Global Information Assurance Certification Paper

SANS GIAC TRAINING and CERTIFICATION
Level Two Firewalls, Perimeter Protection and VPNs
Practical Assignment

Mary Anthes

SANS New Orleans
January 28 – February 1, 2001

TABLE of CONTENTS

Assignment 1 - Security Architecture (25 Points)

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).

In preparing the security architecture for GIAC Enterprises, the following assumptions were made regarding the organization:

- GIAC Enterprises will have dedicated IT Security Staff to implement and administer their security architecture
- This assignment is concerned with the perimeter network security and will not consider physical security or disaster recovery, though a complete security plan would include those items.
- Anti-virus protection will also not be discussed. However, a thorough security policy will provide for anti-virus software at the desktop, server, mail server and firewall level. This software must be updated as frequently as possible.

Multiple groups of users with different needs will be accessing GIAC Enterprises resources and services. Assumptions and parameters about each group are listed below:

- Customers are companies that will buy the fortunes. They will make their purchases through secure web servers running http and https with digital certificates. The customer database will be located in a separate subnet protected by another firewall.

- GIAC suppliers will upload their fortunes through another set of secure web servers running http and https. Supplier databases will also be located in a separate subnet.

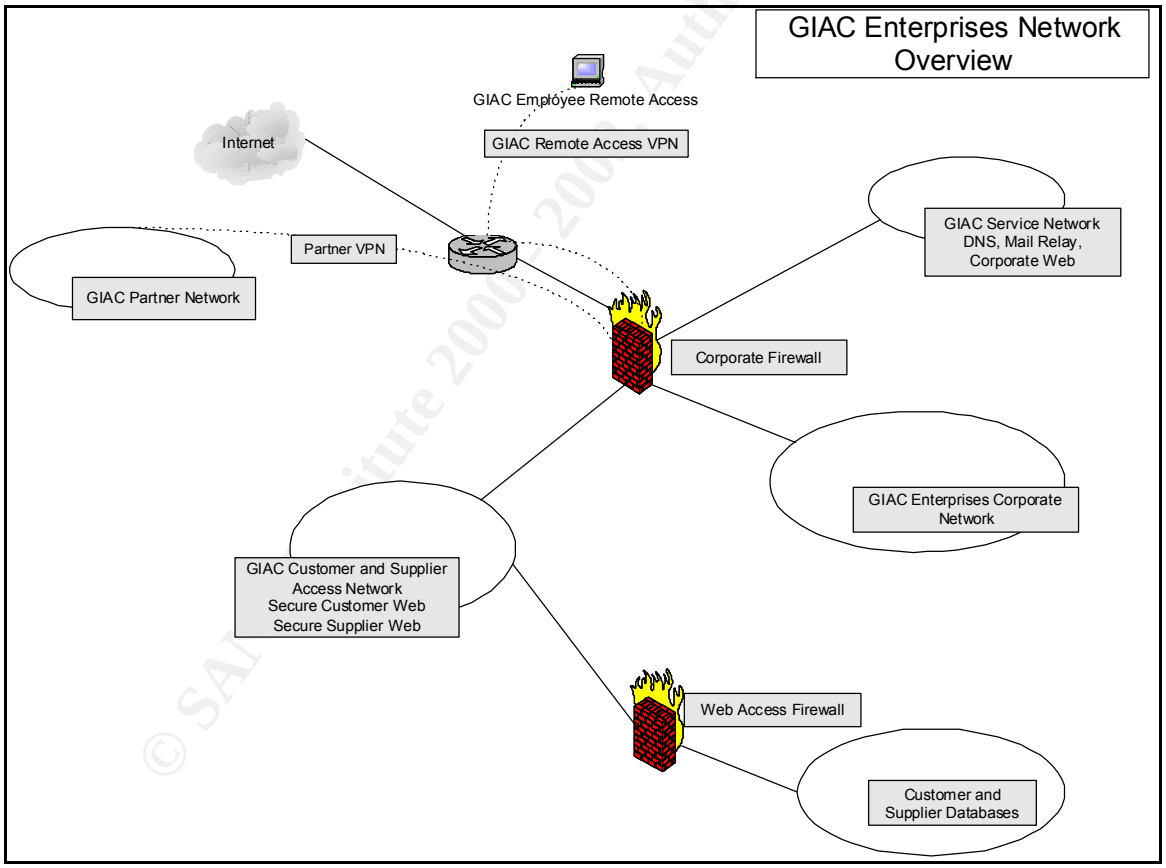
- GIAC partners will need remote access to the customer and supplier databases and will access these resources via VPN. GIAC has established security policies and requirements that partners must meet before they will be allowed to access the GIAC network. Partners must implement a filtering router and firewall and implement other standard network security procedures: i.e. separate service

network or DMZ with split DNS; timely application of system patches and hotfixes.

- GIAC employees will need remote access to the corporate network and customer and supplier databases. They will access these resources via VPN. In order to be supplied with VPN access, employees must install personal firewall software on home PC's and laptops.

- Finally, the general public on the internet will access GIAC web, mail and name services through servers in a separate service network.

A 'high-level' network diagram is below. Greater detail about each component will be provided later. The philosophy behind this network design is to segregate the different business functions as much as possible, so as to make a security breach more difficult to achieve and to minimize the impact of any possible intrusions.



Perimeter Network Devices and Internet Connectivity

The GIAC border router is a Cisco 7204 Router running Cisco IOS version 12.0. The 7204 was chosen because of its high performance, modularity and scalability. It will

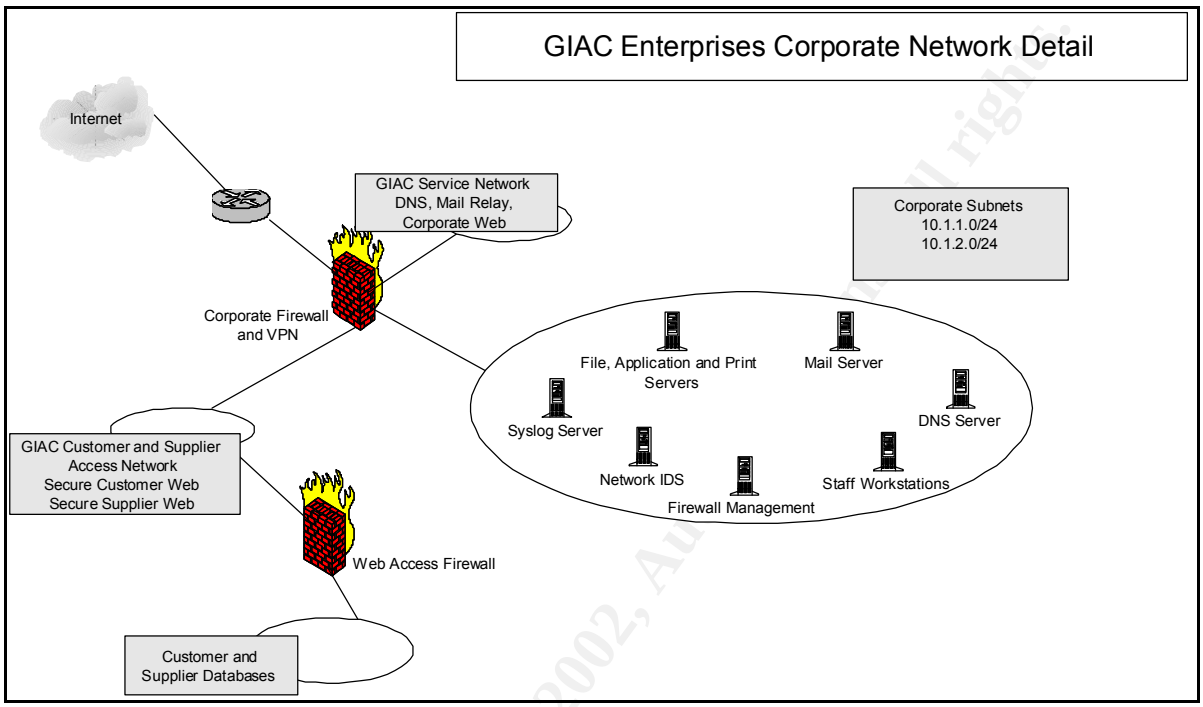
handle the growing needs of a successful internet startup. Higher speed WAN access modules or Gigabit Ethernet or voice support can be added later.

Two Checkpoint Firewall-1 firewalls will be installed. Both will run Firewall-1 version 4.1 Service Pack 3. Two firewalls are used to provide 'defense in depth.' One firewall, the corporate firewall, will be placed between the GIAC networks and the internet. It will also provide segregation of the different networks. This firewall will use four interfaces: one to the router and internet, one to the internal network, one to the services network and one to the customer and supplier web network. The second firewall, the web access firewall, will defend the customer and supplier databases, where highly confidential and valuable information is stored.

Both of the firewalls will run on Sun Microsystems Enterprise 250 servers running Sun Solaris 2.7. The High Availability Module for Firewall-l will be implemented as well, to provide fail-over support. In actuality, there will be four firewalls total. However, for the purposes of this assignment, we will refer to each firewall as if it were a single firewall.

