Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2d

Do You Need a Security Assessment?

by

Joseph Rabener

The Increasing Risk

Every day the number of people using the Internet increases, not just in the United States, but all over the world. The activities range from single users communicating via email or surfing the web to large corporations providing connectivity for remote employees or business partners. There are currently 215.6 million English speaking people and 237.8 million non-English speaking people online and that is projected to increase to 230 million and 560 million respectively by the year 2003. (Global Reach website) http://glreach.com/globstats/index.php3?goto

An excerpt from an article from The Detroit News details the risk.

> *In 1999, companies spent $7.1 billion to ward off cybercrimes -- everything from data theft and disruption of service to virus attacks and online fraud, according to the Aberdeen Group, an Internet analyst firm based in Boston. It projects corporations worldwide will spend $17 billion on cybercrime security measures by 2003. The crimes themselves also have a huge financial impact. For example, computer virus attacks worldwide cost businesses more than $17 billion last year, according to Computer Economics, a research firm based in Carlsbad, Calif.* (The Detroit News) http://detnews.com/2001/technews/0105/29/b01-229644.htm

With so many people online, security risks increase, as does the need for an effective security strategy. There is an increasing amount of activity by people sneaking and peeking, testing to see if they can gain access to your network or systems for various reasons, some just to see how far they can go, others may have malicious intent. Are you willing to take the chance?

Not only do you need to worry about your own resources, there is now cause for concern about liability if one your systems is used to launch an attack against a third party. According to an article from the Tech Republic website, even if you have a firewall in place don't count on that to keep you out of trouble. You may be brought into court to answer questions about the level of commitment your organization has with regard to network security.

> *The New York Law Journal recently asked specialists in computer law if distributed attacks like those seen in February could lead to negligence suits against the systems that hosted the attacks. Their unanimous verdict: Yes. Companies are finding the agents for a DDoS attack lurking on their systems nearly every day, according to the CERT Coordination Center, a research and response program located at Carnegie Mellon University in Pennsylvania.* (TechRepublic) http://www.techrepublic.com/article.jhtml?src=search&id=r00520000405law01.htm

It's time to consider taking a closer look at your network security practices.

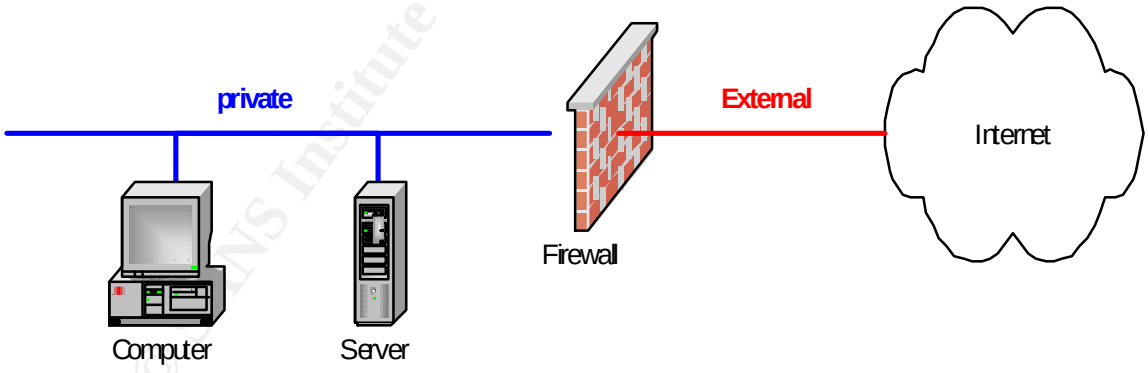
The Puzzle

The world of network security can be an intimidating place. Hackers and attackers doing mysterious things that most of us think we could never begin to understand. Firewalls, VPN, encryption, intrusion detection and forensics are all fairly new concepts and not widely understood. The dynamic and ever evolving nature of the attacks is overwhelming, or so I thought. Upon closer examination and with some training the smoke begins to clear. Understanding some basics about how packets can be crafted to take advantage of certain weaknesses removes much of the mystery around what hackers and attackers are up to. Let's examine some concepts that may clear some confusion.

Firewalls

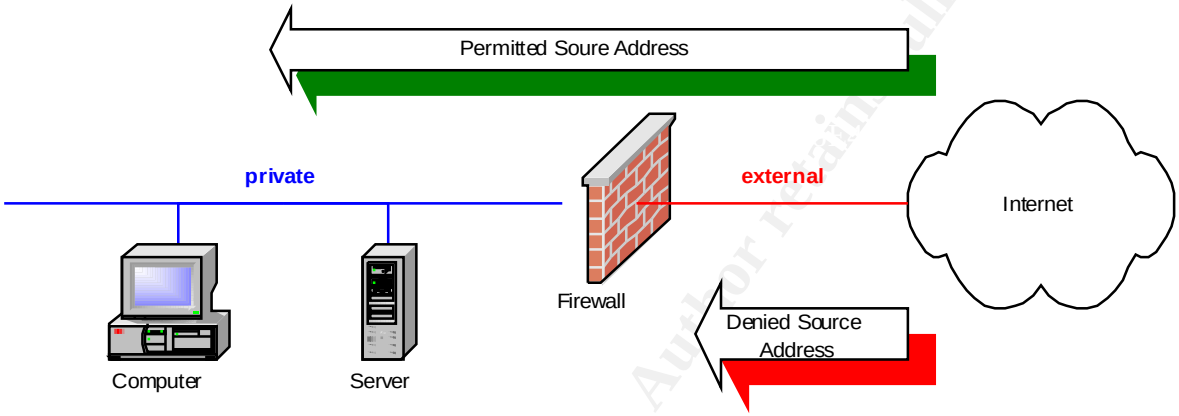
Basics

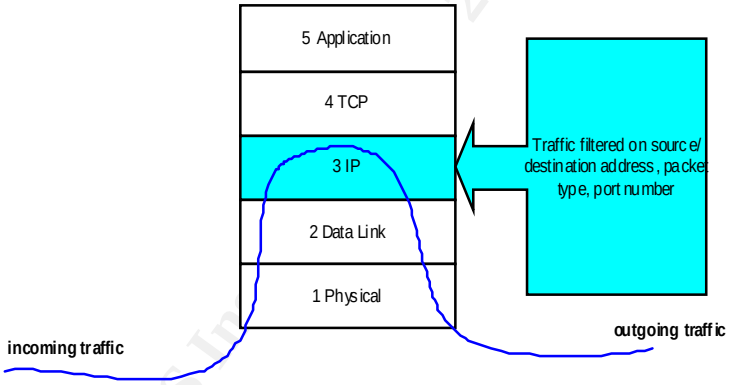
Firewalls are not the magic cure all, they are simply a tool to provide a first line of defense between your network and the Internet. A firewall is a device that protects a private network from hostile intrusion from an outside network. A firewall must have at least two interfaces, one for the private net and one for the public net. A firewall may be implemented by a generic computer and a software product or by a dedicated integrated device.



