GIAC Level2: Firewalls, Perimeter Protection and VPN's

Practical Assignment for SANS Baltimore, Md 2001
Version 1.5e

Donna Dance-Masgay
June 2001

TABLE OF CONTENTS

Assignment I - Security Architecture

1.1 Overview

The proposed architecture for GIAC Enterprises concentrates on the protection of the internal network and their assets that applies security in layers. This architecture also takes into account site surveys, current policies (network/security/firewall), and legitimate business needs. There are International partners, who have restricted encryption requirements, customers who need to do transactions online securely, and suppliers who require access to data that is reliable.

GIAC will monitor access into and from their network but the business partners and suppliers will have system administrators who will be specifically responsible for their own hosts and network security.

1.2 Access Requirements

Customers - The customers will be restricted to GIAC's service network via https utilizing the 128 bit encryption scheme in their web browsers. Based upon policy, if a customer requires access, they must be authenticated through username and password.

Suppliers - The suppliers will be able to access GIAC via a secure VPN tunnel between the supplier's firewall and GIAC's external firewall. They would be authenticated by username and password and access the service network or their servers on GIAC's internal network segment.

Partners - The partners are mainly international partners and will be able to access GIAC's network via a VPN tunnel through an ISP to the VPN server where they would be authenticated by username and password. They will be able to access the service network or their servers on GIAC's internal network segment.

Employees - Employees accessing the network from a remote site will do so via an IPSEC VPN Tunnel to the VPN server. Further authentication will be needed depending on their level of access needed.

1.3 Physical Architecture

Internet access will be provided with a T1 circuit. This will provide GIAC's network with good performance and sufficient growth for future expansion. The network will consist of a Border Router, two firewalls, one external and one internal, a hardware VPN server for remote access by partners and employees. The network will be segregated. There will be a service network, which will host the external DNS server, public web server and the mail server. The web and mail servers will be hardened and loaded with anti-virus and policy checking software such as Mime sweeper that does content filtering and virus scans. The internal network will host employee workstations and print servers, the internal DNS, database, time and SYSLOG servers. Access into the service network will be controlled by the external firewall.

The main security components are the border router, external firewall, internal firewall, and VPN server. These elements are discussed below, but it is important to note that the security is not limited to just these components. Several steps have been taken to harden the operating system of each host as well as applied up-to-date patches and proper training for each system administrator of the servers who will be required to monitor these systems. All hosts and firewalls will log traffic and send it to the syslog server based upon their logging policies.

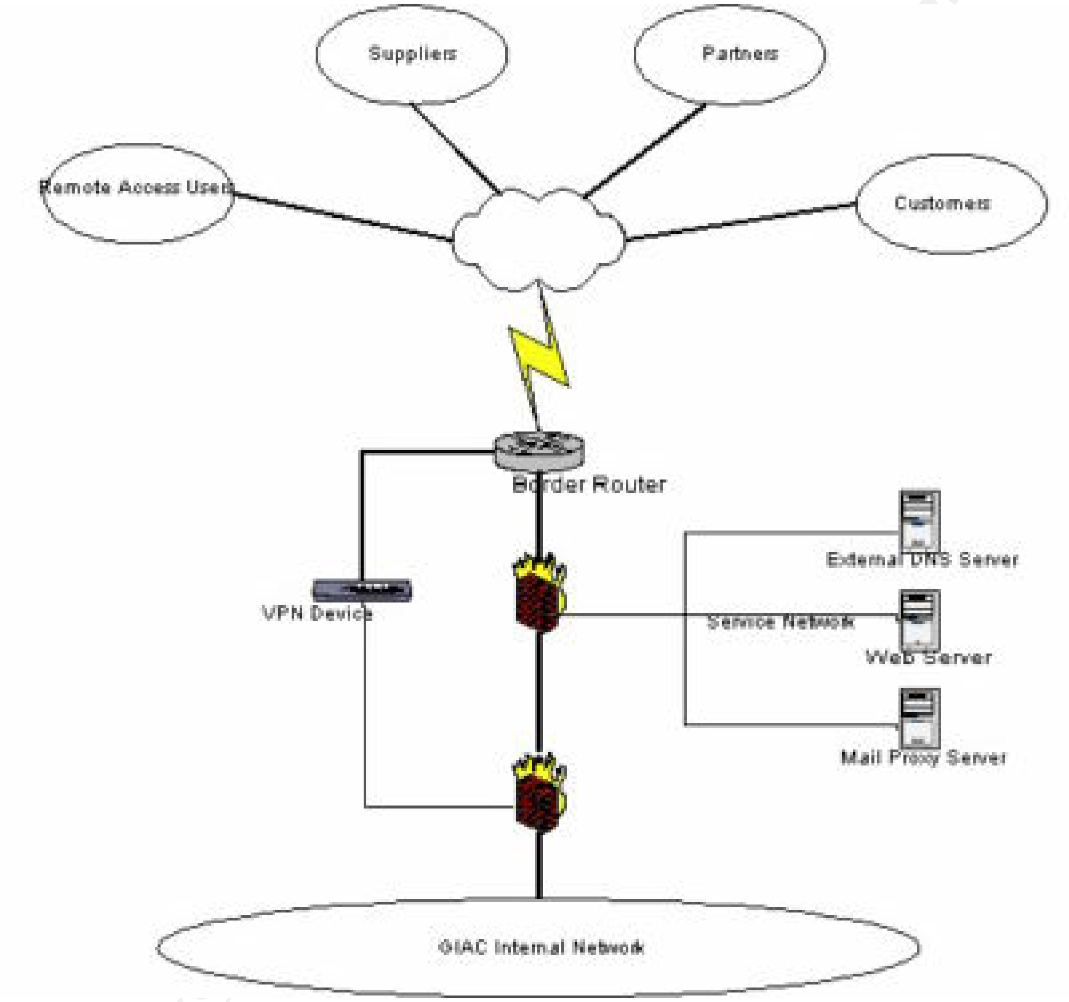
Border Router
The router will be a Cisco 3640, ISO, ver. 12.x with all the latest updates and patches (A list of the current patches available for Cisco is at http://www.cisco.com). The router will be used to block chatty protocols such as netbios, as well as block vulnerable ports and services. The router will also block traffic with invalid source addresses, discard traffic with broadcast /mulitcast source address, deny spoofed traffic and source routing, and limit icmp traffic. No remote logins will be allowed. A hot swappable router will be on-site for fail over.