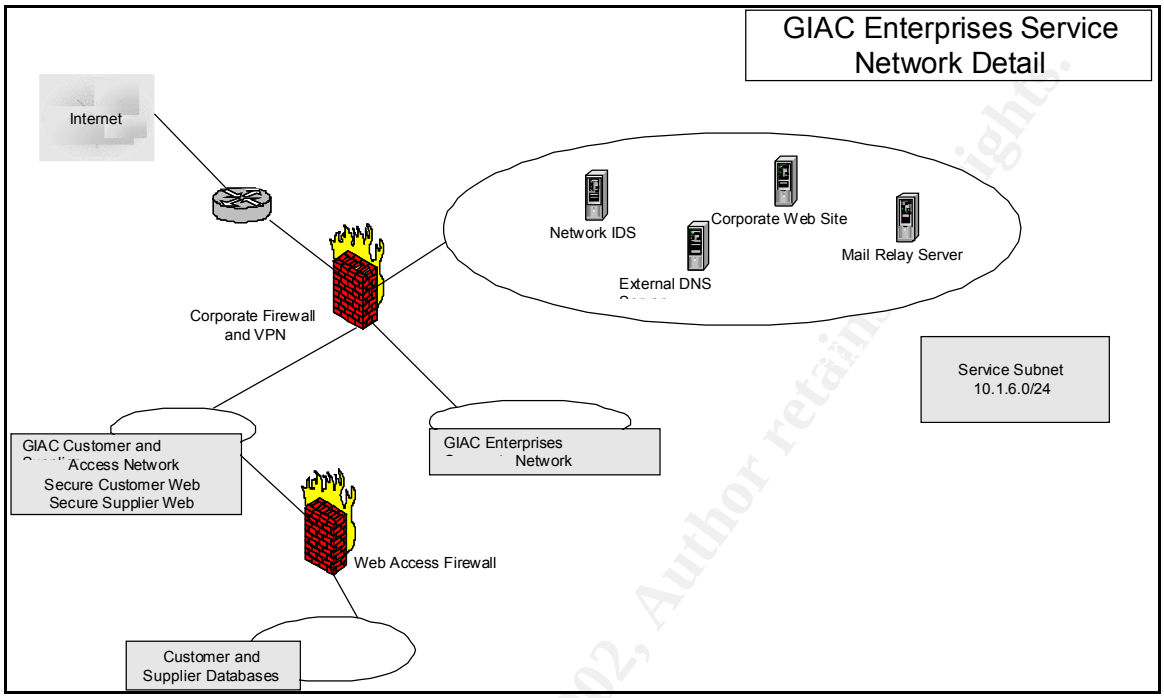
VPN access will be provided by Checkpoint's VPN-1 Gateway, integrated with the corporate firewall. The integration with the firewall will allow inspection of VPN traffic by the firewall and simplify administration. The VPN will also benefit from the redundancy of the High Availability Module. GIAC employees accessing the VPN remotely will have Checkpoint's SecuRemote client installed on their PC. SecuRemote supports Windows, 95, 98, ME, NT and 2000. Partner networks will be able to connect even if they are not using VPN-1 because we will not use proprietary protocols.

GIAC Corporate Network



The GIAC corporate network, shown in detail above, is composed mostly of staff workstations running Windows NT 4.0 and 2000 and servers running Windows NT 4.0 or 2000. Microsoft Exchange provides internal messaging services and forwards SMTP mail to the mail server in the service network. A RedHat Linux 7.0 server running Snort provides network intrusion detection. The corporate and web access firewalls are managed from Checkpoint GUI clients on administrator's workstations. RedHat Linux is also used for GIAC's syslog server, which receives logs from all the Snort devices and the router in the network. Though this network is not exposed to the internet, all servers have been hardened as much as possible to remove any extra services and have the latest service packs and hotfixes applied. Workstations have current anti-virus software applied.

GIAC Service Network



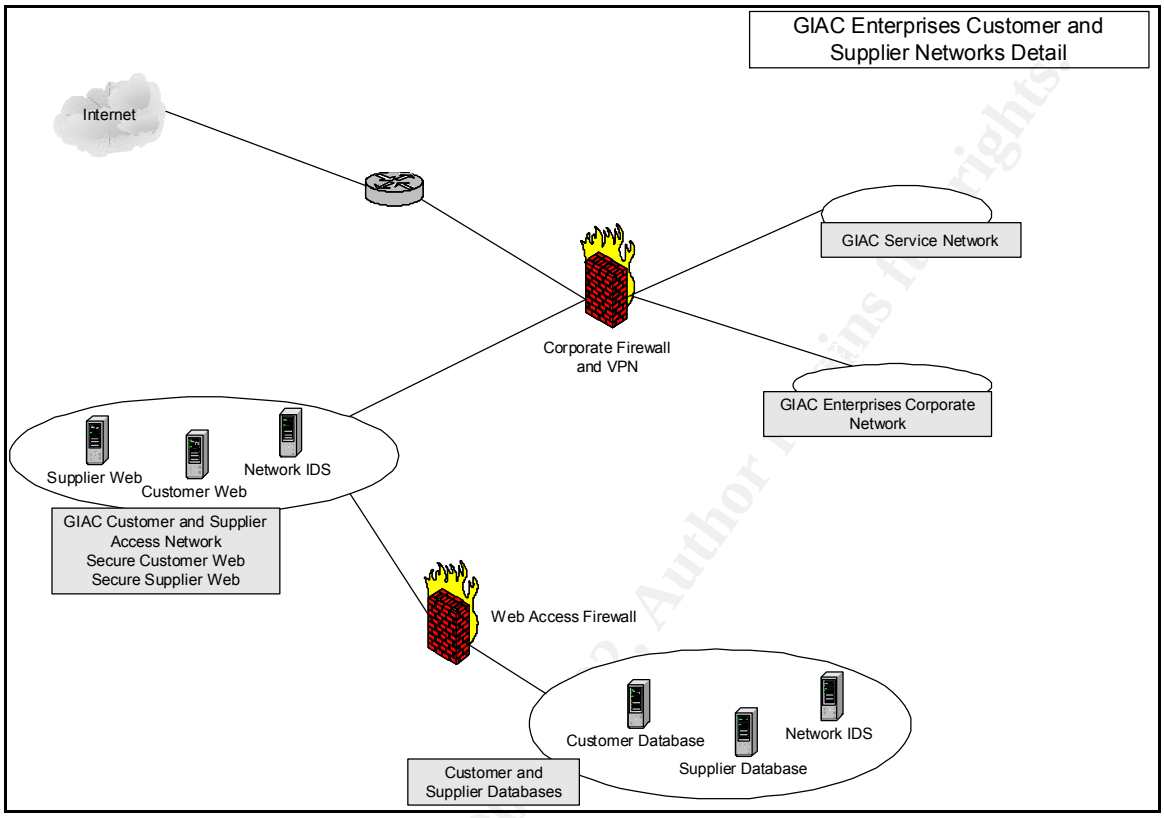
The service network is how the public internet interfaces with GIAC enterprises. Thus it is very vulnerable and subject to hostile attacks. In the service network, we have a four RedHat Linux 7.0 servers: one running Snort for intrusion detection, one for the corporate web site, one for an external mail relay and one for the external DNS. As this network is highly visible and exposed, keeping current with operating system and application patches will be required.

The corporate web site holds mostly information about GIAC products and services. The web server platform is the Apache.

We will use Sendmail 8.11.3 for our SMTP relay server. This server will forward inbound SMTP mail to the Exchange server in the corporate network and will forward outbound internet mail from the Exchange server. The mail server will be carefully configured so it is not an open relay, but will only relay mail from the internal network.

The external DNS server will only list hosts that GIAC wishes to be publicly known and accessible. We will utilize a split DNS structure to protect the internal GIAC networks. The internal DNS server will forward internet queries to the external DNS. The registered primary nameserver for GIAC will be the external DNS, ns1.giac.com. We will not allow zone transfers on this DNS server. The external DNS will be non-recursive. BIND has been the subject of several popular exploits recently, so again it will be critical to be current with patches and fixes for this program. The GIAC external DNS will run BIND version 9.1.0.

GIAC Customer and Supplier Networks



The two networks where customers and suppliers transact business are the 'crown jewels' of GIAC Enterprises. The 'Access Network' consists of secure web servers where customers place orders and suppliers upload fortunes. Both the customer web server and supplier web server are running Solaris 2.6 with Netscape Enterprise Server 3.6. The Netscape server was selected because of its high-performance, reliability and scalability. Customers and suppliers connect to the appropriate server where an SSL session is opened once the transaction begins. This information is passed in encrypted form through the web access firewall to the back-end databases. These databases are running Oracle on Solaris 2.8. Both network segments have Snort intrusion detection running on RedHat Linux, logging to the syslog server in the corporate network. Because the information stored in these databases is valuable and confidential, we will use Oracle database security features to secure the servers.

Assignment 2 - Security Policy (25 Points)

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

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall ruleset, 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!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule

Security Policy for the GIAC Enterprises Router

The Cisco 7204 Router connects GIAC Enterprises to the internet, via their ISP. The principle behind the security policy on this router is that a router should primarily route traffic, while the firewall will do the bulk of examining traffic leaving and entering the network. However, we will configure this router to eliminate many DoS (Denial of

Service) and DDoS (Distributed Denial of Service) attacks. We will also harden the router itself by restricting access to it.

We will use access lists to filter packets based on their source address on both the serial and ethernet interfaces of the router. Because we are only concerned with source addresses at this device, we will use a standard access list, which only looks at the ip source. This kind of list has limited functionality, but it serves our purposes and will be fast and efficient.