Methods- There are various techniques used in implementing a firewall.

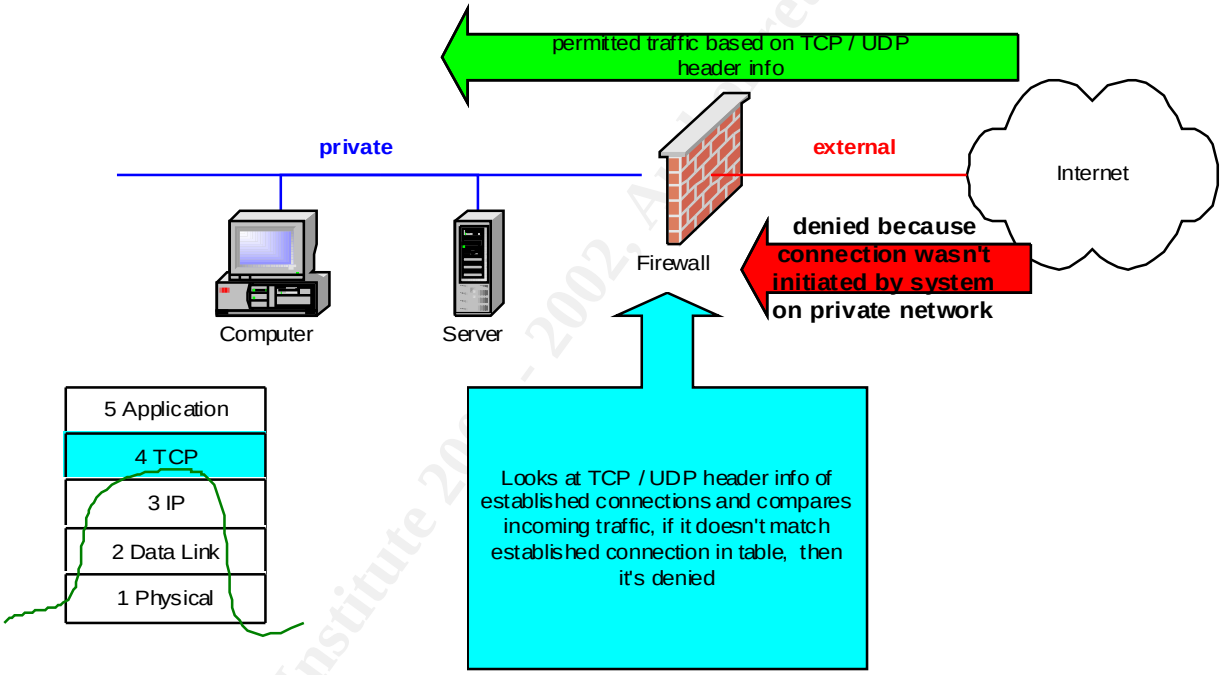
Static Packet Filter- Network layer filtering. Simple permit/deny type of implementation based on source/destination addresses or source/destination port /protocol.
Cisco router access-list is an example.



