Global Information Assurance Certification Paper

ti

SANS

GIAC Certified Firewall Analyst Practical

Version 1.5e

Michael Dennis Pickett

SANS Baltimore 2001

August 15, 2001

Contents

1. ASSIGNMENT #1

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- Customers (the companies that purchase bulk online fortunes)
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes)
- Partners (the international partners that translate and resell fortunes)

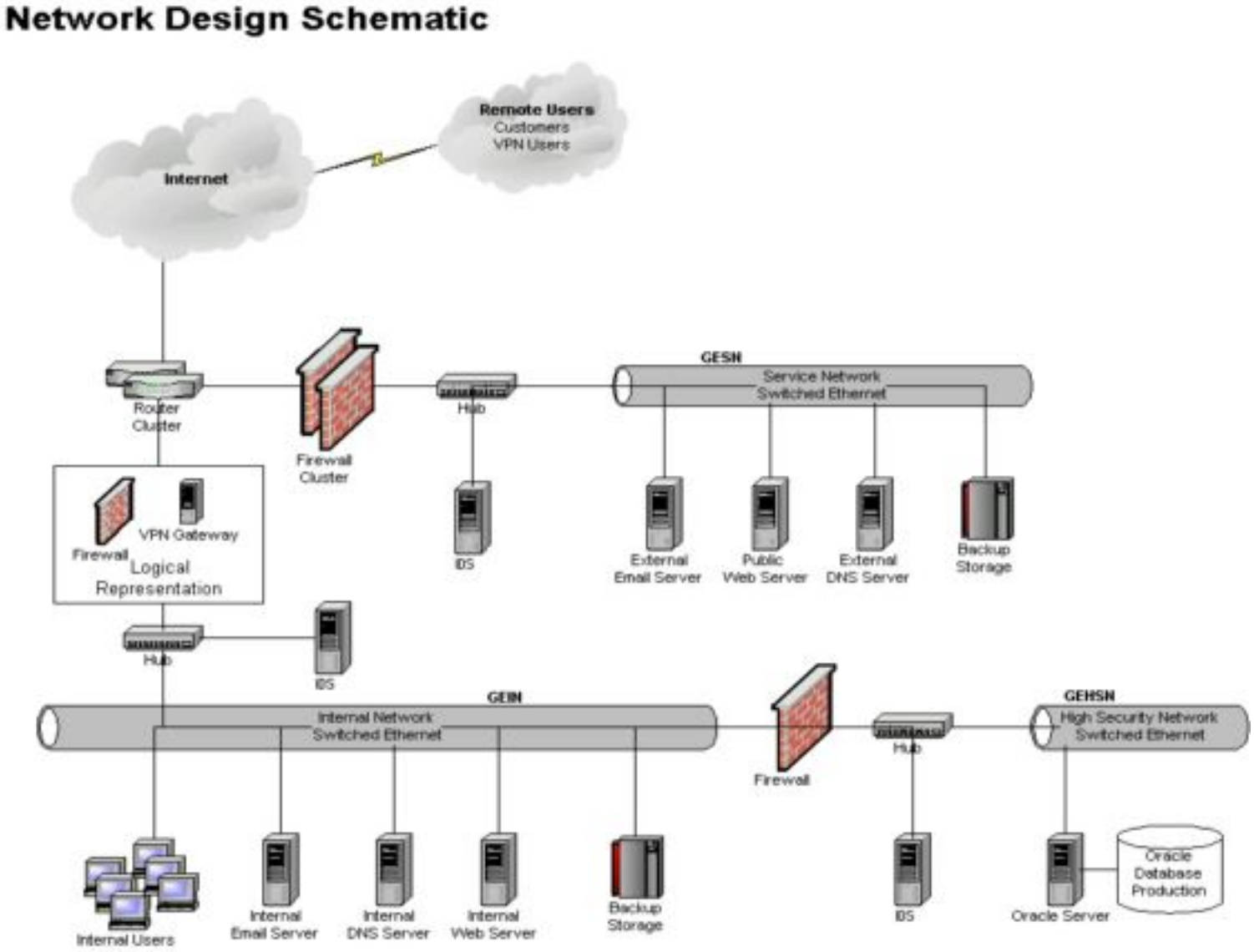
1.1 ASSUMPTIONS

When planning the network architecture for GIAC Enterprises, certain assumptions needed to be made. These assumptions were:

The partners of GIAC Enterprises are trusted people or entities who are to be allowed access via the VPN secure connection into the internal company network. All security related to the partners, once they have established their VPN tunnel, will be handled, via account permissions, according to the company security policy regarding internal employees.

Because of the nature of the fortune cookie saying business, no employees, either on site or off site, need remote access through dial in connections. All remote access is able to be performed through use of the Internet's public infrastructure. If, at a later time, the company requires dial in access, an 800 number, RAS server and modem pool may be implemented.

1.2 DIAGRAM



1.3 PRIORITIES

The GIAC Enterprises network has been designed with three guiding priorities in mind. The first, and most important, is **accessibility** for the individuals and other entities who need information or resources from GIAC Enterprises. The four groups who are expected to need this accessibility are customers, who need to view sample catalogs of fortune cookie sayings, company information and will need to be able to make their purchases electronically. Internal users, who will need standard 'in house' network connectivity. Suppliers, who need to connect in order to supply the fortunes which will be packaged and resold. Partners, who need VPN access through the Internet in order to translate and resell the fortunes.

The second priority, is **security**. People with malicious intent are becoming more and more technologically experienced and will seemingly stop at nothing to compromise a business' infrastructure for their own gains. And, since it's common knowledge how hot the black market is for fortune cookie sayings, the intellectual property that GIAC Enterprises is storing must be protected. In addition to intellectual property, the physical equipment must also be protected from nefarious activity.

Thirdly, while an important consideration it is last in the priority list, is **manageability**. The network for GIAC Enterprises must be one that can be implemented, maintained and monitored with as much simplicity as possible.

1.4 EQUIPMENT

1.4.1 Border Router

In addition to connectivity between networks, including the Internet, the border router provides the first line of defense against the would be attacker. A Pair of **Cisco 3640 Routers using Cisco IOS 12.2** have been chosen to serve these needs. These two routers work together using Hot-Standby Routing Protocol (HSRP) to provide a redundant connections for GIAC Enterprises.

Through the use of access control lists (ACL), the border routers are configured with ingress and egress packet filtering to prevent IP address spoofing (RFC 2827[1] and RFC 1918[2]. As stated in RFC 2827, "All providers of Internet connectivity are urged to implement filtering described in this document to prohibit attackers from using forged source addresses which do not reside within a range of legitimately advertised refixes."[3]

As is standard practice, the external (Internet) network interface on the border router will be configured with a public IP address, while the internal (service network and internal network) interfaces will be configured with a private IP addressing scheme.

---

[1] www.ietf.org/rfc/rfc2827.txt?number=2827

[2] www.ietf.org/rfc/rfc2827.txt?number=1918

[3] www.ietf.org/rfc/rfc2827.txt?number=2827

1.4.2 Firewalls

Ultimate security can never be found in just one device, rather it is a collection of devices, people and policy that ensure a secure infrastructure. With that being said, it is important to note that the most important single device in an infrastructure's security system is the firewall. As GIAC Enterprises is both providing services to the public through the Internet as well as protecting its intellectual and physical property from that same public, the largest percentage of the security budget was spent on the firewall.

There are three firewalls employed at GIAC Enterprises to protect three separate areas of the corporate infrastructure.

1.4.2.1 Service Network Firewall

The most important and most vulnerable area of the network is the service network. Important because it holds the information and machines that customers need access to. Most vulnerable because the machines must be accessible to the public. To protect this area of the network, two **Nokia IP440s** running **IPSO 3.2.1 (IPSO build 13)** have been installed and configured with **Virtual Router Redundancy Protocol (VRRP)** for high assurance and reliability.