Ingress Filtering

First, we will implement the following access list on the serial interface to drop any spoofed packets from entering the router. We will also drop anything trying to enter the network with an address that has been assigned to GIAC Enterprises (GIAC uses NAT but they own the 1.1.1.0/24, 1.1.2.0/24 and 1.1.3.0/24 address ranges). The final line permits anything that has not been denied and is necessary because there is an implicit deny rule at the end of the access list.

```
!
!  drop any addresses with the historical broadcast address
!
access-list 10 deny 0.0.0.0         0.255.255.255   any
!
! drop RFC 1918 (non-routable) addresses
!
access-list 10 deny 10.0.0.0        0.255.255.255   any
access-list 10 deny 172.16.0.0      0.15.255.255    any
access-list 10 deny 192.168.0.0     0.0.255.255     any
!
! drop the loopback address
!
access-list 10 deny 127.0.0.0       0.255.255.255   any
!
! drop reserved networks
!
access-list 10 deny 169.254.0.0     0.0.255.255     any
access-list 10 deny 192.0.2.0       0.0.255.255     any
access-list 10 deny 240.0.0.0       7.255.255.255   any
access-list 10 deny 248.0.0.0       7.255.255.255   any
!
!  drop multicast packets
!
access-list 10 deny 224.0.0.0       15.255.255.255  any
!
! drop broadcast packets
!
access-list 10 deny 255.255.255.255  0.0.0.0        any
!
!  deny anything with GIAC's IP range
!
```

```
access-list 10 deny 1.1.1.0          0.0.0.255       any
access-list 10 deny 1.1.2.0          0.0.0.255       any
access-list 10 deny 1.1.3.0          0.0.0.255       any
!
! allow anything else
!
permit any any
```

Access lists can be applied in either direction on an interface, which can be a source of confusion and may accomplish the opposite of what you were hoping to do. The configuration commands below will apply access-list 101 on the serial interface in the inbound direction.

```
giac-gw(config)#interface serial 0
giac-gw(config-if)#ip access-group 10 in
```

Egress Filtering

We will implement another access list on the ethernet interface of the GIAC router. This list will be applied inbound on the ethernet interface so it filters traffic as it leaves the GIAC network. We will be stopping anything except GIAC network traffic from leaving the network; any legitimate internal traffic will have been NAT'ed at the firewall. This filter will help prevent the GIAC network from being used in a distributed denial of service attack.

```
!
!  allow anything from GIAC's internal network
!
access-list 12 allow 1.1.1.0  0.0.0.255 any
access-list 12 allow 1.1.2.0  0.0.0.255 any
access-list 12 allow 1.1.3.0  0.0.0.255 any
!
! allow anything else
!
deny any any

giac-gw(config)#interface ethernet 0
giac-gw(config-if)#ip access-group 12 in
```

Access Control to the Cisco 7204 Router

We will need to implement access controls on the router itself and to its console and remote terminal connections.

First we will enable MD5 hashing for the enable password, which is the password required to make configuration changes to the router:

```
# enable secret
```

This uses much stronger encryption than the older 'enable password' command. We will also enter the following command:

```
# service password-encryption
```

This command will store the passwords in encrypted form. Finally we will limit remote access to the router with the following:

```
access-list 12 permit 10.1.1.23  0.0.0.0
access-list 12 permit 10.1.1.24  0.0.0.0
access list 12 permit 10.1.1.25  0.0.0.0

line vty 0 4
access-class 12 in
login
```

This will allow only three IP addresses from the internal GIAC network to access to router.

Because GIAC wishes to use SNMP to monitor their router and other network devices, we must configure SNMP security.

```
giac-gw(config)# access-list 12 permit 10.1.1.20 0.0.0.0
giac-gw(config)# snmp-server community giac RO 12
giac-gw(config)# snmp-server community supersecretgiac RW 12
```

This configures the SNMP communities and will restrict SNMP access to a particular IP address in the internal network.

Additional Good Practices for Border Routers

We will also implement the following on the GIAC Enterprises 7204, as additional security and being a good internet citizen:

```
giac-gw(config)# interface eth0
giac-gw(config-if)# no ip directed-broadcast
giac-gw(config)# interface ser0
giac-gw(config-if)# no ip directed-broadcast
```

This will prevent our router from receiving or forwarding directed broadcasts so we are not part of a distributed DoS attack.

We will also disallow IP source routing:

```
giac-gw(config)# interface eth0
giac-gw(config-if)# no ip source-broadcast
giac-gw(config)# interface ser0
giac-gw(config-if)# no ip source-broadcast
```

We will disable the router from sending ICMP errors (destination unreachable) because this may be used by an attacker to map the GIAC network:

```
giac-gw(config)# no ip unreachables
```

We are also going to disable a number of services that are generally enabled by default but unnecessary:

```
giac-gw(config)# no service tcp-small-servers
giac-gw(config)# no service udp-small-servers
```

This disables services like echo and chargen that are not necessary.

```
giac-gw(config)# no service finger
giac-gw(config)# no ip http server
giac-gw(config)# no ip bootp server
```

We do not need the finger, http or bootp services running on our router.

Finally, we want to set a banner message that everyone will see when logging on to the router, regardless of how they connect. This banner will state that this is a private system and only authorized users may connect. In the event, the router security is ever breached, the intruder will not be able to claim that he was 'welcomed' by a welcome message or no message at all:

```
giac-gw(config)# banner incoming ^C
WARNING: This is a private system. Authorized access only.
^C
```

We will also set the same message with the banner login and banner exec commands so that users will see the message whenever they go into enable mode as well.

We can test the router policy by trying some of the things that it does not allow. For example, we can try and telnet to the router from an external location and should not be able to reach it. We could use an SNMP program like GetIf and try and pull the configuration from the router from an external location. We can use a program to craft some ip packets, like spoofed packets or source-routed packets, and send them to the router and use a sniffer like tcpdump to see what happens.

Security Policy for the GIAC Enterprises Firewalls and VPN

Because we are using Checkpoint's Firewall-1 and VPN-1 for our firewall and VPN devices, we can set policy and manage them all from the same user interface. GIAC Enterprises has two firewalls: the corporate firewall, which controls access from the internet and between the network segments, and the web access firewall, which adds a layer of protection between the customer and supplier web access network and their database networks.

First we will consider the corporate firewall.

Rule	Source	Destination	Service	Action	Track	Install On
1	FW_Admins	fw_web_access fw_corporate	FW1_mgmt ssh	Accept	Long	Gateways
2	Any	fw_corporate	NBT	Reject		Gateways
3	Any	fw_corporate	Any	Drop	Long	Gateways

These rules control access to the firewall itself. A specified group of users is permitted access to both GIAC firewalls with ssh and the FW1_management protocol. This rule is necessary so administrators can manage the firewalls and VPN. We will reject NBT as there will be a lot of it in the internal network and would fill the logs.

Rule	Source	Destination	Service	Action	Track	Install On
4	Partner_net	Net_Databases	DB_Services	Encrypt	Long	Gateways
5	GIAC_Users@any	Net_Internal	Any	Client Encrypt	Long	Gateways
6	GIAC_Users@any	Net_Databases	DB_Services	Client Encrypt	Long	Gateways

These rules establish the VPNs for partner networks and for remote access by GIAC employees. We have chosen to use Manual IPSec for our encryption scheme to ease interoperability with partner sites that may not be using Checkpoint as their VPN solution. Our partner to partner VPN is going to use ESP (Encapsulating Security Payload) but not AH (Authentication Header). There are compatibility issues with AH and IPSec and because we will be traversing different networks, we will just use ESP, which will encrypt the contents of the IP packets. We will need to do a key exchange manually with all partner networks that will use VPNs since Manual IPSec has no provision of automated key exchange.

For remote users, we will use the IKE encryption scheme with Triple DES, as SecuRemote does not always work with IPSec. GIAC remote users use SecuRemote on their laptops or home PC's. They will authenticate against a RADIUS database in the internal network to use the VPN. SecuRemote will encrypt traffic for the GIAC network while regular Internet traffic is not encrypted. Split tunneling is not desirable from a security standpoint but we do not have much choice if we want to use VPN-1 and SecuRemote.

Rule	Source	Destination	Service	Action	Track	Install On
7	Router_admins	GIAC_7204	ssh telnet	Accept	Long	Gateways

Rule 7 allows for remote administration of the router by telnet and ssh.

Rule	Source	Destination	Service	Action	Track	Install On
8	Internal_Mail mail.giac.com	Internal_Mail mail.giac.com	smtp	Accept	Long	Gateways

Rule 8 allows the internal Exchange mail server to forward smtp mail to the mail server in the service network. It also allows the service network mail server to forward smtp mail to the Exchange server.

Rule	Source	Destination	Service	Action	Track	Install On
9	Net_Internal	Any	http https	Accept	Long	Gateways
10	Internal_Finance DB_Admin	Customer_DB Supplier_DB	DB Services	Accept	Long	Gateways
11	Net_Internal	Net_Cust_Supp Net_Service	Any	Drop	Long	Gateways

Rules 9-11 set policy for the internal network. Anyone on the internal network can browse anywhere on the internet with http and https. Selected financial staff and database administrators have access to the customer and supplier databases in the secured database network. Finally, we will drop anything else from the internal network any of to the other networks. This will prevent internal users from using our external mail or DNS servers.