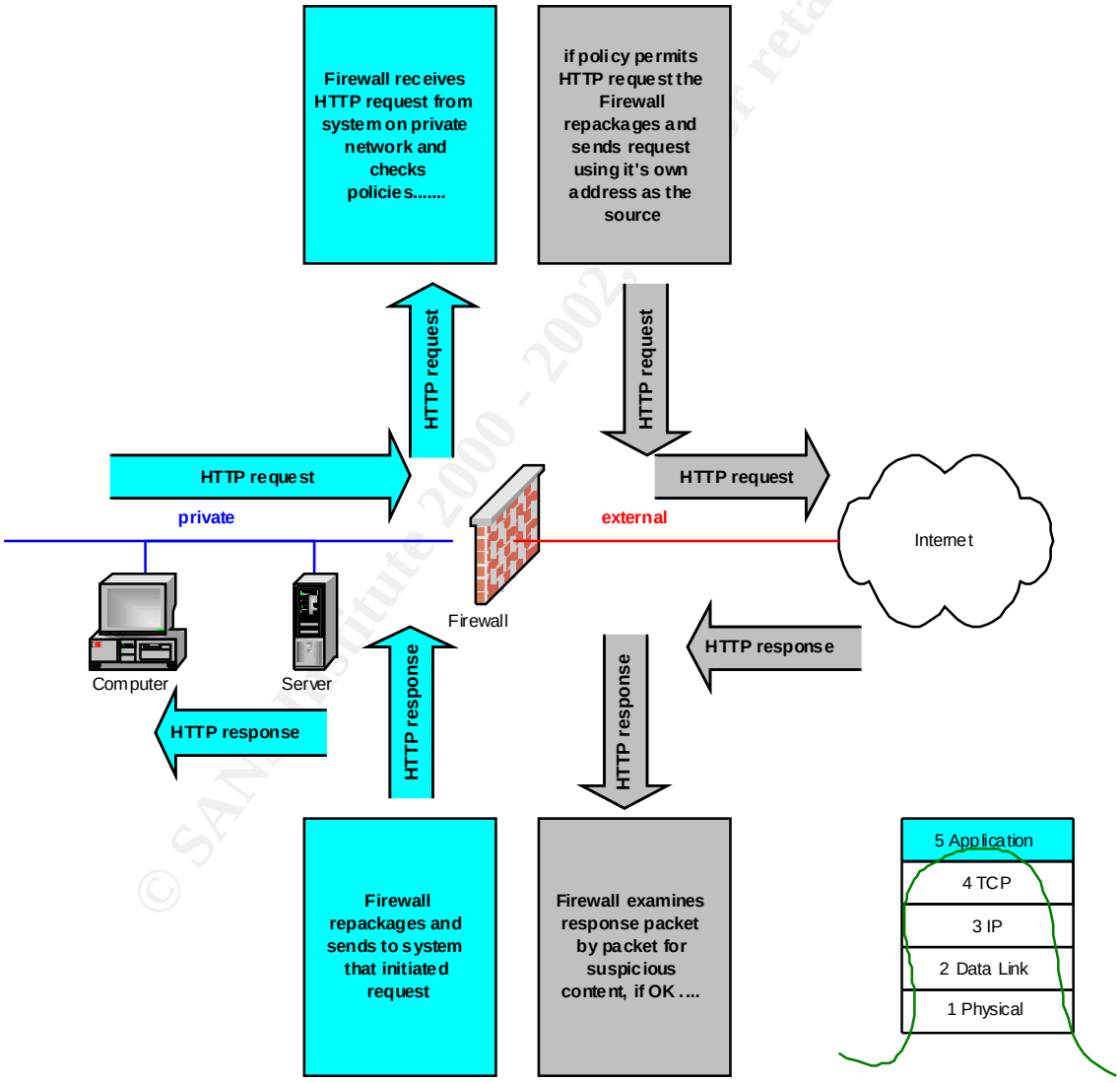


Dynamic Packet Filtering/ Stateful Inspection-

Enhancement to packet filtering. It examines more than just the source/destination info of a packet. It looks at the protocol header fields for TCP/UDP information. Creates and uses a table of established connections and then compares header info against each packet that attempts to pass.

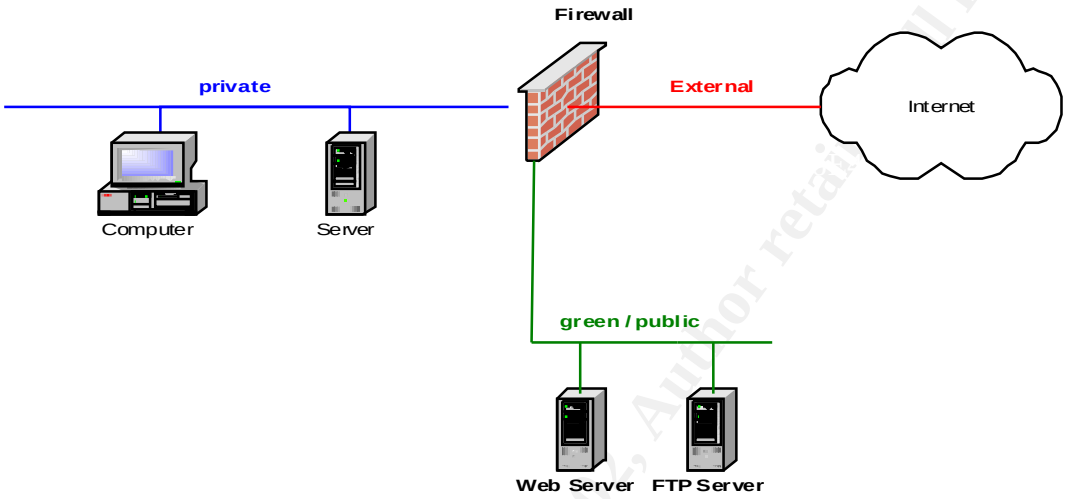


Application / Proxy- This method is the most thorough and rigorous. This type of firewall requires all communications to connect directly to it. It doesn't route connections to a device, it instead acts as proxy for the device. It examines packets at the application level. Filtering can be done on application protocols such as SNMP. HTTP, SMTP etc. The trade off for this level of security is throughput.



Public / Green Subnet or "DMZ"

The Public / Green Network also known as "DMZ" (Copyrighted by Checkpoint) is a network where controlled access is allowed. Web servers and FTP servers may reside here to be utilized by users from external networks while protecting the private network.



Summary

- Firewalls are meant to protect valuable computing resources or confidential information from users on external networks.
- Firewalls are only one piece of a good security strategy.
- Packet filtering is the most basic form of Firewall, but least secure.
- Stateful Inspection offers better security, but is a bit more complex.

  examples: Checkpoint Firewall-1
  Cisco PIX

- Proxy Firewall is the most secure, but sacrifices speed to insure security.