> "The Virtual Router Redundancy Protocol (VRRP) enables implementation of hot-standby firewall appliances in a way that is transparent to host systems. Hosts are able to utilize a hot-standby firewall appliance if the primary appliance fails - without the need for any direct host involvement. By combining VRRP with Check Point Firewall Sync, Nokia firewall appliances can be deployed in configurations that support integrated, redundant, hot-standby routing and firewall services. Internet access is virtually guaranteed through an unprecedented combination of redundant Internet links, redundant access routing (through VRRP), and redundant firewalls (through firewall synchronization). "[4]

The Nokia IP 440 employs Check Point's **Firewall-1**[5] firewall software, GIAC Enterprises is running the most current version, **4.0 build 4094**. Firewall-1 provides the company with stateful inspection of network traffic, something that is a necessity for any high assurance infrastructure. For in depth information on Firewall-1's state table refer to Lance Spitzner's "Understanding the FW-1 State Table".[6]

1.4.2.2 Internal Network Firewall

The internal network has been configured to use a single **Nokia IP440 running IPSO 3.2.1 (IPSO build 13)**. If budget allows, a second IP440 using VRRP may be implemented at a later

---

[4] www.nokia.com/securitysolutions/network/availability.html

[5] www.checkpoint.com/products/firewall-1

[6] www.enteract.com/~lspitz/fwtable.html

date. An excellent security practice when using multiple firewalls is to choose different brands for the different units. This sound theory is that an attacker would have a much more difficult time compromising a system if they were confronted with multiple firewalls that, in theory, would never have the same vulnerability at the same time. While at GIAC Enterprises we recognize this as an excellent model, and in fact it will be put into practice for the next firewall to be discussed, it was not implemented for this second network firewall. The reason behind this is twofold. First, this firewall protects a network segment that is not 'behind' the first firewall, its inception is at a separate point on the border router. Therefore, no increased security benefit would be gained by using a different firewall system here. Second, with no security benefit to be gained, our third guiding priority comes into play: manageability. Having this unit the same as the unit protecting the service network allows the IT staff to have to learn and maintain fewer devices. This will save both time and money.

This Nokia IP 440 is configured slightly differently than the same model box that protect the service network. Because this same unit is also GIAC Enterprises' VPN access point, Check Point's **VPN-1 Gateway**[7], an integrated Firewall-1 and VPN-1 solution has been chosen as the IP440's configuration. More details on the VPN configuration in the VPN section of Equipment.

1.4.2.3 High Security Internal Network Firewall

The most valuable GIAC Enterprises intellectual property to be protected is the corporate Oracle database. Because much, if not the majority, of a company's security risk is internal, specific protection specifically designed to protect the production database has been implemented.

> "Administrators say there's no question that internal risks far outweigh external security concerns. FBI statistics back that conclusion. A survey of Fortune 500 companies conducted last year found that most data thefts came from internal users."[8]

In addition to the firewall that rests between the Internet and the internal network, a firewall running **IPTABLES on a Red Hat 7.1** system which uses the Linux 2.4 kernel sits between the internal network and the high security network segment. As discussed in the previous section, there is a sound security practice being employed here by choosing to make this firewall, which sits 'behind' an existing firewall, a different product. The theory is that an attacker would have a much more difficult time compromising a system if they were confronted with multiple firewalls that, in theory, would never have the same vulnerability at the same time.

1.4.3 VPN

As stated in the Firewall section, the VPN access point is the same **Nokia IP440** running **IPSO 3.2.1 (IPSO build 13)** unit that acts as the firewall protecting the GIAC Enterprises Internal

[7] www.checkpoint.com/products/vpn1/gateway.html

[8] www.zdnet.com/eweek/stories/general/0,11011,383857,00.html

Network. By combining both the VPN and firewall functions on the same unit a cost and time savings is achieved. The IP440 uses Check Point's **VPN-1 Gateway** stateful firewall and VPN solution to realize the company's security needs. IPSec[9] will be used to create the VPN pipe. For more information on IPSec reference the IETF's IPSec web site[10].

Remote users who need VPN access to the internal network will have Check Point's **Secure Client**[11] **version 4.1 build 4185 (SP4)** installed on their local machines.

> "VPN-1 SecureClient adds powerful client security features such as access control and security configuration control. VPN-1 SecureClient strengthens the security of the entire corporate network by ensuring that intruders--such as users on shared outside networks--cannot take advantage of an insecure remote client machine to hijack an existing VPN connection into the corporate network." [12]

1.4.4 IDS

Intrusion detection systems have been implemented in the three major network segments. The IDS software being used is **Snort**[13] **version 1.7 on a Red Hat 7.1** system which uses the Linux 2.4 kernel. These Linux machines are configured to run in 'stealth' mode, meaning that they will not actually have IP addresses, increasing the security associated with these machines.[14]

Each IDS machine is attached to a hub that sits on the wire just behind the firewall protecting that segment of the network, but before the switch that guides traffic to specific locations on that segment. This insures that, because a hub is a broadcast device, the IDS box is able to monitor and log all network traffic that passes through each particular firewall. While it is also possible to attach and IDS system to the switch's SPAN port, a hub is used here instead to allow greater flexibility. By using the hub, manageability of connecting, disconnecting and other physical system manipulation becomes easier. Systems that might be attached to a hub such as this would be the IDS systems as well as any infrastructure packet auditing devices of the kind that will be discussed later in this paper.

All logs will be collected and compiled in a central log storage area for security reviews. Reports will be generated in HTML format using SnortSnarf[15].

---

[9] www.ietf.org/rfc/rfc2401.txt?number=2401

[10] www.ietf.cnri.reston.va.us/html.charters/ipsec-charter.html

[11] www.checkpoint.com/products/vpn1/secureclient.html

[12] www.checkpoint.com/products/vpn1/secureclient.html

[13] www.snort.org

[14] www.geocrawler.com/archives/3/4890/2000/9/0/4399696/

[15] www.silicondefense.com/software/snortsnarf/index.htm

1.5 GUIDE

Looking at the GIAC Enterprises network design in a top to bottom flow, one will see that the all outside network traffic, whether it originates from customers, VPN users or a potential attacker, arrives through the Internet at the GIAC Enterprises border router which has three network interfaces active. One is directed to the Internet with a public IP address, the second leads to the GIAC Enterprises Service Network, and the third leads to the GIAC Enterprises Internal Network.

If the traffic is from a customer looking for company information through the web site, the router directs their network traffic through the firewall 'cluster' to the GIAC Enterprises Service Network (GESN) segment. If the network traffic is a VPN connection, the border router passes it to the VPN Server. If the traffic is communication intended for the GIAC Enterprises Internal Network (GEIN) then the border router passes it to the firewall which will then relay it, if it meets the security criteria, on to the GEIN. Although represented in a logical fashion in the network diagram as two separate devices, they are boxed together because both the firewall and VPN are on a single unit. The border router is also responsible for routing communication between the internal network segments when they need to communicate with one another.

1.5.1 Service Network

In the GESN is all the company equipment that needs to be accessible in some fashion to users via the Internet. Because these machines are ultimately vulnerable to attack simply because they must be able to be accessed from the public Internet, they are separated from the internal company network. The end result is that, if one or more of these machines are compromised, the amount of damage that can be done is greatly reduced and, ideally, contained.

The GESN contains an a firewall cluster, detailed in an earlier section, in order to achieve redundant protection. Because the GESN contains the servers which are the company's electronic 'face' to the world, it is vital that they have as little downtime as possible.

After traffic that meets the necessary criteria is passed through the firewall, it is sent to a hub with an IDS server, detailed earlier, attached and then on to the switched GESN Ethernet network. Using switches on the network is not only a performance gain but a security gain as well. Unlike a hub, the switch directs network traffic out specific ports to the correct destination rather than broadcasting all traffic to all ports. Because of this, if a machine was compromised and the intruder attempted to sniff packets on the wire, they would be limited to capturing packets only intended for or sent from the compromised machine. It is because of this same principal that the IDS system is attached to the hub that all traffic that gets past the firewall must pass though. Because a hub broadcasts all traffic, the IDS system will be able to monitor all packets coming over the wire no matter which internal system they are intended for. As detailed earlier in the IDS section, the IDS system is running in stealth mode with no IP address, therefore the likelihood that that machine is the one that might be cracked is greatly reduced.

Also in the GESN is the External Mail Server. This server is a hardened Solaris 8 machine[16] with Qmail running as a mail relay only. The public web server here is an Apache web server running on a hardened Solaris 8 box.

GIAC Enterprises' external DNS server is Bind[17] 9.1.3 running on another hardened Solaris 8 machine. This DNS server handles all of the company's external DNS needs as well as the needs of remote users who wish to access the company's service network computers. In order to protect the external DNS server from attacks, the following configurations have been applied:

- Operate as a master DNS server for the GIAC Enterprises network's public resources
- No information about the GEIN available
- Recursion allowed
- Zone transfers only allowed from ISP's DNS server

Remote administration of this network will be done using Secure Shell[18] (SSH). SSH is widely used for this purpose as it provides a secure connection for generally insecure administration applications.

> "Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels."[19]

There is also a backup storage array on this network segment as an added measure of protection for the company's data.