Rule	Source	Destination	Service	Action	Track	Install On
12	Any	Giac_Web	http	Accept	Long	Gateways
13	Any	Customer_web Supplier_Web	http	Accept	Long	Gateways
14	Any	mail.giac.com	smtp	Accept	Long	Gateways
15	Any	ns1.giac.com	domain-udp	Accept	Long	Gateways
16	ns1.giac.com	Any	domain-udp	Accept	Long	Gateways
17	mail.giac.com	Any	smtp	Accept	Long	Gateways

The next set of rules pertain to GIAC's internet connectivity. We will allow connections from anywhere to the GIAC corporate web. Since our customers and suppliers could be anywhere, we need to allow any access to those websites over http and https. Finally, we need to send and receive e-mail and perform domain lookups.

Rule	Source	Destination	Service	Action	Track	Install On
18	NIDS_Databases NIDS_Service NIDS_WebAccess	Syslogger	syslog	Accept	Long	Gateways

Rule 18 allows our Snort devices to log to a syslog server in the internal network.

Rule	Source	Destination	Service	Action	Track	Install On
19	Any	Any	Any	Drop	Long	Gateways

Finally, we have the "clean up" rule which drops anything that has not been allowed or denied already. Like most corporations, we have a 'default deny' firewall policy.

The rule set for the web access firewall is much simpler by comparison, as it is only mediating access between two networks.

Rule	Source	Destination	Service	Action	Track	Install On
1	fw_admins	fw_web_access	FW1_mgmt ssh	Accept	Long	Gateways
2	Any	fw_web_access	Any	Drop	Long	Gateways
3	Customer_Web	Customer_DB	DB_Services1	Accept	Long	Gateways
4	Supplier_Web	Supplier_DB	DB_Services2	Accept	Long	Gateways
5	Partner_net	Net_Databases	DB_Services	Accept	Long	Gateways
6	GIAC_Users@a ny	Net_Databases	DB_Services	Accept	Long	Gateways
7	Internal_Finance DB_Admin	Customer_DB Supplier_DB	DB Services	Accept	Long	Gateways
8	NIDS_Databases	Syslogger	syslog	Accept	Long	Gateways
9	Any	Any	Any	Drop	Long	Gateways

Rules 1 and 2 control access to the firewall itself. Rule 1 allows selected hosts in the internal network to access the firewall with the GUI management client and ssh. Rule 2 drops all other attempts to access the firewall.

Rules 3 and 4 permit access between the web servers in the customer and supplier access network and the databases in the protected network. These servers will use application-specific TCP protocols to make the connections to the databases.

Rules 5 and 6 allow the VPN users from partner networks and GIAC users to access the databases.

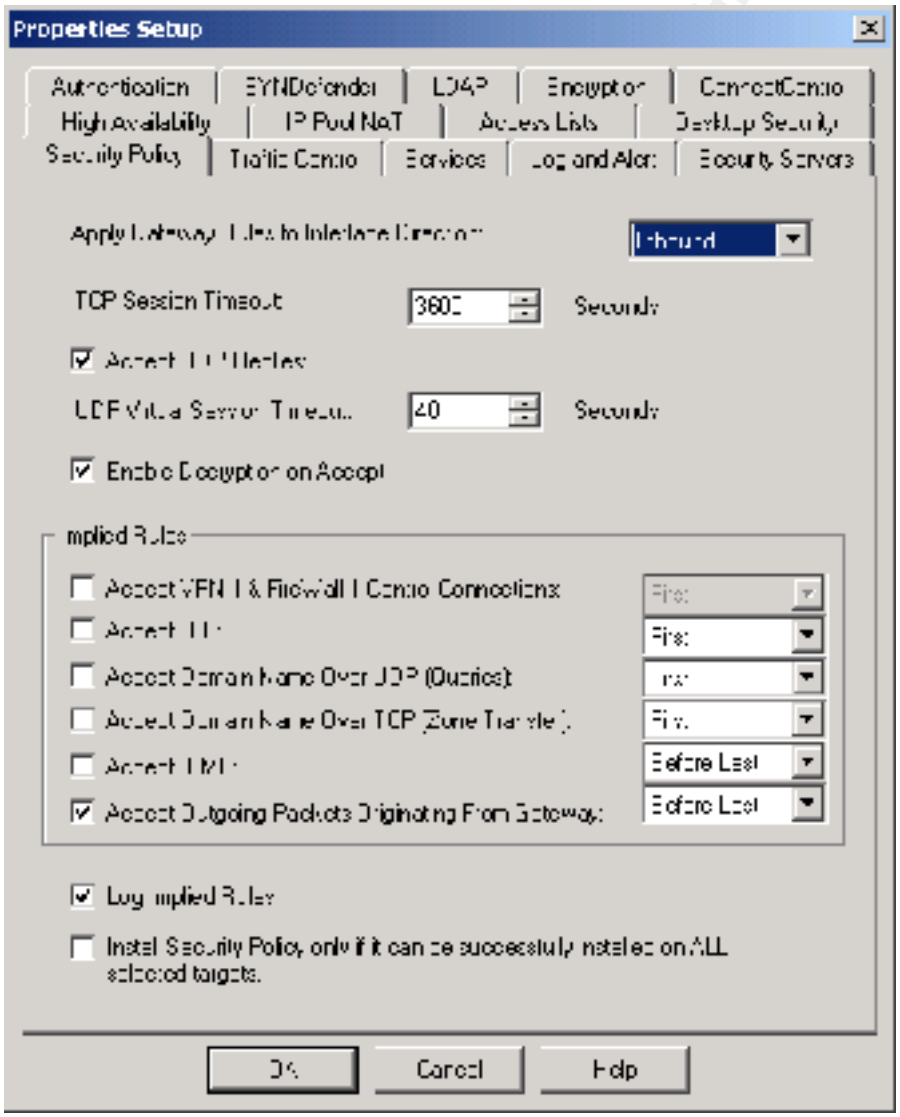
Rule 7 allows database administrators and finance staff access to the databases from the internal network.

Rule 8 allows the Snort IDS system in the protected database network to communicate to the syslog server in the internal GIAC network. Note that the IDS in the customer and

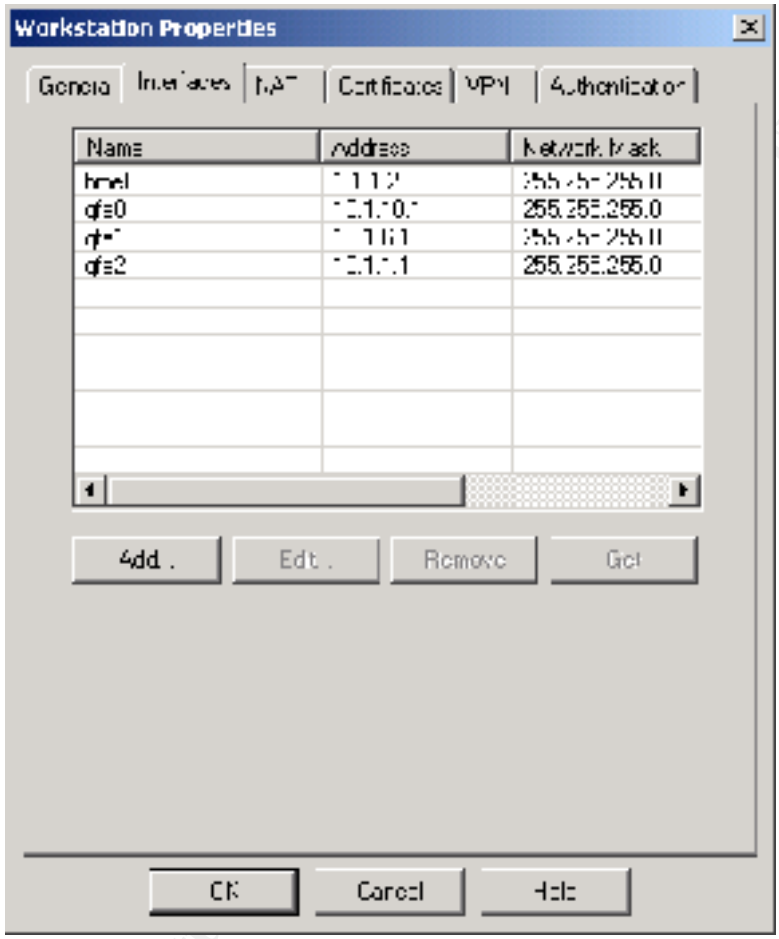
supplier web network will only pass through the corporate firewall, so we are not concerned with it here.

