPPoE (Point-to-Point Protocol over Ethernet) the administrator should be sure the router considered supports this feature. Port forwarding to individual computers on the LAN, or setting up one computer in a DMZ to receive all port requests, is also configurable via the user interface.

Firewall Appliance

The router with NAT is a hardware solution that provides basic protection to the small business network. One limitation of NAT is that it can not determine if the traffic on a particular port is in response to a request from a computer on the LAN, or instead unsolicited malicious traffic. In order to accomplish this, we need the ability to inspect the packet of information to try and determine its purpose. By inspecting the state of the packet we can usually determine if we should allow this packet into the network. This functionality is called stateful inspection, and Webopedia.com defines it as follows:

> Stateful Inspection[14]: Also referred to as *dynamic packet filtering*.
>
> 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.
>
> Check Point Software is credited with coining the term *stateful inspection* in the use of its FireWall-1 in 1993.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Think of this feature as a hall monitor in a school. Each packet that wants to traverse between various classrooms needs a hall pass. The hall monitor examines the pass based on the rules established by the principal, in our case the network administrator. If the hall pass is acceptable, the packet is allowed to proceed. Once that first packet proceeds, the hall monitor keeps track of this session, knowing that each subsequent packet in that line has been approved. Once the last packet is past the hall monitor he will close that classroom door. If another packet wants to go to that classroom he will have to present his pass to the hall monitor. Packets caught in the hall without the proper pass are not allowed to enter a classroom and have their names written down in the logs.

The growth of affordable broadband internet connections has resulted in the growth of the firewall appliance market as well. As the number of vendors increases, features improve and prices decrease. Table 3 lists several popular firewall appliances. The author has experience with the Sonicwall SOHO2 (predecessor to the SOHO3) and Netscreen 5XP appliances. Both function well, with the Sonicwall being somewhat easier to setup, but the Netscreen providing a more detailed level of control.

Product	**Vendor Website**	**Additional Notes**
Sonicwall Tele3	http://www.sonicwall.com/products/tele/index.html	Protects 5 LAN nodes simultaneously. Also provides 5 VPN tunnels.
Sonicwall SOHO3	http://www.sonicwall.com/products/soho/index.html	Protects 10 LAN nodes simultaneously, upgradeable to 50 nodes. 10 VPN tunnels optional.
Netscreen 5XP	http://www.netscreen.com/products/appliances.html#ns5xp	Protects 10 LAN nodes simultaneously, upgradeable to unlimited. 10 VPN tunnels included.
Netgrear FV318	http://www.netgear.com/product_view.asp?xrp=4&yrp=12&zrp=110	Supports 20 users, upgradeable to 45. Up to 5 VPN tunnels.
ZyXEL ZyWALL 10	http://www.zyxel.com/product/security/zywall10.htm	Protects 5-25 users. Up to 10 VPN tunnels.

Table 3 – Some Popular Firewall Appliances

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Figure 5 - Firewall Appliance

Most firewall appliances provide a web interface similar to the router with NAT products discussed previously. They typically provide logging functions to notify the network administrator of access attempts that violate the access policies they have defined. Some of the products offer advanced monitoring capabilities using Syslog or SNMP protocols. Figure 5 shows a typical installation of a firewall appliance on the network.

Microsoft Internet Security and Acceleration (ISA) Server

Small business owners that selected Microsoft Small Business Server (SBS) 2000 for their server platform have a software solution available to help protect their network. Microsoft Internet Security and Acceleration (ISA) Server is included as part of the suite

Figure 4 - Microsoft ISA Server

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

of applications that make up SBS 2000, but is also available as a stand alone package.

ISA Server combines stateful packet inspection, virtual private networks, filtering, and web caching in a single, integrated package[15]. The web caching engine of ISA Server keeps copies of frequently visited web sites, speeding up the browsing experience for LAN users since pages they request may load from a local copy on their server instead of from the internet. This is especially beneficial with slower internet connections.