1.5.2 Internal Network

GIAC Enterprises' Internal Network (GEIN) would be considered the heart of the company. Here is where all of the company's local users have their computers connected. Additionally, all the internal services and needs of those users are provided for by servers on this network segment.

While redundant, because it was detailed in the Service Network section, the following information is relevant to the Internal Network Segment as well: After traffic that meets the necessary criteria is passed through the firewall, it is sent to a hub with an IDS server, detailed earlier, attached and then on to the switched GEIN Ethernet network. Using switches on the network is not only a performance gain but a security gain as well. Unlike a hub, the switch directs network traffic out specific ports to the correct destination rather than broadcasting all

---

[16] Two excellent resources for information and scripts to assist in armoring systems come from Lance Spitzner's site at www.enteract.com/~lspitz/pubs.html, and the YASSP site at www.yassp.org.

[17] www.isc.org/products/BIND

[18] www.ssh.com/products/ssh/

[19] www.onsight.com/faq/ssh/ssh-faq-1.html#ss1.1

traffic to all ports. Because of this, if a machine was compromised and the intruder attempted to sniff packets on the wire, they would be limited to capturing packets only intended for or sent from the compromised machine. It is because of this same principal that the IDS system is attached to the hub that all traffic that gets past the firewall must pass though. Because a hub broadcasts all traffic, the IDS system will be able to monitor all packets coming over the wire no matter which internal system they are intended for. As detailed earlier in the IDS section, the IDS system is running in stealth mode with no IP address, therefore the likelihood that that machine is the one that might be cracked is greatly reduced.

All internal user machines are configured with Norton Antivirus[20]. The company's web site is checked on a regular schedule, as per security policy, so that the .dat files are kept current and are able to offer the best protection possible.

The internal DNS server is a hardened Windows 2000 server configured to use Dynamic DNS. It is configured to serve all the needs of the internal users wishing to access internal resources and to forward to the external DNS server on the GESN those items that it cannot resolve. The following configurations have been applied:

- Only queries from internal GIAC Enterprises clients allowed
- Recursion only allowed for GIAC Enterprises clients
- No zone transfers

The GIAC Enterprises internal web server resides on this segment of the network to provide internal GIAC Enterprises users with any web needs. There is also a backup storage array on this network segment as an added measure of protection for the company's data.

Remote administration of this network will be done using SSH. SSH is widely used for this purpose as it provides a secure connection for generally insecure administration applications.

One thing to note with regard to remote administration in the GEIN: Even if a VPN connection is first established with the GEIN, SSH will still be used to connect and administer the internal servers. The reason that SSH is still needed even though a VPN tunnel will already have been created is because many administration applications pass data in clear text. SSH will wrap all the transmissions in its secure shell protecting it from the prying eyes of internal users.

1.5.3 High Security Network

The GEHSN high security network provides an extremely secure internal network segment on which the company's internal Oracle database resides. The Oracle database is installed on a hardened Solaris 8 machine and is protected by a second firewall of a different brand. This protection is designed to guard against external attacks, attacks from GEIN machines that may have been compromised and GEIN machines that may be used by dishonest employees on the internal network.

[20] www.symantec.com/nav

While redundant, because it was detailed in both the Service Network and Internal Network section, the following information is relevant to the High Security Network Segment as well: After traffic that meets the necessary criteria is passed through the firewall, it is sent to a hub with an IDS server, detailed earlier, attached and then on to the switched GEHSN Ethernet network. Using switches on the network is not only a performance gain but a security gain as well. Unlike a hub, the switch directs network traffic out specific ports to the correct destination rather than broadcasting all traffic to all ports. Because of this, if a machine was compromised and the intruder attempted to sniff packets on the wire, they would be limited to capturing packets only intended for or sent from the compromised machine. It is because of this same principal that the IDS system is attached to the hub that all traffic that gets past the firewall must pass though. Because a hub broadcasts all traffic, the IDS system will be able to monitor all packets coming over the wire no matter which internal system they are intended for. As detailed earlier in the IDS section, the IDS system is running in stealth mode with no IP address, therefore the likelihood that that machine is the one that might be cracked is greatly reduced.

As in the case of the GESN and GEIN, SSH will be used for remote administration of all servers in the GEHSN.

2. ASSIGNMENT #2

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

By 'security policy' we mean the specific ACLs, firewall rule set, IPsec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

2.1 SECURITY POLICY

The GIAC Enterprises security policy comprises a wide range of practices and devices. For the purposes of this assignment several general practices and three specific devices, the border router, primary firewall and the VPN, will be documented.

The IP address structure of GIAC Enterprises is as follows:

Network Device	Net or Host IP
Public IP on Border Router	207.46.230.218
GEIN	192.168.1.x
GESN	192.168.2.x
GEHSN	192.168.3.x
Log Server	192.168.1.98
External Mail Server	192.168.1.10
External Web Server	192.168.1.20
External DNS Server	192.168.1.30
Oracle Database Server	192.168.3.10

2.1.1 General Practices

General practices for the individuals involved in securing the infrastructure at GIAC Enterprises include:

- Daily checks of router log reports
- Daily checks of firewall log reports
- Email checks for updates from the Bugtraq[21] mailing list
- Daily checks of the following web sites for news and information:
  - www.securityfocus.org/frames/index.html
  - www.incidents.org/
  - sunsolve.sun.com
  - www.cisco.com/warp/public/707/advisory.html
  - www.microsoft.com/technet/security
  - www.phoneboy.com
- All confidential email correspondence, whether it is between IT personnel, management or otherwise, must be encrypted and digitally signed using x.509 S/MIME certificates purchased from VeriSign.

2.1.2 Border Router

Unlike the firewall, at GIAC Enterprises the general philosophy, or school of thought, put in practice at the router level is to, by default, **allow** all traffic except what is specifically denied. This router will act as the first line of defense against malicious external activity. By enabling packet filtering we are able to significantly lower the workload placed upon the firewalls. In addition to this, the workload placed upon the IDS systems and those who have to review the firewall and IDS logs is lowered because a large portion of the 'bad' traffic is dropped before it can even reach those internal security units.

When possible, specific IP addresses of individual servers are omitted here for a reason. According to GIAC Enterprises security policy, packets permitted and denied at the border router are considered to be absolute. Meaning, that barring new security news or developments, those entries will almost never change. IP specific entries, which may change as new servers are brought online, maintenance or testing is conducted or old machines are taken off line, will be entered at the firewall level. This provides the IT security staff with ease of manageability because there is only one application, the firewall, that needs to be manipulated on a consistent basis.

The first issues that need to be taken care of have to do with armoring the router itself.

[21] www.securityfocus.org/bugtraq/archive

In order to keep passwords from displaying in clear text and to enable more secure access to command mode, the following commands are added:

```
service password-encryption
enable secret
```

To prevent known and as yet undiscovered vulnerabilities from being used against the router, several unused services will be disabled:

```
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no ip http server
no service finger
no snmp
```

In order to prevent possible hacker reconnaissance and to protect the GIAC Enterprises network from being used in a smurf attack, the following commands are added:

```
no ip unreachables
no ip direct-broadcast
```

If IP's Loose Source Routing were left enabled, it would open the router up to 're-routing' hack attempts.

```
no ip source-route
```

Because security with no way to monitor its effectiveness will quickly be undermined, logging of certain ACL activity will be monitored and logged to a storage server for later review:

```
logging 192.168.1.98
```

Just to make sure it is clearly known that this is a private system, a banner is added:

```
banner / WARNING: This is a private area, no unauthorized access
allowed! /
```

Once the router has been hardened, packet filtering ACLs are put into place. The order in which these entries are listed in the router is extremely important because as soon as a match is found for a packet in question the rule is applied. Because the GIAC Enterprises Cisco 3640 router is using Extended Access Control Lists, the list numbers must be between 100-199. The SANS Top Ten Appendix B reference list has been consulted in construction of these ACLs[22].

Access List 110 is applied to inbound traffic from the internet into the router's serial interface.