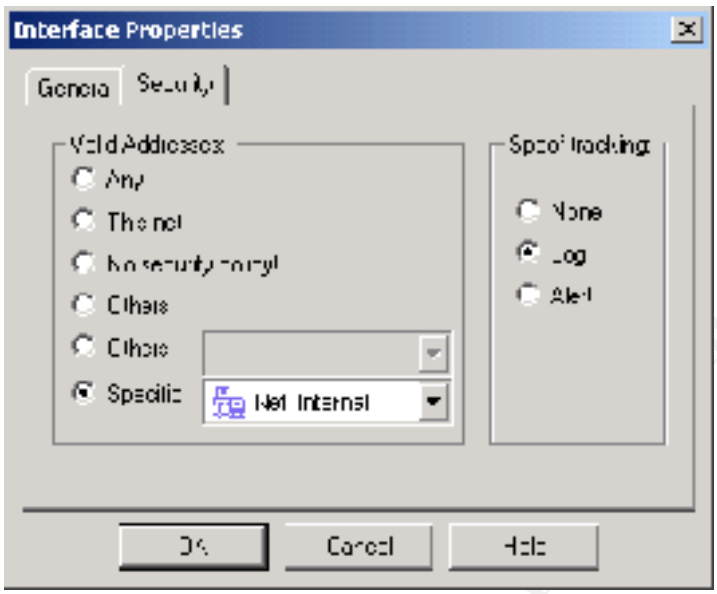
Finally, Rule 9 drops anything that has not been allowed or denied previously.

For both firewalls, we will need to do some configuration of the firewall properties as well. In Checkpoint FW-1 version 4.1, many of the Security Policy properties that had been enabled in previous versions are now disabled. We will leave the options for accepting RIP, Domain Name over UDP, Domain Name over TCP and ICMP disabled. The option to 'Accept VPN-1 and Firewall-1 Control Connections' has been disabled so that we can control access to the firewall more carefully.

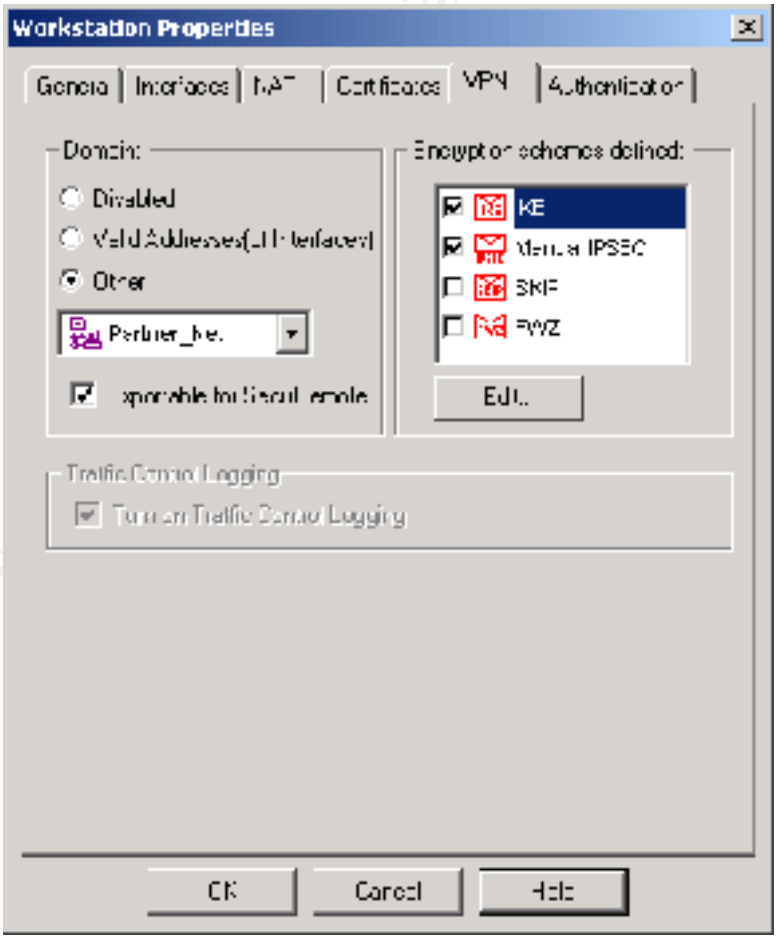


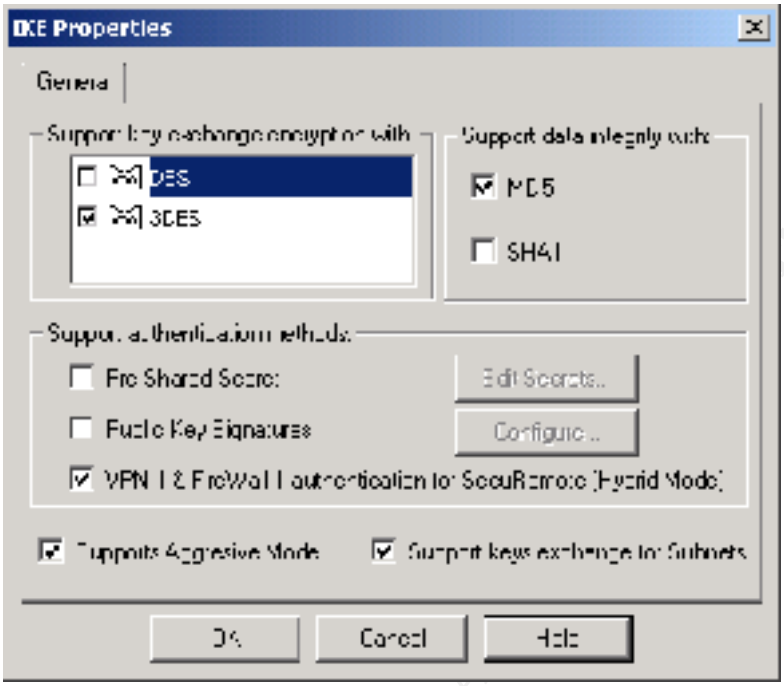
We will also need to configure anti-spoofing on all firewall interfaces. This is done in the properties of the firewall object. The policy needs to be set up so that only legitimate traffic will be allowed to go through the interface.



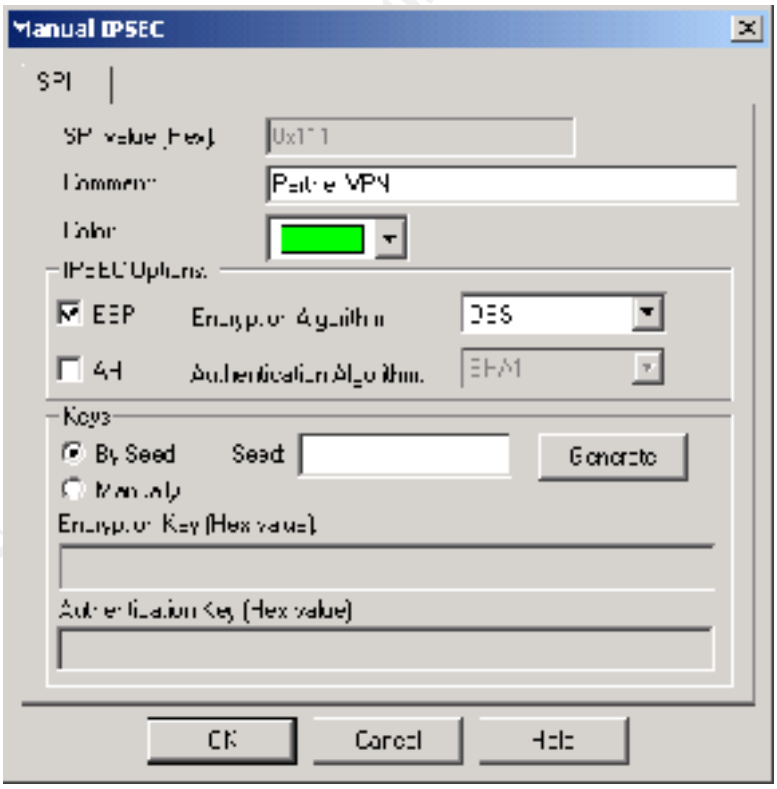


We will need to configure our VPN in the properties of the firewall as well.





For Manual IPSec, there are no properties to configure but we need to generate keys.



We can test our firewall policy by portscanning our external hosts with nmap. We should only see the ports that we have opened on the firewalls.

Assignment 3 - Audit Your Security Architecture (25 Points)

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:

1. 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.
2. 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.
3. 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.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

We will conduct a security audit and assessment of GIAC Enterprises in several stages. We will start with an external audit and then do an internal audit. The goal of the external audit will be to look at the GIAC network as seen from the internet, by someone with little or no insider knowledge. We will start with some basic information gathering and then move on to actual scans of the network. For the information gathering, since it is non-intrusive, we can do it at anytime. We will conduct the scanning during non-business hours, in an effort to minimize any negative impact on the GIAC business. We will notify the administrators that the assessment will be happening but will not give them the exact times or days. We will use a variety of tools, both open source and proprietary. The cost of this type of assessment will be expensive but valuable to get an outsider's perspective of the network.

Once we have a picture of the external network, we will work from the inside. For this part, we will require the cooperation of GIAC IT staff as we will need to examine firewall and router configurations. We will revisit our scans to make sure the router and firewalls are enforcing the security policies. We will also look at internal policies and procedures at GIAC to make sure they conform to good security practices. For example: password policies for staff, safeguarding of administrative passwords, log review procedures.

Finally, we will make recommendations on how GIAC could improve their security architecture.