External Firewall
The external firewall will be stateful, running on a Solaris box with the latest Op.Sys, updates and security patches. The firewall software chosen will be Checkpoint FW1, Ver. 4.1, and SP-3. By stateful, we mean "When a packet is received by the firewall, the first thing it does is check it against the state table to see if there is an existing connection to which this packet belongs. If there is then the packet is forwarded along. If there is no matching connection in the state table for that specific packet, then the firewall compares it against the security policy to see if there is a match that allows the packet to pass. If there is, then the connection is added to the state table and all subsequent packets belonging to that conversation will be forwarded along immediately, without being checked against the policy, making this technology extremely efficient. The command to view the state table is fw tab –t connections -u." Reference the following SANs site listed for further information. http://www.sans.org/infosecFAQ/firewall/inspection.htm

Internal Firewall
The internal firewall will be running on an IBM AIX, Ver 4.3.3 with the latest operating system updates and security patches. The box and OS is hardened. The firewall software is ENetwork, Ver 3.3.

VPN Server
The VPN server will be a Nokia box running Checkpoint FW1/VPN1, Ver 4.1, SP-3 software. The employees requiring secure remote access will utilize Secure remote VPN client software.

1.4 Network Diagram



Assignment II - Security Policy

2.1 Introduction

A security policy is a formal statement of the security regulations intended to protect the organizations critical resources. It reflects the methods used by a company to protect its resources. It also reflects the application of laws, regulations, policies and directives that govern the use and protection of the resources.

There are two areas requiring security policies, ADP Systems and Network Perimeters. These documents are inter-related and necessarily overlap one another in content and areas to be protected. However, there are significant areas of concern in each policy that are not overlapped - Facility security (physical access, fire, water, etc.) in the ADP Security Policy and Network routing (address translation, network protocols, etc) in the Network Perimeter Security Policy. This paper addresses the Network Perimeter Security Policy for GIAC Corporation.

This security policy imposes the following requirements for GIAC resources and network activities

- All connections between GIAC network and the Internet must pass through the Firewall (except for approved, dedicated connections via the VPN) and all connections will be either proxied and/or filtered.
- Only approved network services will be allowed by the Border router/Firewall.
- This policy will be reviewed on an annual basis.
- Requests for modifications to this policy or new services will be submitted to the Network Manager for review.
- Remote connectivity must be approved and must pass through the VPN gateway with the approved authentication/encryption.

2.2 Overview

The following is a general description of the steps that will be taken for each part of the physical architecture that is required for this paper.

Border Router
* Harden the router
* Disable services
* Block IP source routing
* Block IP directed broadcasts
* Restrict administrative access
* Block anti-spoofing (Ingress)
* Block anti-spoofing (Egress)
* Block ICMP traffic inbound on the external interface
* Block RFC 1918 services inbound on the external interface
* Allow SNMP to firewall
* Allow DNS to firewall
* Allow HTTP to firewall
Primary Firewall

* Allow HTTP port 80 TCP traffic to the web server
* Allow HTTP replies to internal private network
* Allow port 53 UDP DNS
* Allow SMTP port 25 TCP traffic to Mail server
* Allow Web server to access database servers via SSL
* Deny all

Secondary Firewall
* Allow HTTP port 80 TCP destined to anywhere
* Allow SMTP port 25 traffic to Mail server
* Allow DNS port 53 UDP to internal DNS
* Allow traffic from VPN
* Deny all

VPN
Implement SHA-1 for an authentication algorithm
The encryption algorithm will be 168-bit Triple DES (IPSEC)
Key Management: Internet Key Exchange (IKE)
Tunneling Protocol: IPSec with IKE Key Management

2.3 Security Policy In-Depth

2.3.1 Boarder Router

Taking the approach of the "Defense in Depth", as recommended by the SANs institute, we will start by securing our Internet access router. We will block protocols and services that are inherently vulnerable and are not necessary for our policy.