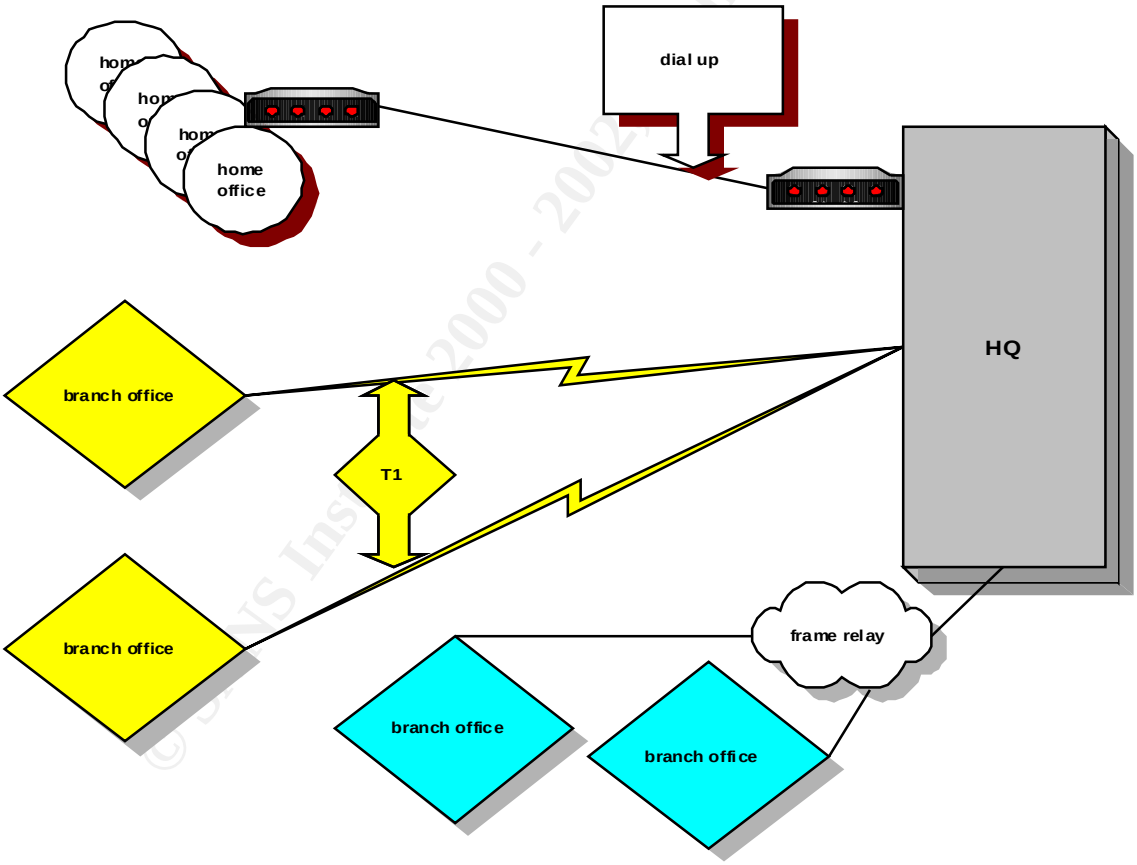
  examples: Altavista
  Raptor–EC

- There seems to be a convergence in Firewall implementation with vendors incorporating features from Packet Filtering and Stateful Inspection to improve performance and features from Proxy type to improve security.

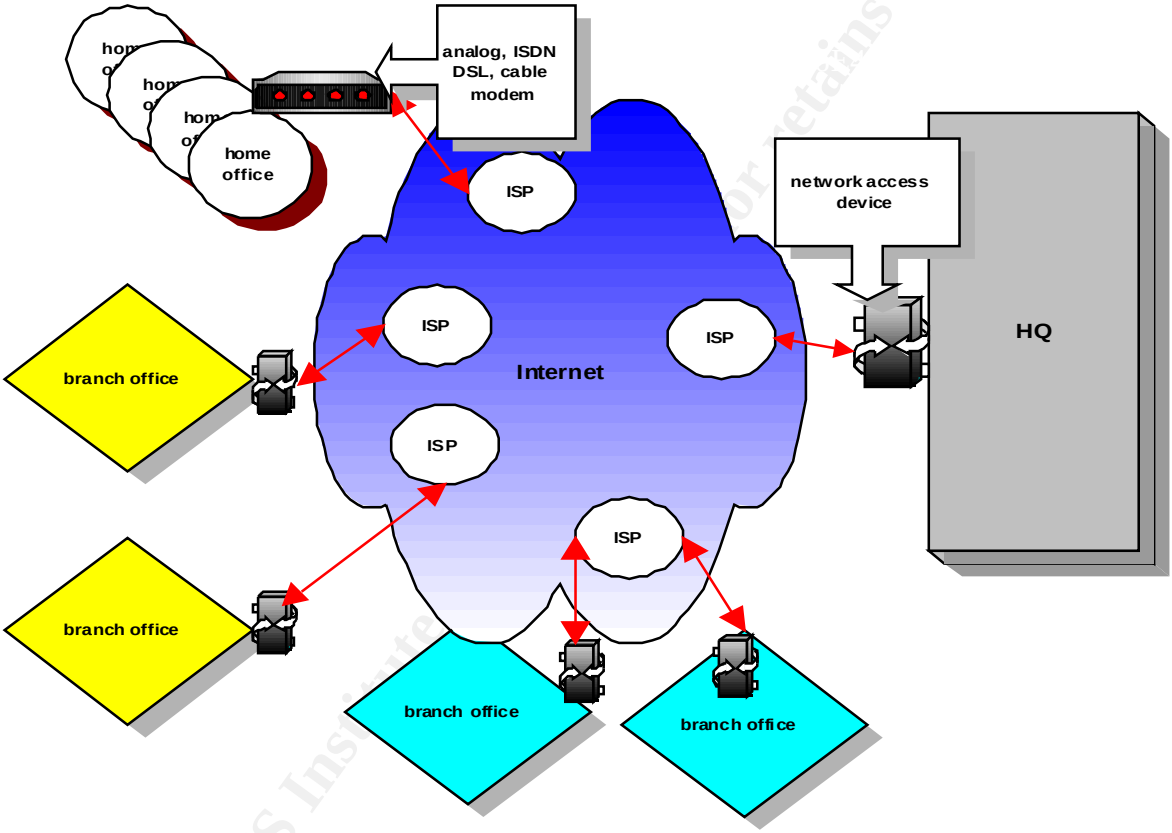
VPN- Virtual Private Network

History and Background-

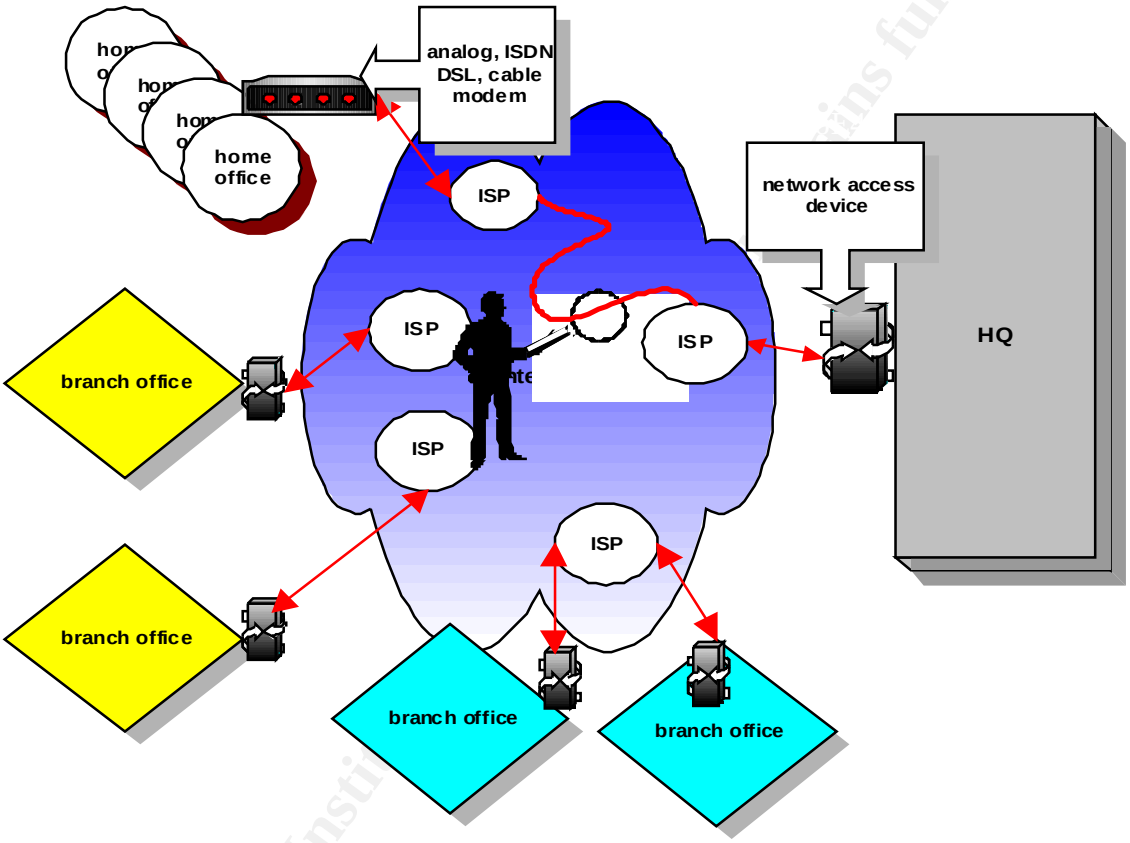
- There is an increasing need for people at different locations to access information.
- Whether from a home office or a branch office, the traditional methods of providing access via leased line or dial-in can expensive or inefficient.