We will begin with basic information gathering. We will start with nslookup.

```
D:\>nslookup
Default Server:  ns2.swbell.net
Address:  151.164.1.7

> set type=any
> giac.com
Server:  ns2.swbell.net
Address:  151.164.1.7

Non-authoritative answer:
giac.com        nameserver = NS1.giac.com
giac.com        nameserver = ISP.NET
giac.com
        primary name server = NS1.giac.com
        responsible mail addr = admin.giac.com
        serial  = 2001032601
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 604800 (7 days)
        default TTL = 600 (10 mins)
giac.com        internet address = 1.1.1.50

giac.com        nameserver = NS1.giac.com
giac.com        nameserver = ISP.NET

NS1.giac.com            internet address = 1.1.1.10
ISP.NET                 internet address = 2.2.3.4
```

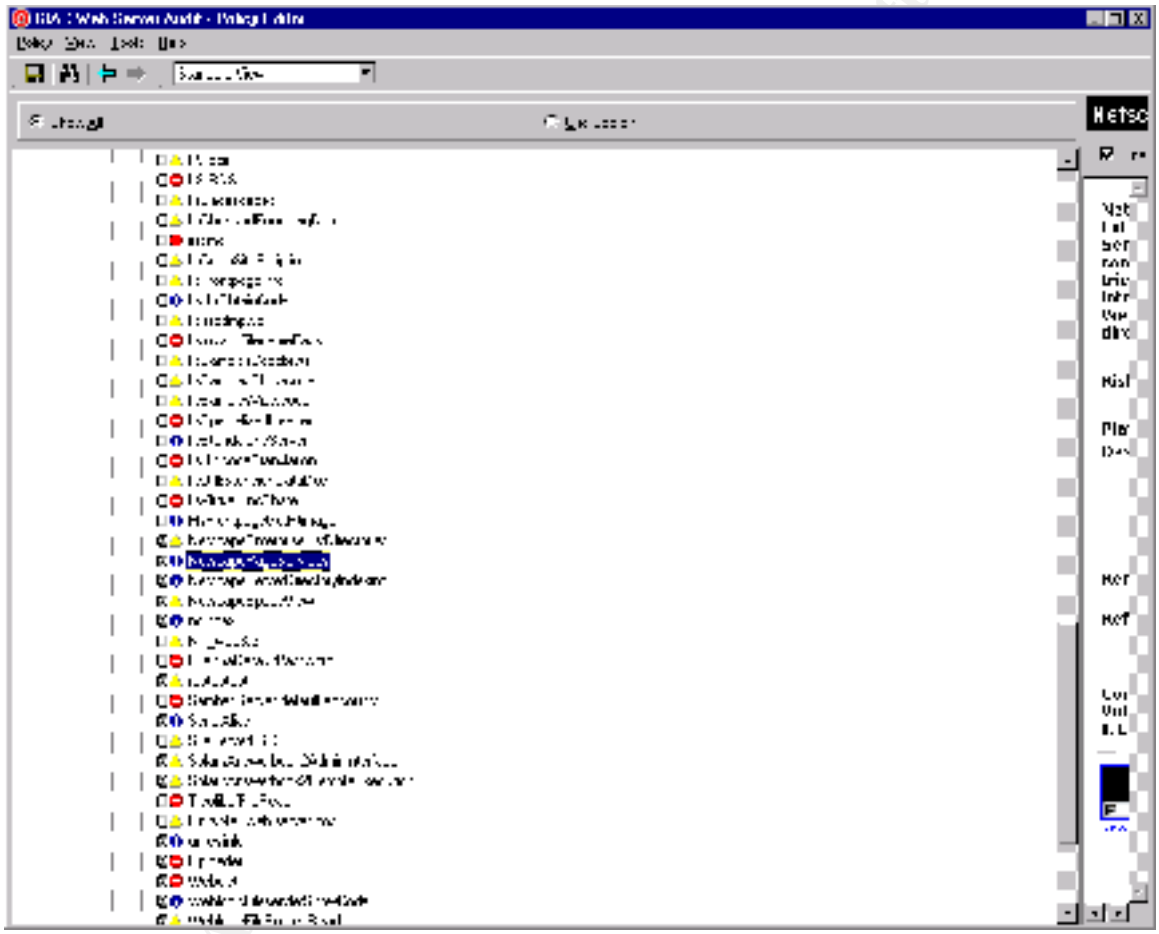
Now that we have the server address for GIAC, we can connect to it and see if we can do a zone transfer. The results below show that we cannot, which is how we like to see the DNS set up.

```
> server ns1.giac.com

Default Server:  ns1.giac.com

Address:  1.1.1.10

> ls -d giac.com.

[ns1.giac.com]

*** Can't list domain giac.com.: Query refused
```

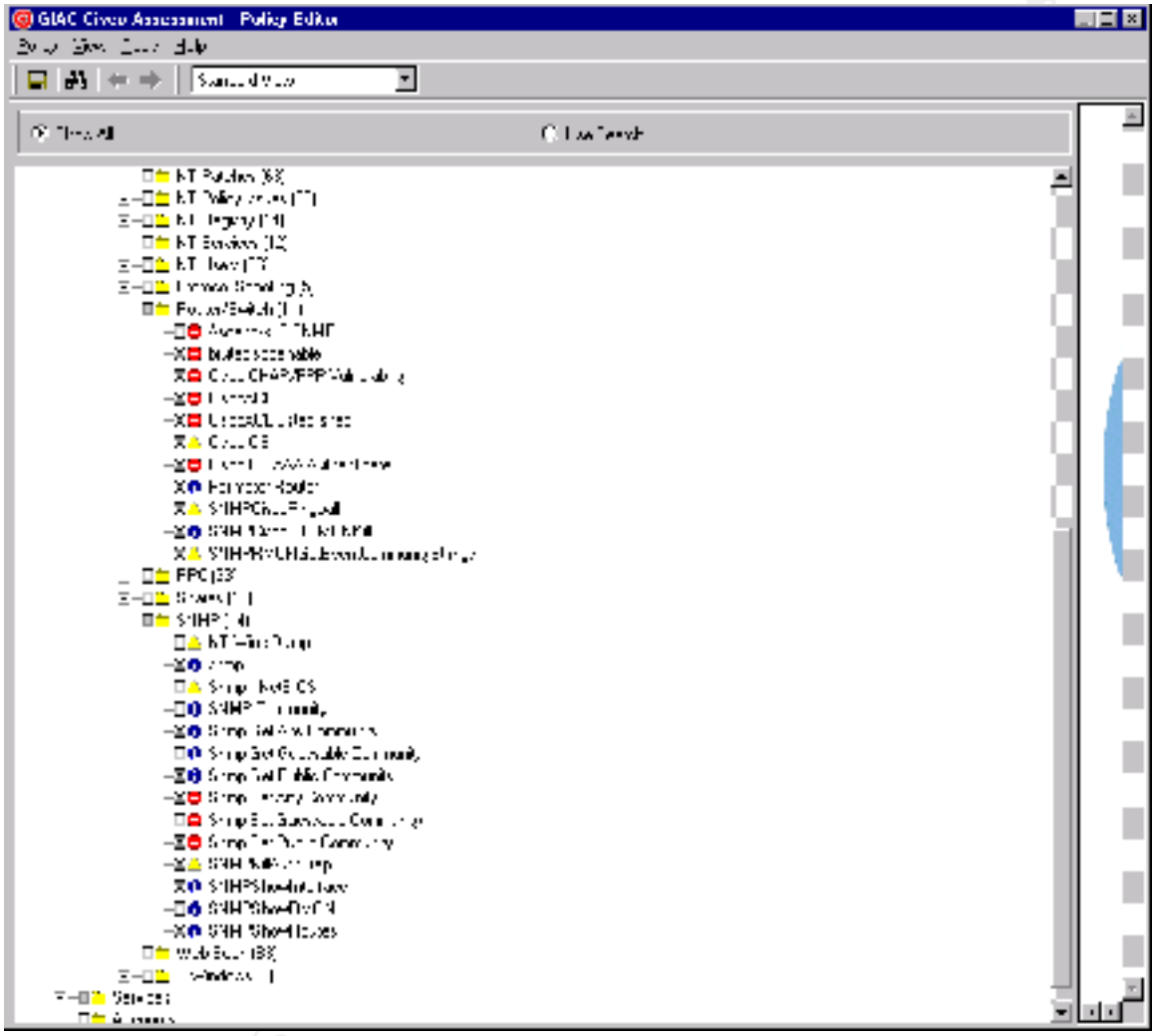
Since we now have a clue about GIAC's IP address space, we can run nmap with a ping only scan to see what hosts respond. However, GIAC has chosen to block ICMP echo-reply from leaving the network, so we get no response. However, we can still scan hosts to see what services are running. Because GIAC has segmented their network and uses

NAT, we will only find a few hosts that are externally visible: the customer, supplier and GIAC corporate web sites, the external mail relay and the external name server.

We will next use Internet Security System's Internet Scanner to do a comprehensive vulnerability scan of these servers. We have developed custom policies to scan GIAC based on what we have learned about their hosts so far. For example, by telnetting to port 80 on a web server and typing 'HTTP / GET 1.0' we can often determine the type of web server that is running. Since we know the customer and supplier webs are running on Netscape Enterprise Server, there is no need to scan for IIS vulnerabilities.



We can also develop a custom scan for different brands of routers. An example of one designed for Cisco routers is shown below.