Access to the router will not be available via a remote connection. So, we will begin by disabling remote access and allow access via the console only. To gain access to the console we will type at the console login prompt:

```
Line console 0
Login
Password "xxxxxxx"    - xxxxxx will be your password
```

Harden the router with some global security parameters

```
no ip source route                ! Prevent source routing
no service tcp-small-servers      ! Prevent source routing
no service udp-small-servers      ! Prevent source routing
no service finger                 ! Prevent release of user information
no cdp                            ! Prevents the display that it's a
                                  Cisco Router
banner login                      ! Set security banner warning
enable secret                     ! Provide a secure password
service password-encryption       ! Ensure all passwords are encrypted
no ip directed-broadcast          ! Prevent smurf attacks
no ip unreachables                       ! Stops ICMP unreachable messages
logging <host ip addr.>                  ! Logging to another host

Restrict Administrative access
access-list 13 permit x.x.x.x x.x.x.x
        line vty 0 4
                access-class 10
                login
        line vty 5
                access-class 11
                password
```

Establish Ingress ACL

This acl will help prevent DDOS attacks, which is a very common attack that hackers will use to penetrate your network. The router will be setup so it will not receive any packets from private addresses based upon RFC 1918.

```
Interface Serial 0
        ip address x.x.x.x x.x.x.x
        ip access-group 10 in

access-list 10 deny 192.168.0.0 0.0.255.255
access-list 10 deny 172.16.0.0 0.15.255.255
access-list deny 10.0.0.0 0.255.255.255
access-list 10 deny <internal network >
access-list 10 permit any
```

Establish Egress ACL

To ensure that the network will not send spoofed packets, this acl is put in place.

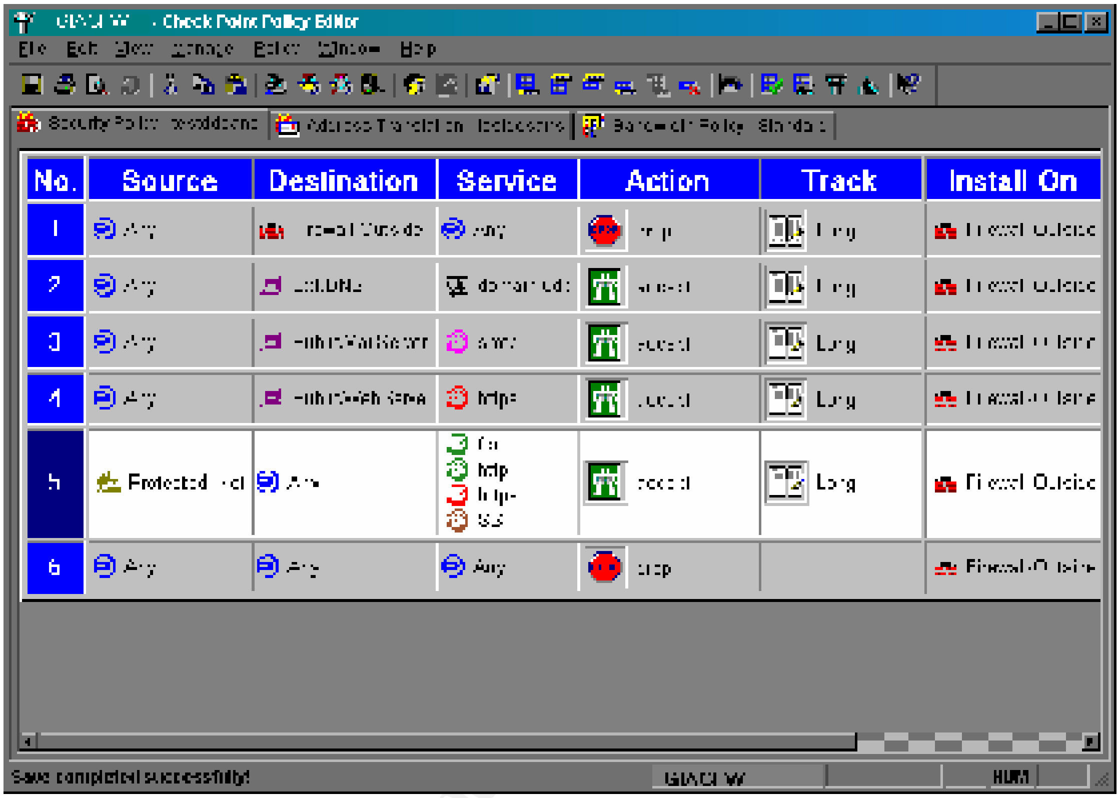
```
Interface Serial 0
        ip address x.x.x.x x.x.x.x
        ip access-group 11 in

access-list 11 permit <your public addr.> x.x.x.x
```

The final step will be to block all other protocols and services that does not have a legitimate business need as recommended by the SANs article, “Securing Your Internet Router”.

2.3.2 External Firewall

The external firewall will be another layer of defense of the "Defense in Depth" strategy. It will provide additional protection for the screened subnet.

There are some default settings that would leave the perimeter vulnerable and need to be shut down. Checkpoint 1 comes with the following ports open by default: ICMP, DNS (UDP and TCP), RIP and FW-1 Management ports 256, 257 and 258.