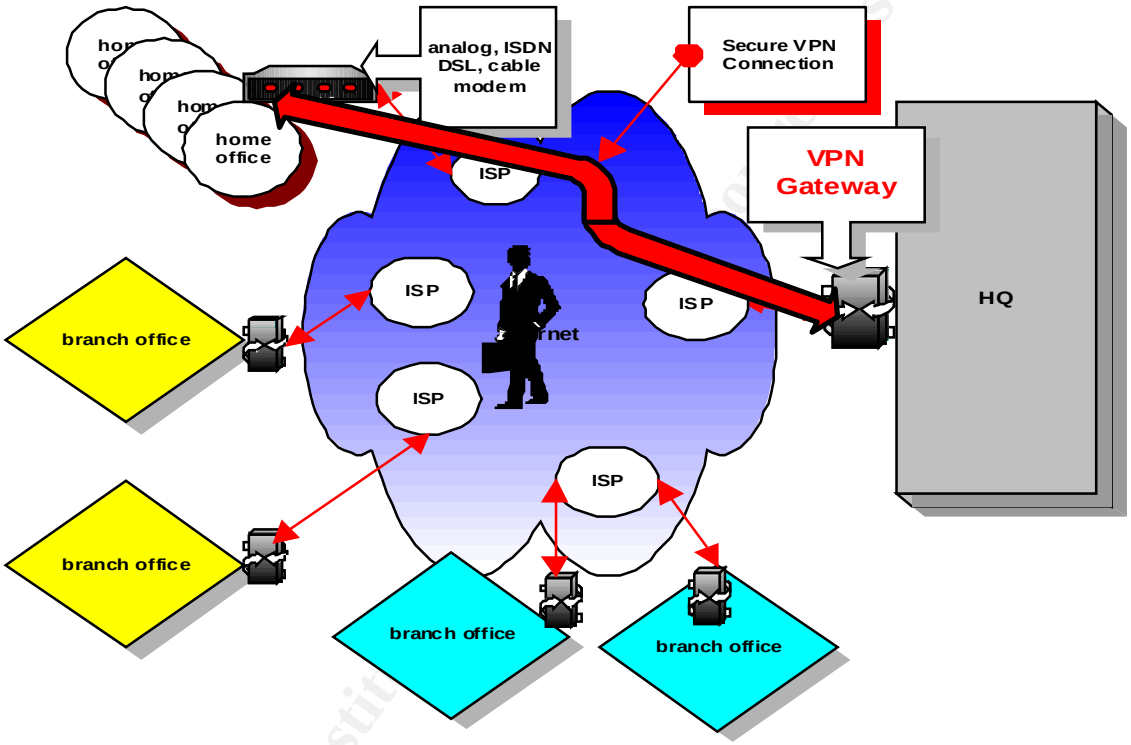
- There is now the infrastructure available through the Internet to support corporate communications through ISP's.
- It's much less expensive!



- **PROBLEM!** - **The Internet is a public network and is inherently unsecured. Who else has access to your data?**



- **Solution VPN- Virtual Private Network**
- **VPN provides secure connections by means of**
  - ***Authentication***
  - ***Encryption***
  - ***Encapsulation***



How a VPN Works

A VPN uses a combination of authentication, data encryption, and tunneling to create a secure channel between a user and a corporate network or between two networks. In a remote access situation, the users dial in to the local access provider's POP, establish a connection to the Internet, and then identify themselves to the corporate VPN's authentication system. The VPN verifies the identity of a user either on the basis of username and password, a hardware token and PIN number, or some other authentication mechanism. Upon successful authentication, tunneling and/or encryption is set up for all traffic between the VPN client and VPN server

Authentication

- establishes the identity of the sender or receiver of information.
- is implemented through passwords, challenge / response schemes or public / private key encryption.
- as relating to VPN's generally consists of a password to initiate the connection followed by the exchange of "key" information between the client and the server. After the tunnel endpoints authenticate themselves, secure communications can begin. Typically the VPN server generates a key file, which then must be loaded on the client, which allows this authentication procedure.

Encryption

- is implemented using a mathematical algorithm applied to the plain text
- Before data is transmitted over the public network it is *encrypted*. There are various encryption schemes including RSA's RIVSET Cipher, DES and Triple-DES. "Keys" are used to encrypt and decrypt data. "Keys from 40 – 128 bits are used.
- The larger the key, the more difficult to crack the code, and the more overhead involved thus a decrease in performance.
- 128 bit encryption has yet to be compromised**.**

Encapsulation

- a VPN gateway / router takes encrypted cipher text and encapsulates it in packets with it's own address as the source, also known as *tunneling*.
- There are two basic types of tunneling. End to end tunneling is client to server connection. Node to node tunneling terminates at the edge of a network and is used to connect LAN's.
- There are three major tunneling protocols, IPSec (IP Security), L2TP (Layer 2 Tunneling Protocol) and PPTP (Point to Point Tunneling Protocol).

Intrusion Detection

Intrusion detection is another piece that is important in an overall security strategy. Various methods are employed to alert people to suspicious activity on the network. There are a number of products available from freeware to expensive commercial offerings. They each have their strengths and weaknesses. They possess different capabilities that range from passive logging and notification to taking prescribed actions such as terminating a suspicious session. A major piece of intrusion detection is uncovering the details of an attack. How it was done, when it was done and possibly where it came from. An effective intrusion detection product should recognize suspicious activity and react accordingly, and its logs should help your staff understand the nature of the attack and take steps to prevent future attacks. Again the key is, intrusion detection is just one piece of good security policy.