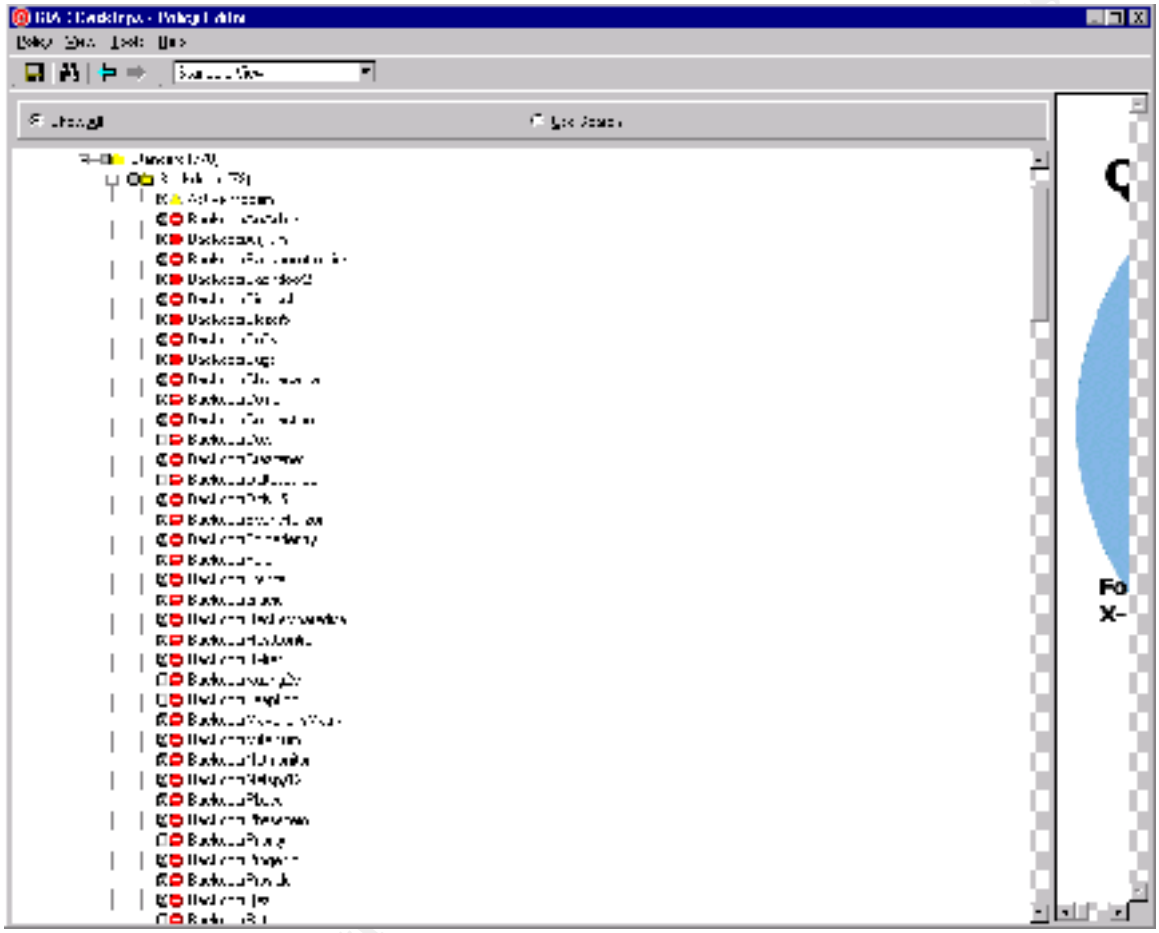


We can also test the router policies by trying to send crafted packets with spoofed IP addresses or source-routed packets through it.

The intrusion detection systems will be tested by this external audit process. We should set off many alarms in Snort and will need to work with GIAC so that we can still get our assessment completed.

Once we have finished the audit from the external perspective, we will perform an internal assessment. For this, we will work with the GIAC IT staff. We will run the same scans, using nmap and ISS Internet Scanner again to see what is different from

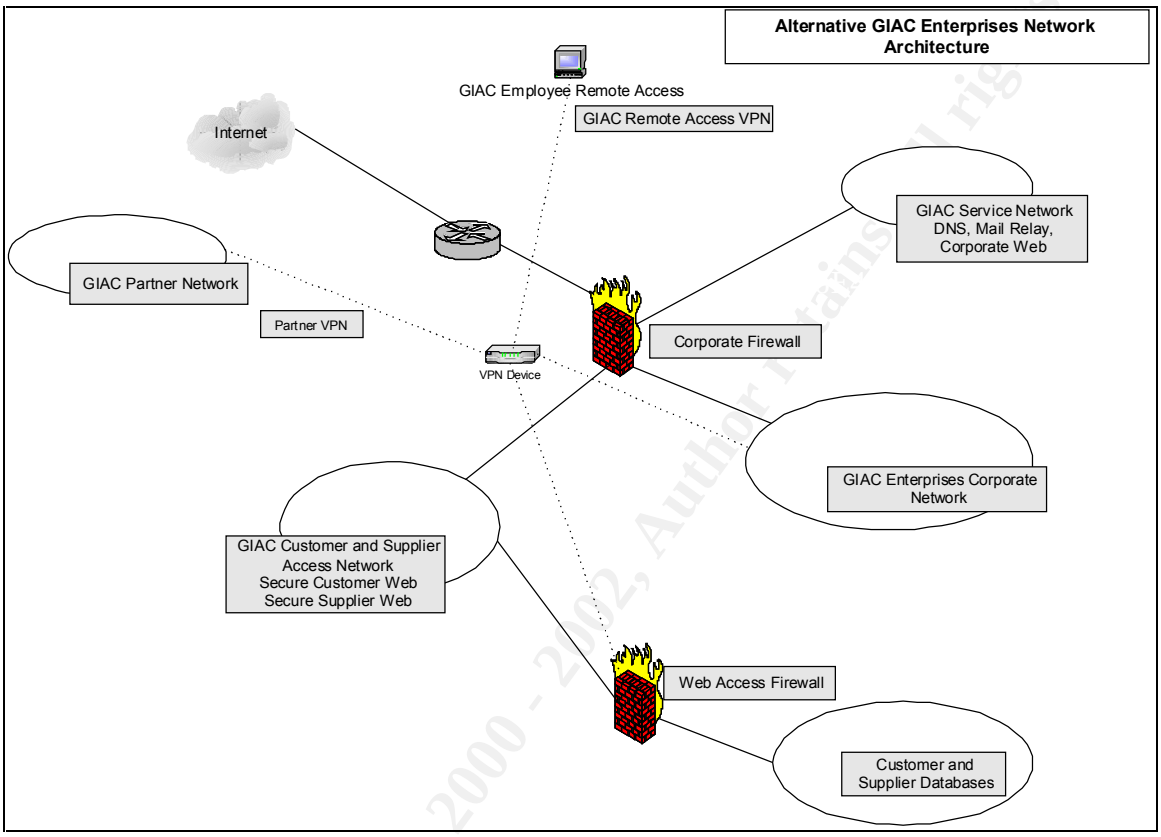
inside the network. We can also scan desktops and servers, looking carefully for 'Backdoor' programs. We will also look at security policies and procedures.



In our presentation of assessment findings, we note that it appears that GIAC's firewall and border router are properly enforcing the security policies. We do have some concerns about some of the hosts, however. There have been recent exploits against BIND and a long history of exploits against sendmail so it is essential that administrators keep up with security patches and upgrades for those services. RedHat Linux has also been the subject of exploits, so that must be closely monitored as well. GIAC is running a number of different platforms: Solaris, Linux, NT and 2000. It will not be an easy job for administrators to keep up with all of them.

We can recommend a possible alternative network architecture for GIAC. Rather than having the VPN on the firewall, we will set up a separate VPN device, parallel to the firewall. This would take the VPN load off the firewall and simplify the rules and administration of the firewall. We would also be able to use something other than VPN-1

and SecuRemote, which allows split tunneling, which we do not like as it could allow internet traffic into your internal networks via your employee's workstations. VPN access to the customer and supplier databases would still be firewalled by the web access firewall.