Check Point Policy Editor

No.	Source	Destination	Service	Action	Track	Install On
1	Any	Firewall Outside	Any	drop	Long	Firewall Outside
2	Any	Ext.DNS	domain-udp	accept	Long	Firewall Outside
3	Any	PublicMailServer	smtp	accept	Long	Firewall Outside
4	Any	PublicWebServer	https	accept	Long	Firewall Outside
5	Protected-net	Any	ftp http https ssh	accept	Long	Firewall Outside
6	Any	Any	Any	drop		Firewall Outside

Save completed successfully!

The external firewall will allow http/https to the web server, smtp to the mail server, and dns requests to the dns server on the screened subnet. The ruleset is as follows:

Rule 1 – It says that any request to access the external firewall will be dropped and logged. We do this because we do not allow any remote access to the firewall.

TEST IT: To test this rule, you can attempt a telnet session to the firewall, if the rule is working correctly, it will not allow the connection.

Rule 2 – It says that any DNS request from anywhere can query the external DNS server.

TEST IT: To test this rule, you can query the external DNS server both from outside and inside the network. Query servers that are on the screened network that would give you an ip address and then query internal servers, which it should not respond to the request.

Rule 3 – It says that any SMTP request from anywhere can query the public mail server.

TEST IT: Attempt to telnet to the SMTP server via port 25 from the outside. If the rule is setup properly, it will allow you send a mail message. Also try to telnet to it from the inside and attempt the same thing.

Rule 4 – It says that any HTTP/HTTPS request from anywhere can query the public web server.

TEST IT: From your web browser from the outside, attempt an http/https session with the web server, if you are able to load the page, the rule is setup correctly. Also try to do the same thing from inside the network.

Rule 5 – It says that anything from the protected network can access anywhere using ftp, http/https or ssh.

TEST IT: Attempt a ftp session from the outside, it should not let you in. Also attempt one from the inside to anywhere, if the rule is setup correctly, it will allow the connection through.

Rule 6 – It says to deny everything else.
NOTE: Checkpoint will automatically put this rule at the end of the rulebase by default.

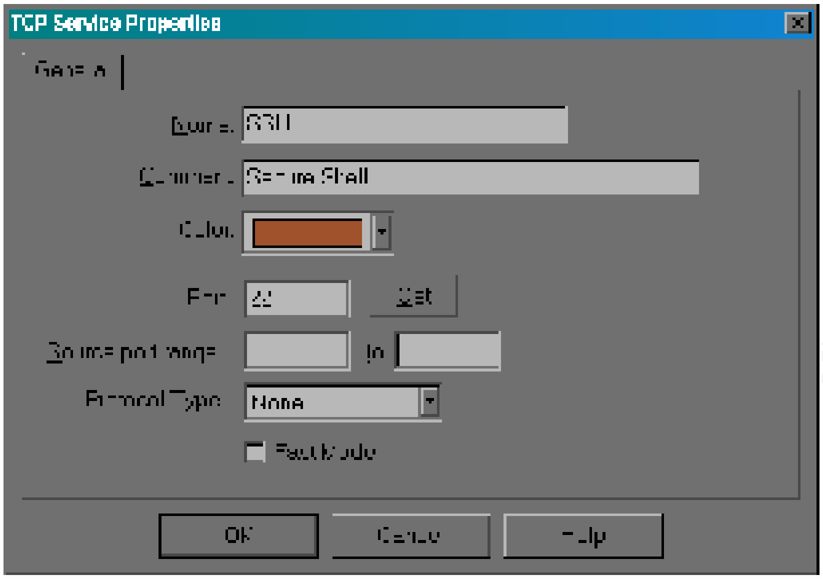
TEST IT: To test this you try several things, but mainly just to attempt using a service not listed above. The connections should be denied.

NOTE: To further test any of these rules, it would also be a good idea to run a port scanning tool like NMAP from the outside to check to see what ports are open.

NOTE: SSH does not come as a default service in Checkpoint as of Ver. 4.1 So we created the service as follows:

Under Policy Editor, click Manage from the top menu,
then click Services, then click add,
For the name, type SSH, in comment type Secure Shell, under Port, type 22.

When finished it should look like this:



TCP Service Properties

General

Name: SSH

Comment: Secure Shell

Color:

Port: 22

Source port range: to

Protocol Type: None

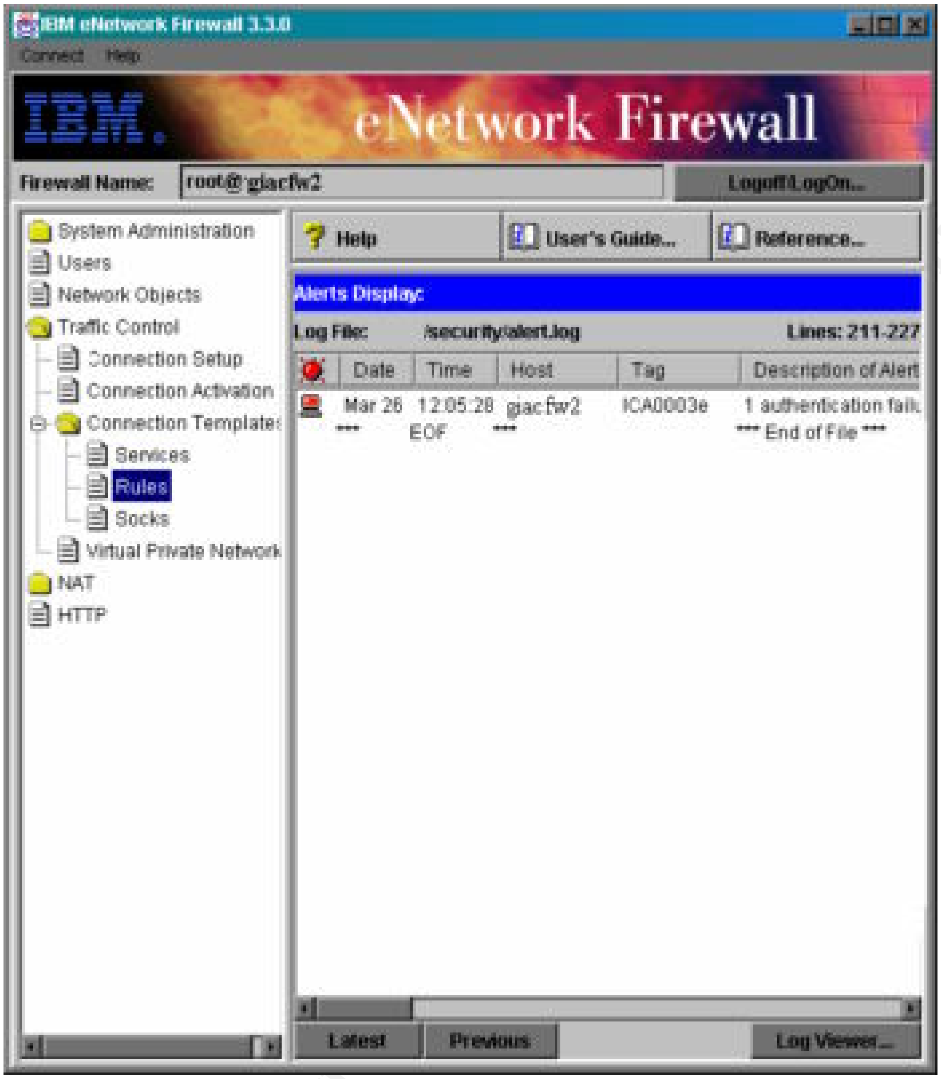
□ Fast Mode

Then click OK to save it.

2.3.3 Internal Firewall

The internal firewall will accept requests from the VPN device to access the internal network. This access will be authenticated by id/password combination.
It will pass SMTP to the internal mail server, it will allow HTTP/HTTPS destined to anywhere, it will allow DNS port 53 UDP to internal DNS
Allow traffic from VPN
Deny all

We will demonstrate how to add a connection from the E-Network menu.
Under *Traffic Control*, click on *Connection setup*, then click *add.*



Firewall Name: root@giacfw2

Alerts Display:

Log File: /security/alert.log Lines: 211-227

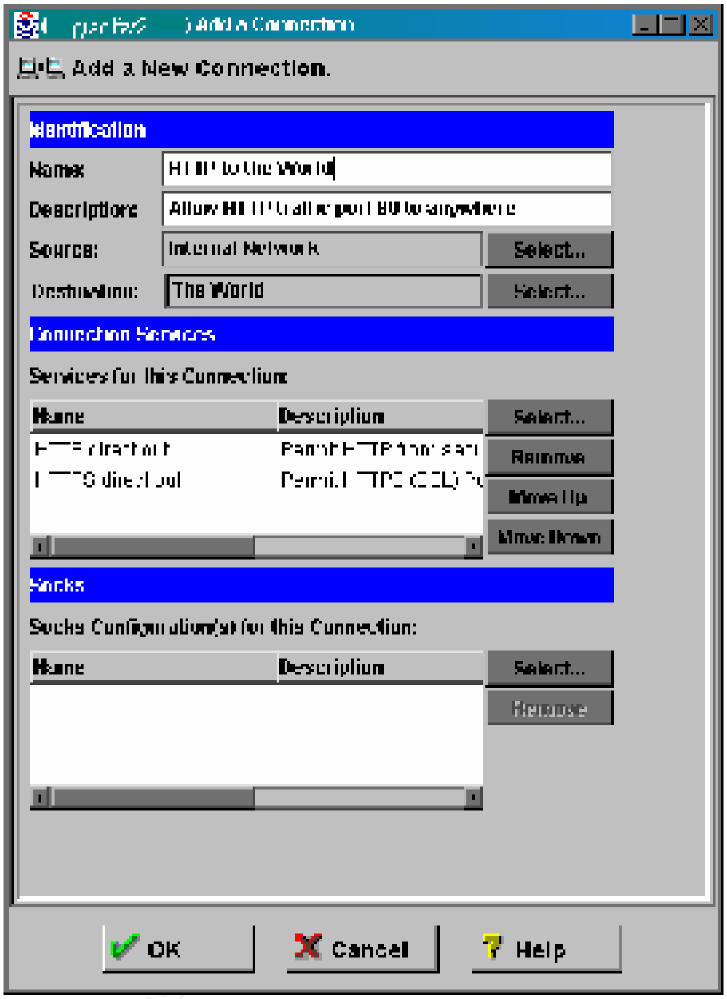
```
Date    Time      Host     Tag        Description of Alert
Mar 26  12:05:28  giacfw2  ICA0003e   1 authentication failu
***     EOF       ***                 *** End of File ***
```

Connections consist of the name of the connection, the source, the destination (these are the network objects which have an associated ip address), and the services that are supported. These services are rule based and indicate the direction of the rule, either in or out of the firewall.