Forensics

The word forensics conjures up images of detectives in a seedy hotel room sifting through the evidence for clues about the crime. In the world of computers and networks it's more likely to be IT staff members in a messy office or a chilly computer room, eyes locked on a screen or poring over printouts trying to determine how the network was compromised. It's all about clues. Intrusion detection systems should provide a great deal of information about the nature of the attack. Firewall, system and router log files should be used as well. The idea behind forensics is that there should tools and mechanisms in place to capture data that provides insight and clues into an attack. There should also be policies and procedures in place so that the data collected is utilized properly. The most important concept here is that another attack of the same nature can be prevented based on what was learned by examining the data from a previous incident. This data may also provide the proof necessary to prosecute the attacker(s).

Attacks and Threats

Attacks from the outside generally begin with data gathering activity. Attackers use various tools and methods to learn about your network and computing environment. They can map your network, determine device and OS information and find vulnerabilities. Using this information, attackers can launch denial of service attacks, send costly viruses or steal critical information. They are ways to make it time consuming and difficult for an attacker to gather the information necessary to compromise your network and that should be your goal.

While it's good practice to do every thing you can do to prevent attacks from the outside, a larger problem is the internal threat. *"In fact some studies state that as much as 70 percent of all attacks come from someone within an organization or from someone with inside information (such as an ex-employee)."* (Mastering Network Security)

Peter Shipley's article "The Threat from Within" provides an even higher estimate of internal attacks.

> *In this month's article we will talk about the "threat from within:" internal security dangers as opposed to threats from an outside source. Incidents of both internal and external computer crimes appear to be on the rise. Recent surveys indicate that disgruntled employees may account for up to eighty-nine percent (89%) of attacks and security violations.*
> (networkcommand website) http://www.networkcommand.com/docs/mole.html

These threats, internal and external must be addressed with a thorough analysis of your computing and network environment and a comprehensive plan to protect it.

At first glace all of the components that go into a security strategy seem a bit overwhelming, like an unsolvable puzzle, however with the proper training, research and investigation, the pieces of the puzzle start coming together. The key is to realize that there is no single solution to your security needs. Many components must be employed to provide a strong defense against the scoundrels who would compromise your network. Defense in depth, a layered approach is necessary to protect your resources against attack.

Security Assessment Delivery

While a Security Assessment can be delivered as a stand-alone service, there is an advantage to incorporating it into a larger Site Assessment project. A typical Site Assessment might include analysis of the OS management practices, a look at how applications are being used, storage and backup practices and network performance. The information and insight provided by the other phases of a total Site Assessment allow us to see the big picture. With a more complete understanding of the total environment, we can better focus on the most important aspects of our customer's security practices and priorities. The Site Assessment provides a great deal of information needed to perform the Security Assessment.

Phase 1- Prerequisite Information

Before an effective security assessment can begin there a few prerequisites to deal with. In order to assess a network we must know what it looks like. All companies have up to date documentation and drawings of their network infrastructure. Don't they? All organizations use a strict move, add or change policy to approve and document changes. No? Please excuse the sarcasm, but I continue to be amazed at how often the most basic elements of network management are ignored. Don't build your operation on shifting sands. Attention to fundamentals will help you lay a solid foundation for your computing enterprise and your security strategy, and will pay off in the long run. In order to begin we need to have an understanding of the network.

Network documentation.

- physical / logical drawings or network maps
- identify key network components and servers
- ip addressing scheme

Phase 2 - The Survey

After reviewing the prerequisite information so that we have a good understanding of the basic network infrastructure, it's time look at the various components that comprise a security strategy. We need to note which products are being used, revisions, how they are configured and performance issues. It's important to listen to the folks who work in this environment every day. They can provide insight into operational issues that may yield important and helpful information. A basic checklist can be useful when acquiring the information.

Firewall

- ✓ product
- ✓ revision
- ✓ configuration details
- ✓ issues or comments

VPN

- ✓ product
- ✓ revision
- ✓ configuration details
- ✓ issues or comments

Virus Protection

- ✓ product
- ✓ revision
- ✓ configuration details
- ✓ update policy
- ✓ effectiveness
- ✓ issues or comments

Intrusion Detection

- ✓ product
- ✓ revision
- ✓ configuration details
- ✓ update policy
- ✓ effectiveness
- ✓ issues or comments

User Community

- ✓ Operating system(s) used
- ✓ type of applications
- ✓ % of remote users
- ✓ remote access method
- ✓ password policies
- ✓ external modem policies
- ✓ web access policies
- ✓ personal software policies
- ✓ authorization policy- who can do what

Management

Is there a written policy and procedures document specifying actions to be taken and who is responsible for various tasks?

- ✓ auditing practices
- ✓ move, add , change policy
- ✓ backup practices
- ✓ incident response-
  - response to firewall issues
  - VPN problems
  - intrusion alerts
  - how is a virus dealt with

Testing and Data Collection

The exact tools and procedures used are dependant on the customer's environment and policies. Please be aware that some phases of testing can be intrusive and cause disruptions for the customer. They must be made fully aware of this and grant written permission before beginning these tests.

Data Collection

If this is part of a Site Assessment then much of this work has already been done, if not then various snmp-based tools may be employed to collect network performance data. Utilization and error baseline information may be used to determine where to focus security efforts. Fluke LANmeter or a sniffer type tools can be useful to identify protocols and to look at unencrypted traffic that may be a security weakness. Some may think that this is over kill, but I believe the more information available about the computing and network environment the more effective you will be in protecting it.

Testing

Once again I must reiterate, please make sure the customer understands the implications and risks of active testing. Protect yourself, your company and the customer you are working with by having a buy off in writing from management before doing any testing. There are many tools available to do vulnerability scanning. The environment and your personal preference determine which tools to use. The point of this testing is determine vulnerabilities, and performance of logging features of the firewall and intrusion detection system. Password security should also be tested on systems to make sure password policies are being followed. Various audit tools should be used to gather baseline information.