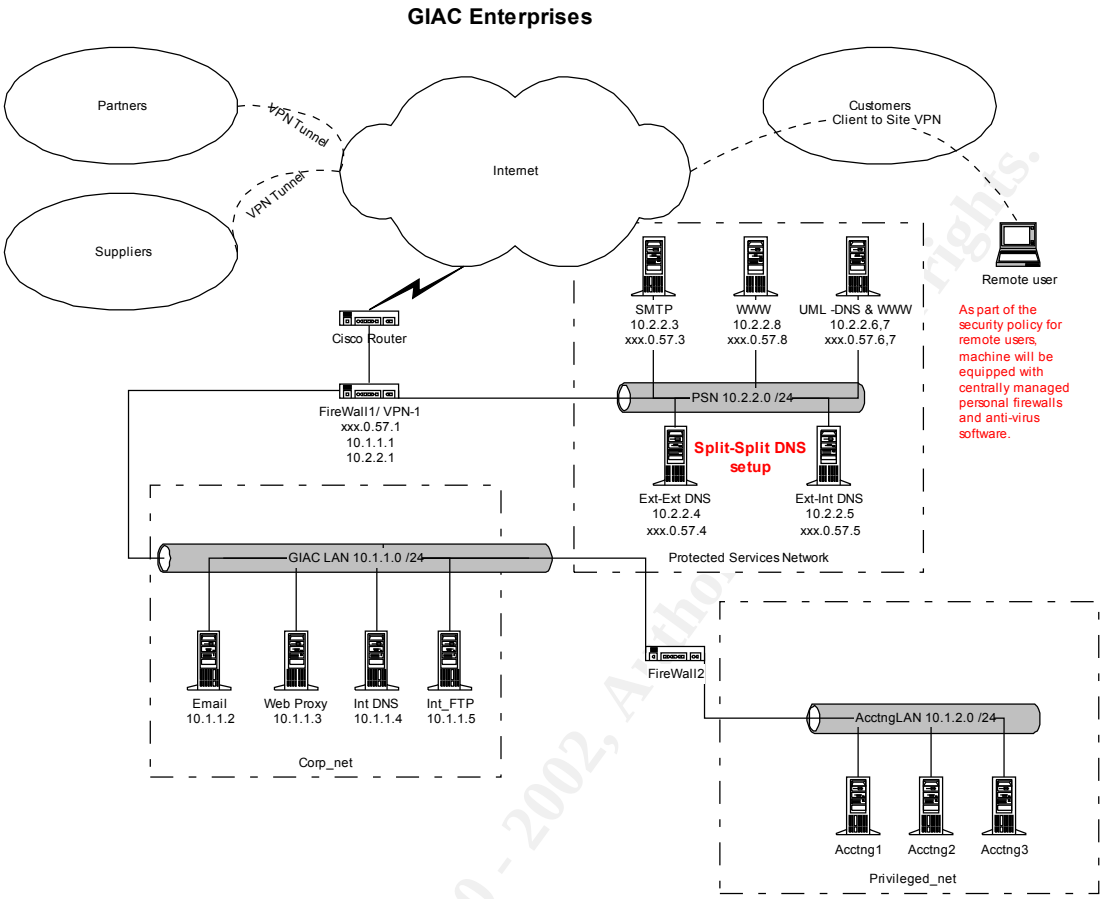
Assignment 4 - Design Under Fire (25 Points)

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:

1. 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.
2. 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.
3. 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.

I have chosen to analyze and attack Brett Gordon's (http://www.sans.org/y2k/practical/Brett_Gordon_GCFW.doc) perimeter security architecture.



Exploit against the firewall

Research turned up few exploits against the firewall itself, Checkpoint Firewall-1. Brett's design has the firewall installed on NT 4.0, which has a greater number of exploits that could be attempted. However, I am going to focus on a denial of service attack against the firewall using fragmented packets. This vulnerability was discovered by Lance Spitzner and described in a message to BUGTRAQ , June 5, 2000.

If we send very large fragmented packets at the firewall, we could cause it the firewall to go to 100% CPU usage. Checkpoint FW-1 is designed to reassemble fragmented packets before inspecting them against the state table or rulebase. When the firewall attempts to reassemble all these packets, that exhausts the processor. We can use the jolt program to generate these packets.

Denial of Service Attack on the Network

For a denial of service attack on Brett's network, we have the services of 50 compromised cable modem/DSL systems so we can attempt a distributed denial of service attack. We will attempt to bring down his network with the Tribal Flood 2K tool. We can use Unix or NT systems to help in our attack. Once we have our master and slaves set up, we can communicate to our compromised slaves by TCP, UDP or ICMP. We can attack our target with TCP, UDP or ICMP or a mixture of the three. In addition, the commands to the slaves are encrypted.

To try and counteract or mitigate this attack, Brett needs to have anti-spoofing in his border router policy, which he does. An application layer firewall, like a proxy server, would also help. He should also disallow as many TCP and UDP ports and ICMP types as possible.

Attack to compromise an internal system

For this attack, we are going to target a specific host on Brett's network for vulnerabilities and then attempt to exploit it. We will start with nmap to portscan his services network. We would like to target a web server as there are exploits for all flavors of web servers. Using nmap, we find a possible victim:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host www.giac-enterprises.com (xxx.0.57.3) appears to be up ... good.
Initiating SYN half-open stealth scan against www.giac-enterprises.com
(xxx.0.57.3)

Interesting ports on www.giac-enterprises.com (xxx.0.57.3):
(The 1521 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https

TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=22 (Easy)

Sequence numbers: 441407C6 441407EA 44140800 44140831 441407FD 44140854
```

```
Remote operating system guess: Windows NT4 / Win95 / Win98
```

Since nmap thinks the remote operating system is Windows, we will start with some common IIS exploits in hopes that Brett doesn't keep his servers updated with the current patches. The exploits we will be trying go through port 80, so his firewall is irrelevant. We can do a quick check for the Unicode vulnerability by entering the following URL or a one using similar Unicode characters:
http://xxx.0.57.3/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\ . If that yields a list of what is on the C: drive, his server is vulnerable and we may be able to view files anywhere on the system. If permissions are not set correctly, we may be able to delete or change files as well.

We can also see if Brett's web server is vulnerable to the RDS vulnerability. We can use the msadc.pl script written by Rain Forest Puppy to test for this vulnerability. If the server has this vulnerability, we can run a remote shell (cmd.exe) and basically own the server.

References Used

Assignment 1: Security Architecture

Linux Hardening:

- Spitzner, Lance, "Armoring Linux," URL : http://www.enteract.com/~lspitz/linux.htm
- Bastille Linux Hardening System, http://www.bastille-linux.org

Solaris Hardening:

- Spitzner, Lance, "Armoring Solaris," URL: http://www.enteract.com/~lspitz/armoring.html

BIND and Split DNS Configuration:

- BIND homepage: http://www.isc.org/products/BIND

- Ask Mr Dns, "How to Properly set up split DNS in a firewalled environment," URL: http://www.acmebw.com/askmrdns/archive.php?question=408
- Liu, Cricket, "Securing an Internet Name Server," URL: http://www.acmebw.com/resources/papers/securing.pdf

Sendmail:

- http://www.sendmail.org/
- "Allowing controlled SMTP relaying in Sendmail 8.9", URL: http://www.sendmail.org/tips/relaying.html

Apache Web Server

- http://www.apache.org

Netscape Enterprise Server

- http://home.netscape.com/enterprise/v3.6/

Oracle Database Security:

- http://www.oracle.com/ip/solve/security/index.html

Assignment 2: Security Policy

Solaris Hardening for Firewalls:

- Spitzner, Lance, No Title, URL: http://www.enteract.com/~lspitz/core7.txt

Checkpoint Firewall-1 and VPN-1 Configuration Issues:

- Check Point Software Technologies, Ltd., "Remote Access VPN Solutions," URL: http://cgi.us.checkpoint.com/rl/resourcelib.asp?state=1&item=remoteaccess
- Check Point Software Technologies, Ltd., "Why Choose Integrated VPN/Firewall Solutions Over Stand-alone VPNs," URL: http://cgi.us.checkpoint.com/rl/resourcelib.asp?state=1&item=VPNWhyChoose
- Spitzner, Lance, Advanced Perimeter Protection and Defense In-Depth, SANS New Orleans, 2.3, 2001.
- Brenton, Chris, VPNs and Remote Access, SANS New Orleans, 2.4, 2001.

Cisco Router Hardening and Access Lists:

- Cisco, "Cisco IOS Release 12.0 Configuration Fundamentals Command Reference," URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/index.htm

- Cisco, "Improving Security on Cisco Routers," URL: http://www.cisco.com/warp/public/707/21.html
- Cisco, "Increasing Security on IP Networks," URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm
- Keeney, Frank, "Screening Router Access List," URL: http://pasadena.net/cisco/secure.html
- SANS Institute, "Help Defeat Denial of Service Attacks: Step-by-Step," URL: http://www.sans.org/dosstep/index.htm

General VPN Information:

- Bird, Tina. "VPN Info on the World Wide Web," URL: http://kubarb.phsx.ukans.edu/~tbird/vpn.html (April 3, 2001)

SNMP Tools

- GetIf, URL: http://www.geocities.com/SiliconValley/Hills/8260

Assignment 3: Audit Your Security Architecture

Nmap Portscanning tool:

- http://www.insecure.org/nmap

Internet Security Systems Internet Scanner

- http://www.iss.net

Packet Spoofing Tools

- Spoof Library can be downloaded from:

http://209.143.242.119/cgi-bin/search/search.cgi?searchvalue=spoof&type=archives

Assignment 4: Design Under Fire

Fragmented Packet Attack on Firewall-1:

- Spitzner, Lance, URL: http://www.securityfocus.com/archive/1/63478
- Common Vulnerabilities and Exposures Database, URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0482

Jolt program to generate fragmented packets:

- http://www.securityfocus.com/data/vulnerabilities/exploits/jolt2.c
- http://packetstorm.securify.com/0005-exploits/jolt2.c.

TribalFlood2K tool:

- Download from http://mixter.warrior2k.com

- Barlow, Jason, and Thrower, Woody "TFN2K – An analysis," 10 March 2000, URL: http://packetstorm.securify.com/distributed/TFN2k_Analysis-1.3.txt
- Dittrich, David, "Distributed Denial of Service (Ddos) Attacks/Tools," URL: http://staff.washington.edu/dittrich/misc/ddos/

Unicode vulnerability:

- Microsoft Advisory, URL: http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

RDS vulnerability:

- Microsoft Advisory, URL: http://www.microsoft.com/technet/security/bulletin/MS99-025.asp

- Rain Forest Puppy, URL: http://www.wiretrip.net/rfp/p/doc.asp?id=1&iface=2