To add the HTTP connection, fill in the *Name* of the connection, the *Description* of the connection, and select the *Services* for the connection. Then click *OK*:

The connection setup looks like this:

NOTE: The connection setup is part of the software that will define the filters on the firewall. It is order dependant with specific rules before general ones. The rules that are used the most are also placed before those, which are not.



Add a New Connection.

Identification

Name: HTTP to the World

Description: Allow HTTP traffic port 80 to anywhere

Source: Internal Network

Destination: The World

Connection Services

Services for this Connection:

Name	Description
HTTP direct out	Permit HTTP from ser
HTTPS direct out	Permit HTTPS (SSL) fr

Socks

Socks Configuration(s) for this Connection:

Name	Description

2.3.4 VPN

The VPN is Checkpoints VPN-1 solution. Our partners who are considered to be trusted will utilize the VPN. The partners can utilize a VPN to VPN scenario or by client to VPN. The Client software that will be provided is Secure remote by Checkpoint. The IPSEC encryption scheme will be IKE/3DES.

The VPN-1 can control the access of the partners to particular applications or to their portion of the network. It also provides authentication to verify the partners are whom they say they are which also ensures the privacy of both gateway-to-gateway and client-to-gateway communications.

2.3.5 Summary of Services:

This list is comprised of the main services and their vulnerabilities that GIAC will need to be aware of that will be permitted. It will also list recommendations to consider for each service that may or may not be implemented on this project.

NOTE:
The services that are going to be used are not full proof against attacks but by being aware of the vulnerabilities in them and logging those services, we will be able to minimize the risks.

Protocols
TCP/IP - TCP is the most used transport protocol on the Internet. it provides for connection-oriented reliable packet services. Each packet or sequence of packets must be acknowledged by the receiving host.

Vulnerabilities: Attack methods that are generic to TCP include packet spoofing (injecting false packets), IP address spoofing (injecting packets that contain the "from" address of a trusted host), sequence number attacks, and sniffing (interception of traffic).

Recommendations: Many TCP services may safely be forwarded through a secured perimeter. A defense in depth approach in addition to continual monitoring will reduce the risk.

UDP - UDP is another commonly used transport protocol, providing for stateless, fast, but unreliable packet service. UDP packets are not acknowledged, and there is no guarantee of their delivery.

Vulnerabilities: The attack methods generic to UDP include packet spoofing (injecting false packets), IP address spoofing (injecting packets that contain the "from" address of a trusted host), sequence number attacks, and sniffing (interception of traffic).

Recommendations: It is easier to spoof UDP that it is to spoof TCP due to the lack of an acknowledgment of packets. Thus, the spoofed host will continue to communicate because of unacknowledged packets and the spoofing software is not required to predict packet sequence numbers. Only the required UDP services should be allowed through the perimeter.

Network Services
SMTP - is text-based, that is, the synchronization of mail agents and the addressing of mail. It is a common means of sending and receiving electronic mail throughout the Internet.

Vulnerabilities: SMTP is text-based, the synchronization of mail agents and the addressing of mail messages are accomplished via a two-way communication using clear text messages. Electronic mail messages can be intercepted by network sniffing. There is the possibility of data-driven attacks or the ease of mail forgery. Because of their complexity, these servers contain many bugs and features that can be exploited to cause damage to a network. For example, sendmail features, such as being able to send mail to a program and the bug feature, left many systems open to attack.

Recommendation: A secure mail forwarder can protect systems against flawed SMTP-based servers. By the employment of a secure mail forwarders and the mail agent for the protected domain SMTP electronic mail may be allowed inbound and outbound through the firewall. This mail forwarder should be run a screened network or DMZ off of the firewall. As a precaution, hosts requiring the sendmail agent should run the most up-to-date version of sendmail.

HTTP - is the basis for the World Wide Web, providing the most user-friendly interface to the Internet. HTTP servers use TCP port 80 as the default but are configurable to allow other ports as well.

Vulnerabilities: Risks inherent in HTTP include the disclosure of information such as credit card numbers and the discovery of Web pages through the use of link pointers. As the protocol and types of services grow, more vulnerabilities are being discovered. These include the ability of malicious programs written in mobile code such as Java script or Visual Basic languages to download malicious code or to mail sensitive files to the attacker without the consent or knowledge of the users. HTTP servers allow unchecked information, documents, and programs to be retrieved, allowing for the possibility of the introduction of a virus or Trojan Horse, many of which can be discovered via anti virus tools. HTTP servers may also be configured to run on nonstandard ports. There is a risk of having a server run on a port that is not blocked by the border router or firewall.