The installation process for SBS integrates the installation of ISA Server if that option is selected, and walks the administrator through the basic steps necessary to create a secure network. In order to deploy ISA Server effectively the server needs two network interface cards (NIC) installed. Figure 4 shows what a typical installation might look like. Ethernet cable 1 connects the first NIC to the LAN segment in the office. Ethernet cable 2 connects the second NIC to the broadband modem that provides the connection to the internet. The separate cards allow ISA Server to establish an electronic barrier between the LAN and the internet.

LAN user requests for internet connectivity arrive on the first network card, ISA Server checks its rule base to see if the traffic is permitted, and if so, passes the traffic to the internet via the second network card. Replies from the internet are inspected by ISA Server before returning to the originating LAN computer.

Remote Access

If the small business network administrator uses the layered approach discussed in this paper they will have created a fairly secure network. The small business owner can feel confident that he has taken prudent steps to protect his information from malicious users, both internal and external. However, if the owner or staff needs remote access to the network, perhaps to work from home or on the road, an additional layer of protection is needed. The administrator needs to configure secure remote access. Two popular ways to achieve this are:

- Dial up modems
- Virtual Private Networks (VPN)

<u>Dial Up Modems</u>

Dial up modems have been around for years, and they are a proven method of providing remote access. Microsoft published a TechNet article, "How To: Set up Remote Access for an Intranet in Windows 2000"[16], that provides basic guidelines for establishing remote access using dial up modems. Figure 5 shows a typical remote access solution using a modem. It is possible to have more than one modem installed, depending on the server configuration. The small business network administrator should consider several issues during the installation and configuration of these devices.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

First, the administrator should consider selecting the modem phone numbers from a different exchange than the primary office numbers; this will provide some protection through obscurity. For example, if the small office had a group of phone numbers such as 713-555-1100 through 713-555-1106, putting a modem on the 1106 number would make it much easier for a malicious user to determine which network they were attempting to connect to, and the potential value of information on that network. This network identity would be more difficult to determine if the modem for the above example network was instead connected to a number such as 713-4xx-1836.

Second, passwords play an important role in the deployment of a dial up modem solution. If users have simple passwords, a malicious user might be able to infiltrate the network using guessing techniques or brute force. The network administrator should enforce complex passwords that must be periodically changed and limit remote access to those with a justified business need.

Other technologies are available to help secure remote modem access. Windows 2000 Remote Access Service (RAS) can be configured to call back the user at a predetermined number. If the remote user will always be calling from the same location, perhaps a house or remote office, this can be a good solution. Some modems, such as the US Robotics V.Everything[17], provide an additional layer of security in the hardware itself. The V.Everything modem supports passwords and dial-back security in addition to the normal Windows authentication of the domain. Another interesting product to consider is the Allied Telesyn AT-AR320.[18] This router/firewall protects two Ethernet ports, plus provides two serial ports for connecting to modems. Users that connect via the modem are protected by the firewall just like they were LAN users.

Figure 5 - Remote Access using a modem

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Virtual Private Networks

Another increasing popular method of providing remote access to the small business network is using virtual private networks (VPNs). A virtual private network is a connection over a public medium, such as the internet, that connects two or more nodes of a network together and makes them appear as a single network[19]. Most VPNs use authentication and encryption methods to keep communications safe from outside parties. Firewall appliances that don not provide VPN tunnels as a standard feature typically offer it as an optional upgrade.

One advantage of a VPN is that the connection occurs on the small business network's internet connection. Since the owner is already paying for this connection this can be an economical alternative to dedicated modem lines. Second, if the internet connection is provided using broadband cable or DSL, the link is usually much faster than a dial up modem line. Finally, since most broadband connections are always on, users have remote access capabilities from almost anywhere they can connect to the internet. This ability to connect from the internet can greatly reduce connection costs if users would normally have to make a long distance call to connect using a modem.