[22] www.sans.org/topten.htm

The first lines block all Internet inbound traffic that appears to be coming from invalid or internal IP addresses. There is no legitimate reason for packets with these ip addresses to be coming from outside the internal organization[23].

```
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny ip 10.0.0.0 0 255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.0.255.255 any log
access-list 110 deny ip 207.46.230.2 180.0.255.255 any log
```

The next line denies access to any packets with no ip address.

```
access-list 110 deny host 0.0.0.0 any log
```

Because any users wishing to log in to the network remotely for any type of access are required to do so via the VPN connection, the next lines block external log in attempts using Telnet, SSH, FTP, NetBIOS and rlogin. While there should be no servers running these services and protocols on the internal network, there is always the chance that something will be forgotten or a machine will be misconfigured. With these blocked at the border router, those potential vulnerabilities are sealed.

```
access-list 110 deny tcp any any eq 23 log
access-list 110 deny tcp any any eq 22 log
access-list 110 deny tcp any any eq 21 log
access-list 110 deny tcp any any eq 139 log
access-list 110 deny tcp any any range 512 514 log
```

Because, "Multiple vulnerabilities caused by flaws in RPC, are being actively exploited."[24] the following lines have been added to block those packets which could make use of those exploits.

```
access-list 110 deny tcp any any eq 111 log
access-list 110 deny udp any any eq 111 log
access-list 110 deny tcp any any eq 2049 log
access-list 110 deny udp any any eq 2049 log
access-list 110 deny tcp any any eq 4045 log
access-list 110 deny udp any any eq 4045 log
```

[23] www.ietf.org/rfc/rfc1918.txt?number=1918

[24] SANS Institute manual "2.2 Firewalls 101: Perimeter Protection with Firewalls" Chris Brenton

Because NetBIOS is not a secure protocol, the following lines have been added to block packets containing NetBIOS protocol data.

```
access-list 110 deny tcp any any eq 135 log
access-list 110 deny udp any any eq 135 log
access-list 110 deny udp any any eq range 137 138 log
access-list 110 deny tcp any any eq 139 log
access-list 110 deny tcp any any eq 445 log
access-list 110 deny udp any any eq 445 log
```

Xwindows has several vulnerabilities and is easily misconfigured. Because of this, ports which Xwindows may be listening on are blocked at the border router.

```
access-list 110 deny tcp any any range 6000 6255
```

Only the GESN is available to answer DNS queries or from the public or perform zone transfers with the ISP's DNS server. In light of this, the following lines are added to the border router to allow DNS queries to the service network (permits and denies to specific IP addresses will be handled by the primary firewall which guards the GESN) and block all other DNS related traffic coming in. This will assist in protecting the GEIN from DNS cache poisoning and other possible exploits.

```
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 53
access-list 110 permit udp any 192.168.2.0 0.0.0.255 eq 53
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 389
access-list 110 permit udp any 192.168.2.0 0.0.0.255 eq 389
access-list 110 deny tcp any any eq 53
access-list 110 deny udp any any eq 53
access-list 110 deny tcp any any eq 389
access-list 110 deny udp any any eq 389
```

Only the GESN is available for email queries from the Internet. In light of this, the following lines are added to the border router to allow email queries to be directed to the service network (permits and denies to specific IP addresses will be handled by the primary firewall which guards the GESN) and to block all other email related traffic coming in.

```
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 25
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 109
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 110
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 143
access-list 110 deny tcp any any eq 25
access-list 110 deny tcp any any eq 109
access-list 110 deny tcp any any eq 110
access-list 110 deny tcp any any eq 143
```

Just like DNS and email, only the GESN is available for HTTP queries from the Internet. In light of this, the following lines are added to the border router to allow HTTP queries to be directed to the service network (permits and denies to specific IP addresses will be handled by the primary firewall which guards the GESN) and to block all other initial HTTP request related traffic coming in. Note that all HTTP traffic going to the GEIN is not being blocked because internal users need and will have access to the Internet. Only HTTP traffic which looks for a web server listening on port 80 or 443 will be blocked.

```
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 80
access-list 110 permit tcp any 192.168.2.0 0.0.0.255 eq 443
access-list 110 deny tcp any any eq 80
access-list 110 deny tcp any any eq 443
```

The following line permits packets in that are related to connections established by internal client machines.

```
access-list 110 permit tcp any any established
```

The final line in the access list needs to be added to follow through on the 'allow all except what is explicitly denied' model. This line will essentially override the implicit 'deny all' that exists in any Cisco ACL.

```
access-list 110 permit tcp any any
access-list 110 permit udp any any
```

In order to apply the ACL on the external interface in the inbound direction, the following command will be issued:

```
interface serial 0/0
     ip access group 100 in
```

2.1.3 Primary Firewall

The firewall which is considered the 'primary' firewall at GIAC Enterprises is the one which protects the service network. Because this firewall has the unenviable job of protecting data on machines that are accessible from the public Internet, it is the most difficult to configure. Unlike the router, at GIAC Enterprises the general philosophy, or school of thought, put in practice at the firewall level is to, by default, **deny** all traffic except what is specifically allowed.

Just like the router, the exact order in which the firewall rules are entered is extremely important. As soon as a match is found for a packet in question, the rule is applied and no further rules in the rule base are consulted. For this reason, specific rules and entries are listed first, followed by general rules. While not all of these categories apply to every GIAC Enterprises firewall, (for example, there is no VPN access directly to the GESN, rather, remote access to the service network is gained by establishing a VPN connection to the GEIN and then communicating with the service network), for creation of all firewall rule bases, this excellent basic order of rules has been followed.[25] The specific entries for the primary firewall (Nokia IP 440 running Check Point's Firewall-1 firewall software) are the ones which will be detailed in this section of the assignment.

1. Firewall Administration
2. Stealth rule
3. Syslog rule
4. Network Administration
5. Internal Connectivity
6. Inbound email
7. Inbound Web/FTP traffic
8. Load Balancing
9. VPN
10. Client encrypt
11. Reject restricted sites
12. DNS queries and zone transfers
13. Block chatty protocols
14. Protect Networks
15. Anti-Virus
16. Block anything outbound
17. Cleanup Rule

Excellent advice which will be followed when implementing the GIAC Enterprises firewall can be gained from Brian M. Kelly's GIAC firewall certification paper. In it he states, " A good rule

[25] The basis for this of rules has been taken from: Martin, Daniel S. "GIAC Certified Firewall Analyst Practical." March 28, 2001

for implementing rules on a firewall is to implement one rule at a time and then test out the connectivity for each server or device…This allows for a more manageable approach and a chance for security to be checked at each point in the process."[26]

Firewall Administration

The very first firewall rule to be set up is the one which will allow the IT security personnel to administer the firewall itself.

Source	Destination	Service	Action	Track	Install On	Time	Comment
Admin Consoles	Mgmt Consoles	Firewall-1	Accept	Long	Gate_GISN	Any	Firewall Admin Access

Stealth rule

By implementing the Stealth Rule, the firewall will become a virtually undetectable object. This technique is not foolproof, however it does greatly enhance the security of the firewall machine itself by disallowing, by dropping packets directed to the firewall, direct contact with the firewall machine itself. In this case, the firewall protecting the GESN is defined as 'Gate_GESN.'

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	Gate_GESN	Any	Drop	Long	Gate_GISN	Any	Stealth Rule

Syslog rule

In order to maintain a centralized logging area for data gathered by the border router, firewalls and IDS systems, the following rule will allow all predefined log generating objects, defined as 'Loggers', to pass traffic to the log server, defined as 'Log_srv'. The log server itself resides on the GEIN which means that the most important firewall security surrounding that device is the firewall protecting the GEIN. For ease of manageability however, the same logging rule is defined in all GIAC Enterprises firewalls.

Source	Destination	Service	Action	Track	Install On	Time	Comment
Loggers	Log-srv	Syslog	Accept	Long	Gate_GISN	Any	Logging

[26] Kelly, Brian M. "GIAC Firewall And Perimeter Protection Curriculum Practical Assignment." April 2, 2001

Network Administration

In order to allow remote administration of the GESN servers, a rule must be defined to allow that type of network traffic to pass. All remote administration traffic originating from the GEIN is considered secure providing it complies with the company security policy requiring remote administration traffic to be encrypted using SSH.

Source	Destination	Service	Action	Track	Install On	Time	Comment
Net Admins	SSH_Servs	SSH	Accept	Long	Gate_GISN	Any	Email IN

Internal Connectivity

This rule allows all users of the GEIN to communicate with machines on the service network for development, testing and other day to day functions. The border router will have dropped all 'spoofed' packets that attempt to enter the network from the Internet posing as internal communication. Therefore, internally addressed packets are considered authentic.

Note that all traffic from the internal network directed to the primary firewall protecting the service network is considered secure but this does not hold true for the reverse situation. Traffic from the service network, which is inherently more vulnerable than the internal network, is considered suspect and will be guarded against on the secondary firewall protecting the internal network.

Source	Destination	Service	Action	Track	Install On	Time	Comment
GEIN GESN	GESN GEIN	Any	Accept	Long	Gate_GISN	Any	Internal Connectivity

Inbound email

This rule allows connectivity, for email related protocols only, to the external email server, defined as 'Mail_rly'. Antivirus and any other email scanning is performed at the email server itself.