Recommendation: Use available HTTP proxies in concert with strong authentication to prevent access from unwanted parties. Outbound connections should be routed through the proxy. Inbound connections should be blocked using port filtering techniques.

An alternative is to use a split -server approach by installing a server outside the firewall containing documents for public consumption and a protected server inside the firewall containing documents for internal use only. The two servers should communicate with each other using Secure Socket Layer (SSL) or Secure HTTP combined with IP address filtering. Inbound connections to the internal server would be disallowed via IP port filtering. Inbound traffic destined to nonstandard ports used by HTTP servers should be blocked at the firewall

DNS - operates on TCP and UDP port 53. It provides a mechanism for translating a host name to an IP address and vice versa. DNS also provides translations for mail host addressing.

Vulnerabilities: Allowing external access to DNS may provide an attacker with a means to obtain a complete list of firewall-protected hosts by way of a DNS zone transfer. Host information and mail routes could also be compromised. If the name server is configured incorrectly, an attacker may cause false information to be loaded into the name servers cache. IP spoofing attacks to DNS could allow an intruder to gain unchallenged access if a remote connection to a host is based on access control list that relies on the name of the remote host.

Recommendation: Install a split server configuration using two DNS servers ,one inside and one outside. All hosts inside the firewall should be configured to look to the internal DNS server for name resolution. All hosts outside the firewall will look to the external DNS server for name resolution.

Use IP port and address filtering to allow traffic between the internal and external DNS servers. Externally block traffic to the internal DNS server by blocking TCP/UDP port 53 from all external addresses except the external DNS server.

The latest version of bind should be used on all internal workstations.

Assignment III - Audit Your Security Architecture
Since we will provide the technical support for GIAC's comprehensive information systems security audit as well as audit the primary firewall, we will provide the following approach:

3.1 Approach
As part of the overall technical support for the Info Sys security audit we will:

- Review any written security policies that GIAC may have.
- Evaluate Hosts: hardening of the os, current os levels & sec. Patches.
- Evaluate perimeter: routers, firewalls, and vpn's.
- Identify all entry points, WAN access, dial-in, etc.
- Identify threats it would be most susceptible to, i.e., DDOS, Web defacing, etc.
- Test each rule/acl for perimeter devices to ensure they are doing what they are supposed to do.
- Perform a vulnerability test on each component to see if there are any holes.
- Time of day would be early morning to take into account the international partners (around 2:00am) and weekends to recover any systems that may have been aversely affected by the testing.
- Costs would include:
- Planning/Evaluation of materials - 2 days
- Perimeter Assessment/Testing – 1 day
- Internal Network Assessment/Testing – 1 day
- Documentation – 3 days

Total Cost : $1,500/day = $10,500

- Level of effort would require 2/3 people in Network and System Security.

3.2 Implementation

There are some powerful network tools we can use for our tests and are freely available. This was taken directly from www.insecure.org top 50 tools list.
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. Nmap runs on most types of computers, and both console and graphical versions are available. Nmap is free software, available with full source code under the terms of the GNU GPL.

Tcpdump - A powerful tool for network monitoring and data acquisition. This program allows you to dump the traffic on a network. It can be used to print out the headers of packets on a network interface that matches a given expression. You can use this tool to track down network problems, to detect "ping attacks" or to monitor the network activities. http://www.tcpdump.org

Snort - flexible packet sniffer/logger that detects attacks Snort is a libpcap-based packet sniffer/logger, which can be used as a lightweight network intrusion detection system. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more. Snort has a real-time alerting capability, with alerts being sent to syslog, a separate "alert" file, or even to a Windows computer via Samba. http://www.snort.org

Sam Spade - http://www.samspade.org/**:** Online tools for investigating IP addresses and tracking down spammers.

For our audit of the Primary Firewall we will use nmap:

We downloaded nmap on a laptop running linux, uncompressed the file, compiled it and ran make.

Step 1 - Verify the policy is doing what it is supposed to do.
From outside the firewall, we would test to see if the firewall is enforcing the policy by testing each rule as stated in our external firewall policy in the previous section. We will test all inbound connections that include the screened network as well as the internal network. We would then test the firewall for any unsupported services using a port scanner such as nmap. (http://www.insecure.org/nmap/). We can also use the netstat command to help assess to see which ports are opened on the host itself.

For our test we will use nmap. This test is a simulated test of what you would find after running nmap against the targeted host.

First we will run the command to test for tcp ports using the SYN flag. The -v stands for verbose. The -sS stands for The SYN flag will test for half open ports.

```
#./nmap -v  -sS giacfw
Starting nmap V. 2.53 by fyoder@insecure.org (http://www.insecure.org/nmap/)
Host  (192.168.1.10) appears to be up ... good.
Initiating SYN half-open stealth scan against (192.168.1.10)
Adding TCP port 80 (state open).
Adding TCP port 443 (state open).
Adding TCP port 25 (state open).
The SYN scan took 1 second to scan 1523 ports.
Interesting ports on   (192.168.1.10):
Port            State           Service
25/tcp          open            smtp
80/tcp          open            http
443/tcpopen             https
```

Next we will scan for UDP ports. The -v stands for verbose. The -sU stands for UDP.

```
#./nmap -v  -sU giacfw
Starting nmap V. 2.53 by fyoder@insecure.org (http://www.insecure.org/nmap/)
Host  (192.168.1.10) appears to be up ... good.
Initiating FIN, NULL, UDP, or Xmas stealth scan against  (192.168.1.10)

The UDP or stealth FIN/NULL/XMAS scan took 4 seconds to scan 1448 ports.
Interesting ports on  (192.168.1.10):
The 1444 ports scanned but not shown below are in state closed)
Port            State           Service
53/UDP          open            domain
```

From inside the firewall we would:

Check to see if the services we want to support are the only ones allowed through. We will also test for unsupported services. We can do this by running nmap to see what ports are open.