Phase 3- Compiling and Analyzing Data- Generate Report

Now that the data has been collected and the results of testing are in, all of the information must be analyzed. Understand that all of the data and results must be considered along with the information acquired through conversations with the customer(s) you have worked with during this process. The system managers and network administrators and other members of the staff can provide valuable insight into their organization's attitudes and priorities that can help to focus on what is important to that particular company.

Prerequisites

Observation:

Was the prerequisite information provided by the customer accurate? Were the drawings up to date? Does the customer understand their network? If not, then hopefully the assessment activities provided the information necessary to proceed. It would be extremely difficult to design an effective security policy if the network topology and addressing scheme are in question.

Recommendation:

The recommendations might range from "customer has excellent procedures in place to keep information accurate" to "customer desperately needs to implement procedures". Suggestions for improvement may include a policy that a request, review, approve and document procedure is used before any changes are made. That some type of network or enterprise management tool be deployed (e.g. Openview or Netview). The policy should designate individuals responsible for monitoring and managing the tools in use. All too often the tools are in place, but nobody is watching them and changes in status go unnoticed.

Firewall

Observation:

Does the particular firewall being used provide adequate protection? Is it configured properly? Is the customer aware of any issues or problems? What vulnerabilities did the testing uncover? What is the performance like, is there a bottleneck? Access-lists on routers should also be looked at and analyzed this time as well.

Recommendation:

Based on observations and results of testing, a stateful inspection or proxy type firewall may be recommended to replace a packet filter type, or it may just come down to reconfiguring the existing firewall, or no change needed.

VPN

Observation:

Does the VPN in use perform well? Is it easy to configure and maintain? Do the encryption and authentication mechanisms perform well?

Recommendation:

Suggestions may include migrating to a more secure encryption and/or authentication scheme.

Virus

Observation:

Which product is being used? What are its capabilities and performance record? What is the update policy? How responsive is the vendor? Where is it deployed?

Recommendation:

Recommendations might range from everything is ok, to considering a different product or a newer version. Another consideration is where the product is deployed. Is it at a network gateway or individuals systems? A multi-layered approach may be recommended.

Intrusion Detection

Observation:

What form of intrusion detection is employed? How effective is it at notification and logging? How did it perform against vulnerability assessment?

Recommendation:

There are many methods available to implement intrusion detection, combinations of freeware and homegrown applications to full blown commercial offerings with many features. The key is that the intrusion detection system is able to recognize suspicious activity, and inform the appropriate parties. It must not only provide timely notification, but it also must have good logging capabilities that provide detailed information that will aid in tracing the attack and provide information to help defend against future attacks.

User Community

Observation:

How many users and what resources are being used? What is the level of sophistication? How many remote users are there? How do they connect? Are the users complying with policies on passwords, web access, personal software etc?

Recommendation:

This is clearly one of the most important areas and probably one of the most difficult to get a handle on. A large percentage of security breaches and compromises are internal. There should be limitations on what resources employees can access and a mechanism in place to monitor access. Many times there is no malicious intent, just uninformed or unaware users combined with sloppy practices that can cause serious problems. The user community must be educated to the dangers of certain practices. They must be made aware of techniques used by attackers to gain knowledge that can be used to compromise security. A password-cracking program may be part of the testing phase and will identify weak passwords. A strong password policy must be incorporated with educating the users why it is necessary, to insure compliance. Another issue to consider is making sure the operating systems are hardened by removing unnecessary services and keeping patches up to date. Personal firewall products should be considered as well for remote users.

Management

Observation:

This is the heart of it all. Upper management must buy in to the importance of putting together a cohesive and effective security strategy, because they control the money needed to carry out any security strategy. This is no easy sell, particularly in times of an economic slow down, but we must do our best to inform and educate on how critical it is to build a strong, resilient and secure computing and network infrastructure.

Recommendation:

With management's support a security strategy must be developed. It should be discussed and considered by key personnel. It must be agreed upon and documented. The policy must be clear and concise. The document should easy to understand and adaptable. It needs to reviewed regularly and changed or modified as necessary. The staff's responsibilities should be clearly defined, so that they may react with confidence when necessary.

Who is responsible for carrying out security audits, what exactly is audited and how often? The move, add and change procedure should be strictly followed, the rules should be clear and the process easy to follow. Who is responsible for backups and what is the procedure? Incident response should outlined and easy to carry out, with a defined escalation path and procedure. Who gets notified for firewall issues, or VPN problems? If there is an intrusion alert or a denial of service attack, what's the procedure? If a dangerous virus is discovered, how does the staff deal with it? The system manager or network administrator may be familiar with the correct procedures to handle emergency situations, but what about the 3rd shift computer room operator? What if key personnel suddenly become unavailable? Are the procedures clearly written so that someone else can step in and take over in times of crisis. Is there a process in place to notify vendors or law enforcement agencies if there is an attack against your network?

There are many considerations when developing a security policy. Each organization needs to tailor it to there own circumstances. The policy will never be perfect and will need to be modified, updated and improved, but having a plan in place will reduce the negative impact during an emergency. The money (and job) you save may be your own.

Security is Crucial!

Security is not a firewall!
Security is not an intrusion detection system!
Security is not an after thought!
Security is an integral piece of your computing environment.
Every upgrade, every new project or purchase should be planned with security in mind.

Attacks are on the rise. There are new viruses being unleashed regularly. Stolen data and denial of service attacks can cost your company money. There are even liability issues if your network is used to launch an attack against someone else. Would you leave the doors to your business unlocked at night? Why would you leave your network unprotected? Do businesses use burglar alarms to notify the authorities if there is a break in? Shouldn't you employ an intrusion detection scheme of some type for the same purpose? I could go on and on with analogies, but I suspect you get the point.

When you look at security solutions, it really helps to look at the big picture. A complete Site Assessment would certainly go a long way in helping to identify the critical pieces of your operation. Configurations and practices can be documented and considered. The network portion of the assessment will provide a good understanding of the network topology and any configuration or performance issues. Once the basic infrastructure items are understood, we can proceed with developing a security strategy. Please keep in mind the concept of defense in depth. No single element can effectively protect your network. Firewalls, VPN's, virus protection and intrusion detection are all necessary to provide a formidable defense against attack. The tools and technology are only a part of the big picture. The human factor is critical. Management must be aware of the risks, and supportive of the effort to protect the corporation's resources. The IT staff must understand their roles and responsibilities. The user community should be educated on the reasons for, and the policies necessary to protect themselves and the company's assets.