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	Mail_rly	imap pop3	Accept	Long	Gate_GISN	Any	Email IN

Inbound Web/FTP traffic

This rule allows connectivity, for web related protocols only, to the external web server, defined as 'Web_srv'. FTP traffic is not defined at the primary firewall because all valid FTP traffic will be coming from the internal network, and will have been allowed via the Internal Connectivity rule, from either local users or VPN connected users. No public FTP server exists at GIAC Enterprises.

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	Web_srv	http https	Permit	Long	Gate_GISN	Any	Web IN

DNS queries and zone transfers

The DNS rules put in place on the GESN insure that all external DNS queries are only allowed to the external DNS server, defined as 'DNS_ext'. Bind itself will insure that zone transfers are only done between itself the ISP's DNS server.

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	DNS_ext	dns	Accept	Long	Gate_GISN	Any	DNS queries

Cleanup Rule

While the Cleanup Rule is not inherently necessary because Firewall-1 will, by default, drop any packets which aren't specifically permitted, in order to log this data the rule must be in place.

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	Any	Any	Drop	Long	Gate_GISN	Any	Cleanup

2.1.4 VPN

The GIAC Enterprises corporate Virtual Private Network (VPN) allows partners and other trusted remote users to access the internal network from off site locations, including international off site locations, through use of a generic connection to the public Internet. Despite security risks, which will be outlined presently, there are several benefits to using the Internet for business communications.

The first benefit is convenience. by using the Internet to allow remote users to communicate, direct dial services to GIAC Enterprises are not a priority, and may be eliminated altogether. In fact, individual phone lines and modem banks, which were previously used to allow remote access to the local network, may become a thing of the past. The administration of the hardware, user authentication systems, whether they be RADIUS or otherwise, and the RAS services can be purged from the infrastructure. The second advantage of the VPN through the Internet is found in cost savings. The removal of all the previously mentioned equipment and man hours associated with maintaining that equipment saves the company a great deal of money when compared to the cost of implementing the VPN.

The reason the creation of a VPN tunnel is necessary is because all traffic that moves across publicly accessible areas can conceivable to be intercepted. Interception of this data could lead to loss of intellectual property or, perhaps even more troublesome, possible alteration of this data before it is allowed to continue on to its destination.

In order to achieve private communications over public space, the data being transferred must be encrypted before it enters that space and decrypted after it has left that space. In the case of GIAC Enterprises, Check Point's Secure Client application will be installed on all potential remote user's computers. This application will insure that, once configured, all communication directed towards the GIAC Enterprises Internal Network is encrypted using IPSec protocols. Decryption will take place at the VPN server and from there the network traffic will travel the internal network 'in the clear.' This particular method of VPN data exchange is called, 'Transport.' Transport is being used because this is a host to server VPN connection as opposed to a server/router to server/router connection.

IPSec allows use of the Authentication Header (AH) and Encapsulation Security Protocol (ESP). Both will be implemented for GIAC Enterprises VPN solution. Although by adding an authentication header to the packet AH would provide several security benefits such as: data origin authentication, connectionless integrity, high authenticity/integrity assurance, there are drawbacks which will prevent it from being implemented. AH mandates DES as it's encryption algorithm and this may not be exportable to many countries where GIAC Enterprises partners will be traveling in their never ending quest for the most accurate and insightful fortune sayings. Additionally, because AH adds a new header to the packet, it does not work with Network Address Translation (NAT). ESP will be used because it offers many of the same security features: confidentiality, data origin authentication (except for IP header), connectionless integrity, protection against replay attacks and limited traffic flow confidentiality. It does this by wrapping much of the packet, not the IP header, in an encrypted payload.

Because many of the VPN users will be connecting from outside of the United States, encryption export laws need to be taken into consideration[27]. Higher levels of encryption are illegal to export outside of the U.S. As such, in order to provide the highest level of security for all users, two groups of VPN users will be created. The first will be 'VPN_Dom' for domestic users. This group will be able to use the 3DES (or triple DES) encryption algorithm during their VPN connection. The other group will be 'VPN_Int' for international users. The highest level of encryption afforded them will be RC2-40. This is not an ideal situation, but, for the current times, it is the best available.

Once the security policy has been put in place, the VPN server, in this case also the secondary firewall server, must have the proper rules in its rule base in order to allow these separate groups of remote VPN users to connect. There will need to be two connection types allowed for each group. The first will override the Stealth Rule for the VPN users. This will allow them to communicate with the firewall server in order to download their security policy. The second rule will actually encrypt and log traffic from the VPN session.

Allow Policy Download

Source	Destination	Service	Action	Track	Install On	Time	Comment
VPN_Dom VPN_Int	Gate_GEIN	Firewall-1	Accept	Long	Gate_GEIN	Any	Encrypt VPN Traffic

Allow Domestic Encryption

Source	Destination	Service	Action	Track	Install On	Time	Comment
VPN_Dom	GEIN	Any	Client Encrypt	Long	Gate_GEIN	Any	Allow domestic VPN

Allow International Encryption

Source	Destination	Service	Action	Track	Install On	Time	Comment
VPN_Int	GEIN	Any	Client Encrypt	Long	Gate_GEIN	Any	Allow International VPN

[27] www.bxa.doc.gov/Encryption/Default.htm

3. ASSIGNMENT #3

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

- Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
- Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
- Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

3.1 ASSESSMENT OVERVIEW

At this point in the GIAC Enterprises infrastructure design and implementation everything is in place and is expected to be offering a varying degrees of protection for the three different areas of the network, the GESN, GEIN, and GEHSN. While the internal IT team may have all the confidence in the world that this is actually happening, the only way to be absolutely certain that the expected level of protection is actually being achieved is to conduct an analysis, or audit of the security infrastructure. In this situation, GIAC Enterprises will hire an outside company, Secure Your Systems Inc. (SYS), to work with the internal team to provide an independent examination of the GIAC Enterprises security system. (Note: this is a fictional company name, if I have accidentally named an actual existing company, any information or opinions expressed in this paper about the company are not directed towards any existing organization. [Got to love disclaimers, better safe than sorry.])

3.2 ASSESSMENT PLAN

The assessment will take place in three parts: The first part will consist of an evaluation of the perimeter defenses. The testing will take place on a Sunday morning, according to network logs this is the time of least external and internal network activity so any significant rise in network usage will have the least impact possible on normal business activity.

The perimeter evaluation, or External Assessment, is designed with the external hacker in mind. The tools used and procedures followed[28] will all be utilized with the expectation that an attack is

[28] While the tools used in the assessment and popular within the industry in and of themselves, my inspiration for use of this exact combination came from the excellent paper: Zeltser, Lenny. " Firewalls, Perimeter Protection, and VPNs " February, 2001

originating from outside the GIAC Enterprises infrastructure. The tests will primarily determine two things. First, they will show whether or not the perimeter defenses set up are blocking expected malicious traffic. Second, the tests will show whether or not there are additional vulnerabilities that were not originally prepared for.

The second part of the assessment involves testing internal defenses. The premise for these tests will be, "What if one of the machines behind the border router and firewall were to be compromised?" There are a variety of tools that hackers will install and activities that they will perform to not only solidify their hold on the company systems, but also to use the internal systems to launch attacks on other companies.

This part of the assessment, the Internal Assessment, will take place during two separate times. First, when possible, Sunday morning work will be done for the same reasons that the External Assessment used that shift. Some of the testing though, will be performed during normal business hours. A typical shift, Wednesday at 2:00pm, has been chosen to represent a day and time during the week when typical network activity may be observed and analyzed.

The final part of the assessment is the Recommendations portion. This will consist of a final report that SYS will prepare and present to the both the IT security team as well as upper management of GIAC Enterprises. This report will first summarize and then detail the work that was performed, how it was performed, what it tested for and finally, what steps can be taken to rectify any security deficiencies that were discovered and what steps may be taken in a proactive, preventative manner against possible future attacks.

The level of effort is expected to consist of:

Company	Personnel	Total Hours	Cost per hr.
GIAC Enterprises	2	48	$60
SYS Inc.	3	240	$80

3.3 EXTERNAL ASSESSMENT

In order to perform the External Assessment, a three tiered, layered approach will be taken.