Workers at home using DSL or cable modems can connect to the office network and the performance is typically good. Home users should check with their service provider to make sure that VPNs are allowed as several cable providers have prohibited them from home accounts.[20]

Figure 6 - Remote Access using a VPN

Many hotels offer broadband connectivity, providing a fast connection back to the office network for traveling employees. Additionally, several dial up internet service providers offer nationwide plans for under $25 per month. Finally, most firewall appliances, and Microsoft's ISA Server, allow more than one simultaneous VPN connection. This means multiple remote users could connect at the same time using the internet connection. In

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

contrast, a dial up modem solution only supports a single user per modem. Figure 6 shows a typical remote access solution using VPN technology. While only one remote user is shown, it is typically possible to have multiple, simultaneous remote users. If the network administrator anticipates several simultaneous connections they should factor this into the proper sizing of the broadband connection.

Conclusions

This paper guided the small business owner and their network administrator through several different areas to consider as they start to deploy their office network. Each of these areas provides an additional layer of protection to help keep malicious users, both internal and external, from disrupting their networks or gaining access to unauthorized files. The paper started with the basic server configuration, with the main goal of providing segmentation of users and their privileges using the principle of least privilege. The next layer of protection, anti-virus software, protects the files on user workstations and the server from viruses and trojan horse programs.

After creating basic protections for the isolated network the paper looked at several ways to connect the network to the internet in a safe manner. The increasing popularity of broadband connections, hardware routers, and firewall appliances has afforded the small business owner with several economical solutions to provide internet connectivity to increase office productivity and customer service.

Finally, the paper considered a couple of methods to extend network connectivity to remote users. Modems are simple and reliable, but virtual private networks should be considered since they have to potential to provide a faster connection from almost any other point on the internet.

Using multiple layers in the design of the network should help the small business owner feel more comfortable with their network installation, freeing them to work on growing their business instead of constantly worrying about malicious users accessing their company information.

List of References

[1] Microsoft Corporation. "Home and Small Office Network Topologies".
http://www.microsoft.com/windowsxp/pro/techinfo/planning/networking/topologies.asp

[2] Microsoft Corporation. Small Business Server Product Overview.
http://www.microsoft.com/sbserver/evaluation/overview/default.asp

[3] Microsoft Corporation. How To: Set up a File System for Secure Access in Windows 2000 (Q300691).
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q300691

[4] Microsoft Corporation. How To: Join a Workgroup in Windows 2000 Server (Q299909).
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q299909

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[5] Microsoft Corporation. Windows 2000 Step-by-Step Guides.
http://www.microsoft.com/windows2000/techinfo/planning/walkthroughs/default.asp

[6] Sans Institute. The Twenty Most Critical Internet Security Vulnerabilities.
http://www.sans.org/top20.htm

[7] Microsoft Corporation. IIS Lockdown Tool.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp

[8] Internet.com Webopedia. http://www.webopedia.com/TERM/v/virus.html

[9] Internet.com Webopedia. http://www.webopedia.com/TERM/W/worm.html

[10] Internet.com Webopedia. http://www.webopedia.com/TERM/T/Trojan_horse.html

[11] http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2001092508450948

[12] RFC1631, 1994. "The IP Network Address Translator". http://www.rfc.net/rfc1631.html

[13] RFC1918, 1996. "Address Allocation for Private Internets". http://www.rfc.net/rfc1918.html

[14] Internet.com Webopedia. http://www.webopedia.com/TERM/S/stateful_inspection.html

[15] Microsoft Corporation. ISA Server Product Overview.
http://www.microsoft.com/isaserver/evaluation/overview/default.asp

[16] Microsoft Corporation. How To: Set up Remote Access for an Intranet in Windows 2000 (Q301193)
http://support.microsoft.com/view/tn.asp?kb=301193

[17] US Robotics V.Everything 56K Analog Corporate Modem web site.
http://www.usrobotics.com/products/business/business-product.asp?sku=3CP3453

[18] Allied Telesyn Web Page.
http://www.alliedtelesyn.com/product/ar320s

[19] Internet.com Webopedia. http://www.webopedia.com/TERM/V/VPN.html

[20] "Cable firms cloud AT&Ts VPN vision", Denise Pappalardo, Network World, 03/12/01.
http://www.nwfusion.com/news/2001/0312aup.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**