The world of network hackers, attackers and the components that go into protecting against them is complex and dynamic. It is a running battle with new exploits every day. It was my intention to provide you with a basic understanding of the some of the key concepts involved, to demonstrate that the puzzle is not as complicated as it would appear. There are many resources available to you. Some free, some not. I've found the "security" community to be extraordinarily helpful and willing to share information. Please explore the list of resources provided in Appendix A.

It is my hope that you now realize that you can take a step-by-step approach to assess, analyze and develop the means to protect yourself even if your not a security "expert". Nobody becomes an expert overnight. Look at your environment, decide on your priorities and begin to build your security infrastructure. Best of Luck!

Appendix A

Web Resources

Network Magazine Security Articles.
http://www.networkmagazine.com/search?queryText=security&SEARCH.x=30&SEARCH.y=13

Information Security Magazine
http://www.infosecuritymag.com/

Intranet Journal
http://www.intranetjournal.com/

Computerworld's Security Community
http://www.computerworld.com/community/security

Computerworld's Security Resource Center–lot's of good links
http://www.computerworld.com/cwi/itresources/resource_center/0,,NAV63_KEY73,00.html

Tech Republic Security Section
http://www.techrepublic.com/briefingcenter.jhtml?id=b013&source=b013

Network Computing Security Articles
http://www.networkcomputing.com/search/search?queryText=security&sort=date&Find=Find&coll=NWC

Network Security Library- guide to security books
http://secinf.net/

SANS Institute online- tons of good stuff, take your time here
http://www.sans.org/

Center for Internet Security
http://www.cisecurity.org/index.html

TruSecure Corp- good info and links
http://www.trusecure.com/

Computer Security Institute
http://www.gocsi.com/

VPN White Papers

http://www.nstl.com/downloads/NSTL_VPN.pdf

http://www.corecom.com/html/vpn.html

http://www.ennovatenetworks.com/technology/apps/vpnsol/overview.htm

http://www.vpnc.org/white-papers.html

http://www.networkcomputing.com/1111/1111ws2side2.html

Firewall Info

http://www.computerworld.com/search/search?qt=firewall&object.x=21&object.y=10

http://www.networkcomputing.com/search/search?queryText=firewall&sort=date&Find=Find&coll=NWC

http://www.techrepublic.com/search/result.jhtml;jsessionid=4RM4LGMIRKVCYCTEAALCFEY?_DARGS=%2Fsearch%2Fquery.jhtml.5

Vendors

http://www.compaq.com/services/infrastructure/ii_security.html

http://www.checkpoint.com/

http://www.netiq.com/

http://www.antivirus.com/

http://www.verisign.com/

http://www.symantec.com/

http://www.rsasecurity.com/

http://www.iss.net/

A Link to Other Links- wide array of security related issues

http://www.securitymanagement.com/library/000132.html#compsec

List of References

Books

Northcutt, Stephen. Novak, Judy. Network Intrusion Detection An Analyst's Handbook, Second Edition. Indianapolis: New Riders, 2000

Brenton, Chris. Mastering Network Security. San Francisco: Sybex Network Press, 1999

Kaeo, Merike. Designing Network Security. Indianapolis: Cisco Press, 1999

Raptor VPN Server-EC Administrator's Guide. Rockville: AXENT Technologies, 1999

Raptor Firewall-EC Administrator's Guide. AXENT Technologies, 2000

Magazines

Farrow, Rik. "The Forensic Challenge." Network Magazine. May 2001: 114 – 116

Hontanon, Ramon J. "Deploying an Effective Intrusion Detection System." Network Magazine. December 2000: 60 – 67

Moskowitz, Robert. "Let's Get Physical." Network Computing. January 22, 2001: 53

Flint, Jim. "Authenticating VPNs With Radius." Network Computing. July 24, 2000: 81 – 84

Farrow, Rik "Not-So-Secret Passwords." Network Magazine. March, 2001: 116 – 118

Web Sites

http://glreach.com/globstats/index.php3?goto

Ramirez, Charles E. "Cyber Crimes Cost Businesses Billions." The Detroit News. 29 May 2001. URL: http://detnews.com/2001/technews/0105/29/b01-229644.htm (1 Jun 2001)

Lawson, Lorraine. "Could a DDoS attack land you in court? Experts say yes." 5 Apr 2000
URL: http://www.techrepublic.com/article.jhtml?src=search&id=r00520000405law01.htm (4 Jun 2001)

Shipley, Peter. "The Threat from Within –Draft-."
URL: http://www.networkcommand.com/docs/mole.html (11 Jun 2001)

"Firewall Q&A" URL:
http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/reference/firewall1.html*track=internal (5 Feb 2001)

Morrissey, Peter. "Seven Firewalls Fit for Your Enterprise." 15 Nov 1998
URL: http://www.networkcomputing.com/921/921f26.html
(29 Jan 2001)

Vacca, John R. "Firewall-1 Performance/Security Tuning." 18 Dec 2000
URL: http://www.networkcomputing.com/unixworld/1125/1125uw.html
(5 Feb 2001)

Forristal, Jeff and Shipley, Greg. "Vulnerability Assessment Scanners." 8 Jan 2001
URL: http://www.networkcomputing.com/1201/1201f1b1.html
(5- Mar 2001)

Phifer, Lisa. "Virtual Private Networks"
URL: http://www.intranetjournal.com/articles/200009/vpn.html
(2 Mar 2001)

Giorgis, Tadesse Azemar, Ed Farhad, Yavari-Issalou and Victorek, Linda.
"VPNs: Performance, Security and Management for All" Jan, 2000
URL: http://www.nstl.com/downloads/NSTL_VPN.pdf (31 May 2001)

"White Paper IPSec"
URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/eqso/ipsec_wp.htm
(26 Feb 2001)

"IP-BASED VPNS - NEXT GENERATION PUBLIC NETWORK SERVICES"
URL: http://www.ennovatenetworks.com/technology/apps/vpnsol/overview.htm
(9 Mar 2001)

"VPNs: Virtually Anything?"
URL: http://www.corecom.com/html/vpn.html (12 Mar 2001)

"Virtual Private Networks (VPN / PPTP)."
URL: http://www.lfchosting.com/helmig/j_helmig/vpn.htm (5 Jun 2001)

Courses

"SANS Security Essentials" SANS GIAC online.
(April 2001 – present)

"Raptor-EC Firewall, Under the Covers" Compaq's CSC Firewall Support Team.
(12-16 Feb 2001)