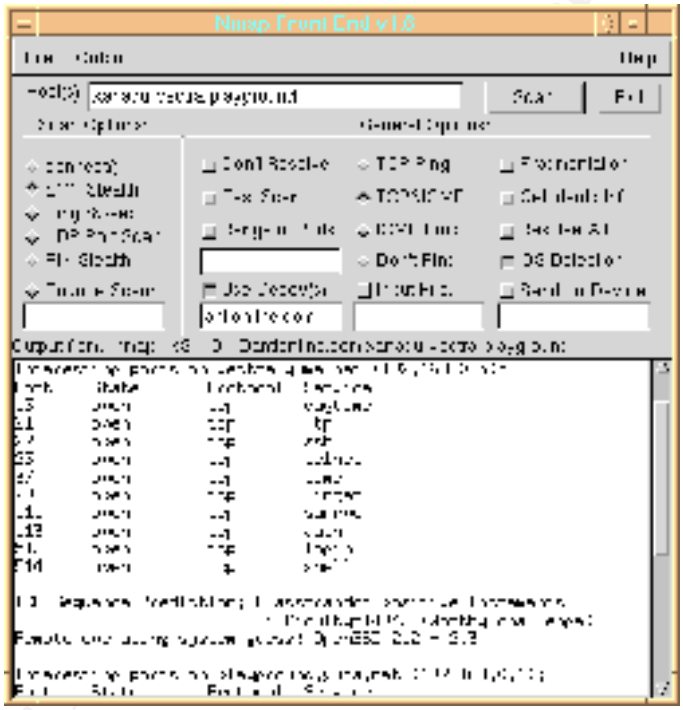
Layer 1	Port Scan
Layer 2	Vulnerability Probe
Layer 3	Sniffer Data Analysis

For the Layer 1 Port Scan, the testing team will be armed with two pieces of information that could easily be obtained by any attacker. The team will have the domain name of GIAC Enterprises and the IP addresses of all publicly accessible servers. The tool to be made use of in

this first test will be Nmap[29]. Nmap is an extremely useful, free application which will is often put to malicious use by individuals wishing to get reconnaissance data on a company's systems.

> "Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics." [30]

Below is an image of the Nmap front end being put to use.[31]



By using Nmap, a list will be generated showing which ports on GIAC Enterprise machines are available to be accessed from the Internet. The will ideally show that the only ports accessible are those which are meant to be available and are primarily located on the GIAC Enterprises Service Network. Nmap will confirm or deny this assumption and will also locate and list additional ports which, for whatever reason, are also accessible from the Internet. Once these ports are identified and documented, the next layer of analysis will take place.

---

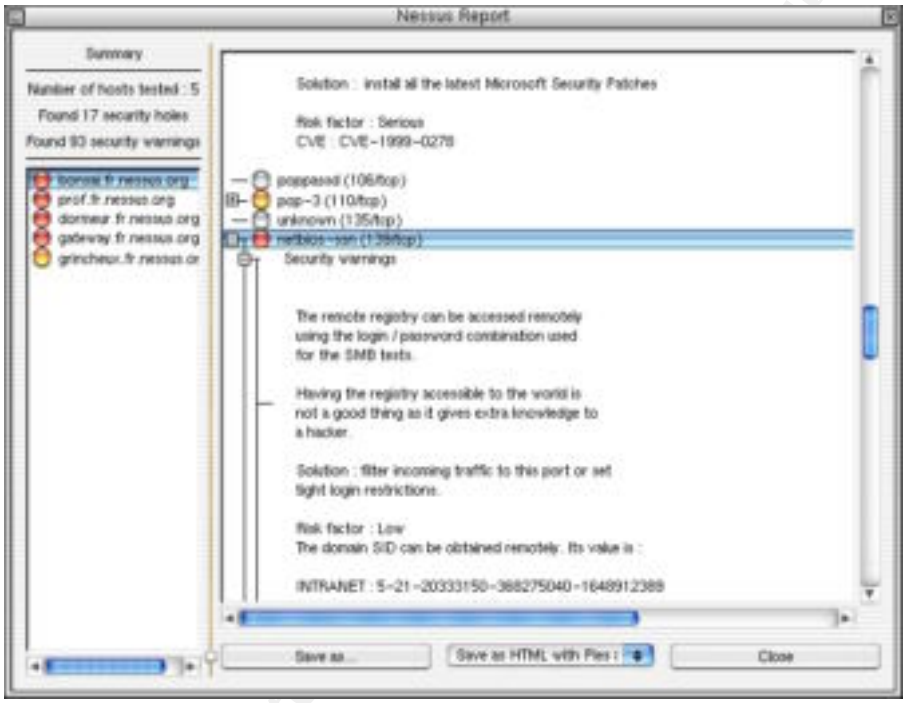
[29] www.insecure.org/nmap

[30] www.insecure.org/nmap

[31] Nmap image taken from Nmap web site, www.insecure.org/nmap

The Layer 2 Vulnerability Probe is designed to attack ports that have been identified by Nmap as being available for access. The tool that will be used is Nessus[32]. Nessus is a free, security scanner application, "which will audit remotely a given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way."[33]

Below is an image of a Nessus test results screen.[34]



By making use of Nessus, a clear understanding of what vulnerabilities exist on the open ports will be gained. It is certainly possible to test all ports for all vulnerabilities manually, however the time involved and risk of human oversight or other error is too great to make it practical. The results of this test will produce a list of security hole repair action items that will be prominently featured in the final report.

The Layer 3 Sniffer Data Analysis is the final phase of the external examination. Normally sniffers are installed on a system within the network, and in the Internal Assessment that's exactly what will be done during this Layer of the test. In this case, the attack and sniffing is occurring externally. Sniffing can still be performed from the outside of the network, although the data attempting to be gathered is not what would be looked for if the sniffer logs came from

[32] www.nessus.org

[33] www.nessus.org

[34] Nessus image taken from Nessus web site, www.nessus.org

an internal system. From the outside all that can be sniffed from a typical computer would be communication directed between a GIAC Enterprises' server and an external user.

During the External Assessment, special care will be taken to analyze the GIAC Enterprises web server. Because the web server is an integral part of the business and is accessible through the Internet, its security is of primary importance. In this case the application Achilles[35] will be used to monitor HTTP traffic passed between the GIAC Enterprises Web Server and an external test machine. Achilles, "is a tool designed for testing the security of web applications. Achilles is a proxy server, which acts as a man-in-the-middle during an HTTP session." By using this application, the opportunity to examine exactly what data is passed between client and server as well as the opportunity to alter and send unexpected data back to the server is afforded the test team. By sending unexpected data to the web server, the team will be able to test its limits and see if the server either fails or returns unallowed confidential information of any kind to the external machine.

3.4 INTERNAL ASSESSMENT

The Internal Assessment will take place in much the same manner as the External Assessment. A layered, or tiered, approach will be used and many of the tools used will be the same. What is different about this assessment are the target systems and the goals of the probes and test attacks. This analysis is attempting to determine whether or not GIAC Enterprises' servers which lie behind the perimeter defenses are as hardened as they are expected to be. The results of the testing will determine if the expected hardening measures taken are correctly guarding those exploits that have been planned for. The tests will also probe to determine if exploits that haven't been planned for exist and are vulnerable.

In order to perform the External Assessment, a four tiered, layered approach will be taken.

Layer 1	Port Scan
Layer 2	Vulnerability Probe
Layer 3	Brute Force Attempt
Layer 4	Sniffer Data Analysis

In light of the fact that layers one and two will be using identical tools and will be performed in much the same way as they were in the External Assessment, for brevity's sake their descriptions will be omitted here.

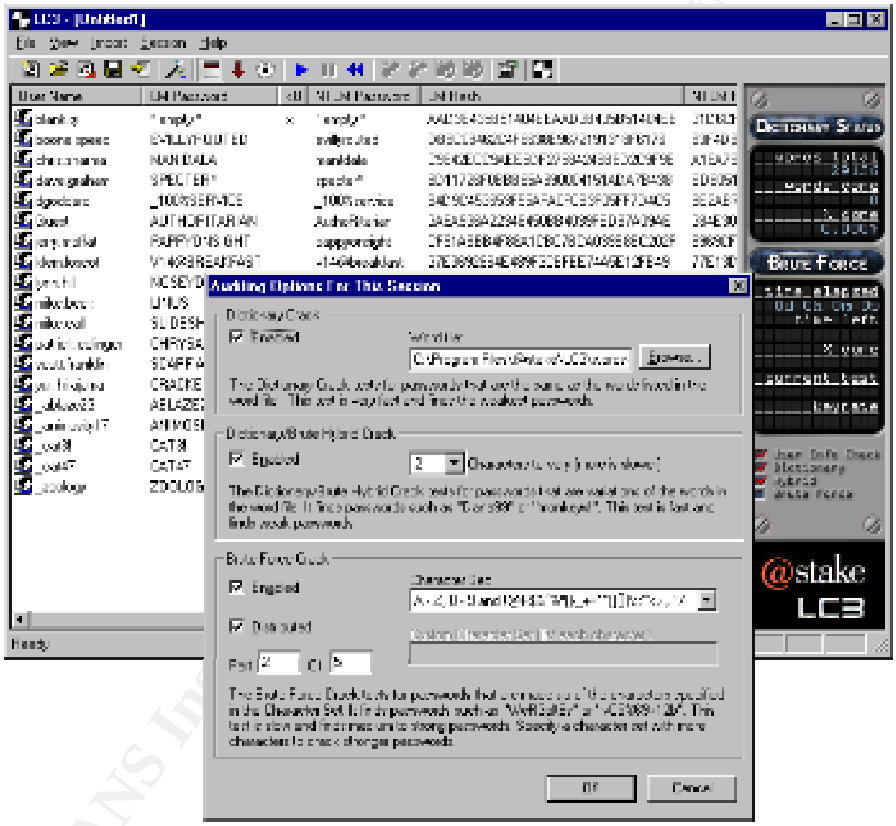
The Layer 3 is a Brute Force Attempt at an attack. A brute force attempt is where no subtlety or stealth of any kind is used in the attack. Typically a brute force attack consists of an attacker

[35] www.digizen-security.com/projects.html

using a tool, in the case of this assessment the tool to be used will be L0phtCrack,[36] also known as LC3.

> "LC3 can obtain encrypted passwords from stand-alone Windows NT and 2000 workstations, networked servers, primary domain controllers, or Active Directory, with or without SYSKEY installed. LC3 can even sniff encrypted passwords from the challenge/response exchanged when one machine authenticates to another over the network." [37]

Below is an image of a L0phtCrack configuration screen.[38]



The L0phtCrack application will be to audit passwords, particularly administrator passwords used on the GIAC Enterprises servers. By having L0phtCrack attempt to crack a server password

[36] www.atstake.com/research/lc3/index.html

[37] www.atstake.com/research/lc3/index.html

[38] L0phtCrack image taken from @stake web site, www.atstake.com/research/lc3/index.html

database, the testers can determine if the passwords being used comply with the standards laid out in the company's security policy.

The Layer 4 Sniffer Data Analysis testing will use the tool tcpdump.[39] This tool will be used with the –w switch in order to capture all manner of network data that travels within the GIAC Enterprises network and to write it to a file. For the purposes of the analysis, tcpdump will be installed on servers located off of the hubs to which the IDS systems are attached. Because these hubs broadcast all traffic, expected and unexpected, that penetrates the respective firewalls that they sit behind, they are ideal locations to attach a packet sniffer.

By sniffing, logging, and analyzing the traffic penetrating the firewalls, the assessment team can determine if data being passed is exposing any critical or confidential information that should otherwise be kept concealed.

An important point to note is the differences between the sniffer and the IDS systems that are already in place, attached to the aforementioned hubs and are already logging and analyzing network traffic. While the IDS systems gather their data in a similar manner to a network sniffer like tcpdump, the goal of the IDS system is a different one than that which the assessment team has when using the sniffer. The IDS systems are analyzing traffic for possible attacks, malicious code, and generally unexpected packet content that enters beyond the GIAC Enterprises perimeter defenses. The goal of the analysis team using the sniffer is to determine if normal, expected, everyday network traffic is revealing more information than is necessary or safe.

3.5 RECOMMENDATIONS

At the conclusion of the security audit, SYS will prepare a final report to be delivered to GIAC Enterprises IT security staff as well as upper GIAC Enterprises management. This report will summarize and detail all work and how it was carried out. Interpretations of the results, including what vulnerabilities exist and recommendations as to how to close the security holes will be included.

Some recommendations included in this report include:

> **Encryption of stored data:** While a strong perimeter defense and hardened internal systems will ideally protect against all intruders, an additional layer of security is possible. This layer would include encryption of data once it is in storage on a file or database server. Encryption of this data would guard against the intruder who has already compromised an internal system as well as any dishonest internal users who may wish to steal and sell the information on the lucrative fortune cookie sayings black market. Once data is encrypted in storage, simply being able to gain access to the information is no longer the last hurdle an

[39] www.tcpdump.org

attacker must surmount. Decryption IDs and passwords, or x.509 PKI certificates would also become necessary in order to view the contents in unencrypted form.

Stronger client validation: Stronger client validation at the company web site could be achieved through use of personal digital x.509 certificates. These certificates use Public Key Infrastructure (PKI) technology and would need to be installed on every individual client system that wishes to access the GIAC Enterprises web site. This is a recommendation that would be optional to institute. By requiring a more secure method of validating clients at the company web site GIAC Enterprises gains a greater degree of security at one of the more vulnerable servers. However, this added security comes at a price. That price would be increased overhead and complexity which may actually drive existing and potential future customers away.

QoS to guard against DOS and DDOS attacks: Currently the GESN is vulnerable to the effects of a Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks that will starve bandwidth. Two recommendations to guard against these attacks would be: One, disallow all ICMP echo requests at the border router. This will insure no ping replies will enter the GIAC Enterprises infrastructure. Two, implement a Quality of Service (QoS) feature at the border router level of the design. This will allow bandwidth to be shaped manually. The GIAC Enterprises IT staff will be able to allocate exact percentages of bandwidth to exact needs. If no more than 20% of bandwidth is allowed to respond to ICMP echo requests then no matter how many request come in, 80% of the network bandwidth will always be available for other network traffic.

4. ASSIGNMENT #4

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

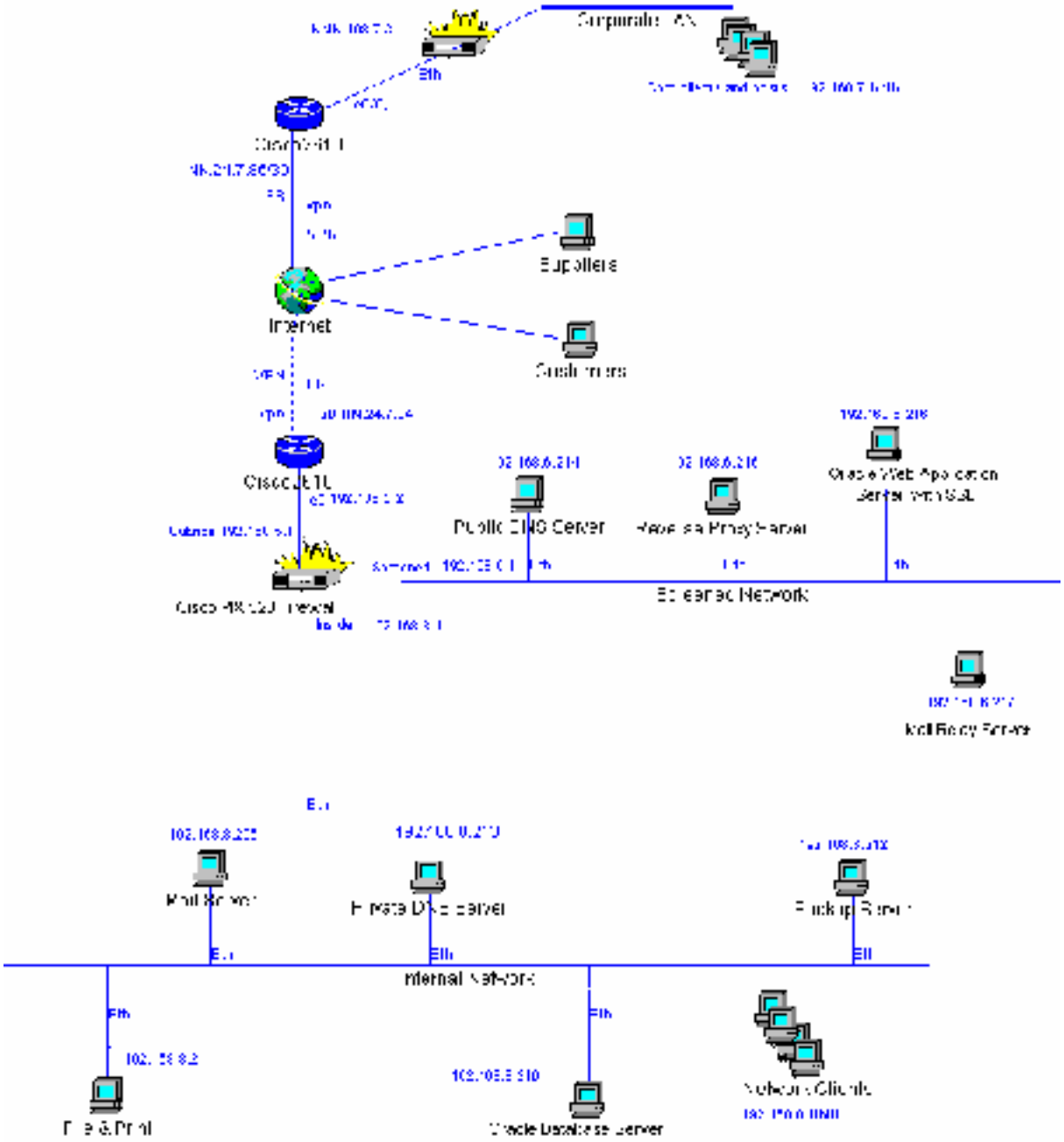
- An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
- A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
- An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

4.1 INTRODUCTION

To conduct the "Design Under Fire" analysis, the paper written by George Stanton, who attended the NS2000 Conference in Monterey CA, will be used. The link to this paper is: http://www.sans.org/y2k/practical/George_Stanton_GCFW.doc. Because the paper is well thought out and very thorough, it affords an opportunity to point out specific vulnerabilities in the design. I would like to point out that George's paper is an excellent one, it was chosen for it's thoroughness, not the lack thereof. As the stated point of this exercise is to show that there are no "silver bullets" that will solve all infrastructure security issues, even a very good design like Mr. Stanton's has vulnerabilities.

One thing that is vague in the paper is the OS used in the Cisco 2610 border router and the PIX 520 firewall. Because this has been omitted, for the purposes of this exercise we will assume that all vulnerabilities that were available in 2000 will be available to be exploited.

George's network design diagram is shown below:



4.2 ATTACK AGAINST FIREWALL

The Cisco PIX firewall solution is generally an outstanding one. It is able to guard against almost all unwanted traffic and will do a fine job, if configured correctly, of protecting internal systems from attack. While there have been very few exploits available for the PIX, they do appear from time to time:

From the Security Focus web site:

Cisco PIX Vulnerabilities listing, August 18, 1998:

> http://www.securityfocus.com/bid/690
>
> "Both the Cisco PIX Firewall software as the Context-based Access Control (CBAC) feature of Cisco's IOS Firewall Feature Set do not properly check non-initial fragmented IP packets. Although the non-initial fragmented IP packets might belong to session which would normally be blocked, they are forwarded to the destination host. This may lead to a denial of services (DOS) attack due to the exhaustion of resources required to keep track of the fragmented IP packets."

Cisco PIX Vulnerabilities listing, October 03, 2000:

> http://www.securityfocus.com/bid/1877
>
> "It is possible to configure the PIX so that it hides the IP address of internal ftp servers from clients connecting to it. By sending a number of requests to enter passive ftp mode (PASV) during an ftp session, the IP address will eventually be disclosed. It is not known what exactly causes this condition."

In order to launch an attack directly against George Stanton's PIX 520 firewall as it was configured in year 2000 when his design was created, a Denial of Service vulnerability would be the most likely exploit to take advantage of.

From Security Focus Cisco PIX Vulnerabilities listing:

DOS vulnerability in PIX, April 06, 2001

> http://www.securityfocus.com/bid/2551
>
> "A problem with the PIX could allow a denial of service. PIX firewalls using TACACS+ are vulnerable to a resource starvation attack which results in a denial of service. Upon receiving multiple requests for TACACS+ authentication from an unauthorized user, the firewalls resources can be exhausted. This causes the firewall to crash, requiring power cycling to resume regular service. This makes it possible for a user from either the public or private side of the PIX to crash the firewall, and deny service to legitimate users."

As stated in the description, the result of an attack launched in the manner would cause the firewall to crash. Not only would this deny service to all users attempting to pass packets through the firewall in either direction, it would require cycling power on the firewall unit in order to bring service back online.

4.3 DENIAL OF SERVICE ATTACK

During a denial of service attack, an attacker will attempt to flood the target with an overwhelming amount of data that will then prevent legitimate network traffic from being able to travel to its destination. This is done by compromising multiple intermediary systems which are used to generate the data streams directed at the target system.

While George Stanton's network design does provide a great deal of protection against a Denial of Service attack by disallowing ICMP echo replies with the ACL line, "access-list 101 deny icmp any any echo-request," there is very little that can be done to guard against bandwidth starvation. Even with the ICMP filtering that Mr. Stanton has in place, the amount of data that his border router would have to deal with can ultimately occupy all his available bandwidth.

The bandwidth starving DOS attack can be made even more damaging by turning it into a Smurf Attack.

> "In the "smurf" attack, attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. There are three parties in these attacks: the attacker, the intermediary, and the victim (note that the intermediary can also be a victim)."[40]

The most effective way to stop a Smurf Attack is by eliminating the intermediary systems from the equation. The only ones of course who can do this would be the operators of these intermediary systems. One way to see if your own system is able to be used as an intermediary is by checking it at the Smurf Amplifier Registry[41] (SAR).

The best option remaining for guarding against all manner of DOS attacks is to implement the Committed Access Rate (CAR) functionality that is supported by several Cisco routers or implement any other system that provides some manner of QoS service. This functionality will allow bandwidth to be shaped manually. The IT staff will be able to allocate exact percentages of bandwidth to exact needs. If no more than 20% of bandwidth is allowed to respond to ICMP echo requests then no matter how many request come in, 80% of the network bandwidth will always be available for other network traffic.

[40] www.cert.org/advisories/CA-1998-01.html

[41] www.powertech.no/smurf

4.4 ATTACK AGAINST INTERNAL SYSTEM

The most commonly attacked component of any infrastructure these days is the web server. They must be accessible to the outside world and will frequently be using a public IP address which allows for easy reconnaissance. In the case of George Stanton's web server, he is making use of Network Address Translation (NAT) which means that the IP address of the web server is in effect, 'hidden' from prying eyes. Despite the use of NAT, because the web server is still accessible to the public, it is easily attacked.

In order to compromise the Oracle Application Server, a Buffer Overflow Attack could be executed using the following exploit:

From Security Focus Oracle Application Server Vulnerabilities listing:

Boundary Condition Error in Oracle Application Server, April 11, 2001

> http://www.securityfocus.com/bid/2569
>
> "The shared library 'ndwfn4.so' that ships with Oracle Application Server is vulnerable to a buffer overflow. The library is used to handle web requests passed to it by the iPlanet web server. If the library is sent a request longer than approximately 2050 characters, it will overflow. A request string could be constructed to trigger the overflow and allow a malicious remote user to execute unprivileged arbitrary code. "

By creating code that will take advantage of this vulnerability, an attacker would essentially be able to execute their own code on the remote system. The firewall and border router would be expected to allow this type of traffic through because, as far as the packets go, they appear legitimate.

The execution of this code would ideally lead to a toolkit of some kind being installed on the target system And, with a toolkit installed an attacker would be able to perform additional reconnaissance from within the company's secure perimeter. The attack could theoretically continue using that reconnaissance information in many different ways. One of these ways might be to sniff packets being passed on the network to attempt to identify accounts and passwords. Another plan an attacker might be interested in pursuing would be to deface the web site. Still another might be to attempt to obtain access to, and download, the UNIX password file. Once downloaded locally on an attackers machine they would have time to crack the encrypted file without worrying about bandwidth usage or detection. An application like L0phtCrack could be used to attempt this forced decryption.

For a more detailed description of a Buffer Overflow attack, refer to the article, "The Tao of Windows Buffer Overflow" at www.cultdeadcow.com/cDc_files/cDc-351/page2.html, authorship is credited to DilDog. While the article itself is aimed squarely at creating Windows buffer overflows, the descriptions and explanations of a buffer overflow are applicable in to environment.

5. ADDITIONAL RESOURCES LIST

SANS GIAC Papers

Martin, Daniel S. "GIAC Certified Firewall Analyst Practical." March 28, 2001

Zeltser, Lenny. " Firewalls, Perimeter Protection, and VPNs." February, 2001

Kelly, Brian M. "GIAC Firewall And Perimeter Protection Curriculum Practical Assignment." April 2, 2001

Stuckless, Colin "SANS GIAC Firewall and Perimeter Protection Practical Assignment." September 24, 2000

Orebaugh, Angela D. "Firewalls, Perimeter Protection, and VPNs." February 20, 2001

Web Sites

ITA-HSR Lab Firewall site at http://www.ita.hsr.ch/nws/labs/firewall.html

INFOSYSSEC: http://www.infosyssec.org/infosyssec/firew1.htm

Books

All SANS Track 2 "Firewalls, Perimeter Protection, and Virtual Private Networks" course material