Verify we can access the services that are accessible, DNS, Mail, Web). We would do this by attempting connections to the servers on the screened network as well as Internet connections.

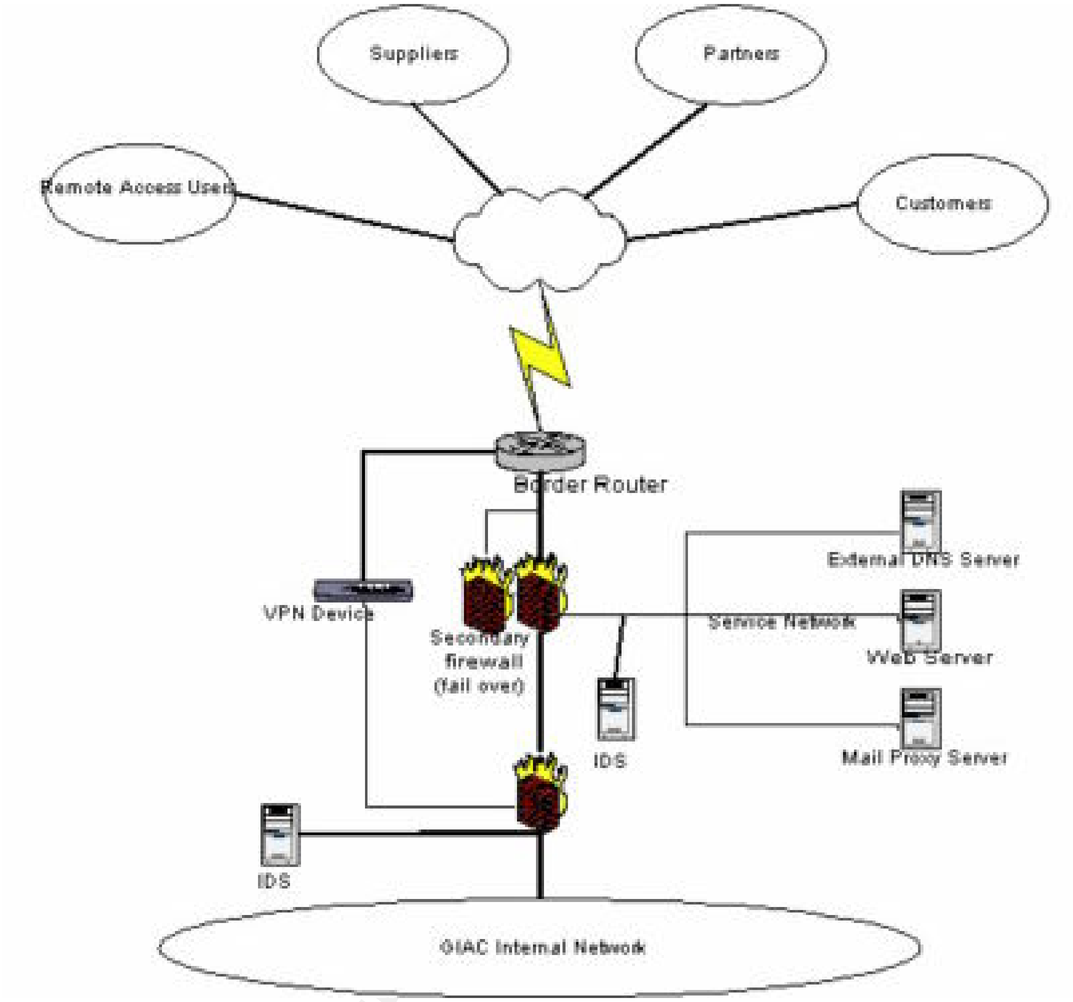
Test all outbound connections from the internal network and from the screened network out through the firewall. We can do this by sending an email message to somewhere outside the perimeter, use our web browser to browse the Internet, perform nslookups.

3.3 Analysis/Recommendations

Based on the previous assessment, we found the network was subject to a single point of failure at the primary firewall. We would recommend configuring the VPN which is

Checkpoint VPN1 be configured as a backup for fail over or purchase another firewall. Nokia will allow you to use another firewall to provide fail over capability by enabling VRRP on both firewalls and assigning address space for the backup firewall ip address. This is just a primary/secondary setup so the secondary firewall will not see any traffic unless the primary firewall fails. We would also recommend using an ISS scanner to further enhance our logging capabilities and early detection of any suspicious activity. Further research on the firewall software by the vendor has also revealed that Enetwork software will no longer be supported after June 2002 so a replacement firewall software will be necessary.

With these recommendations the network would look like this:



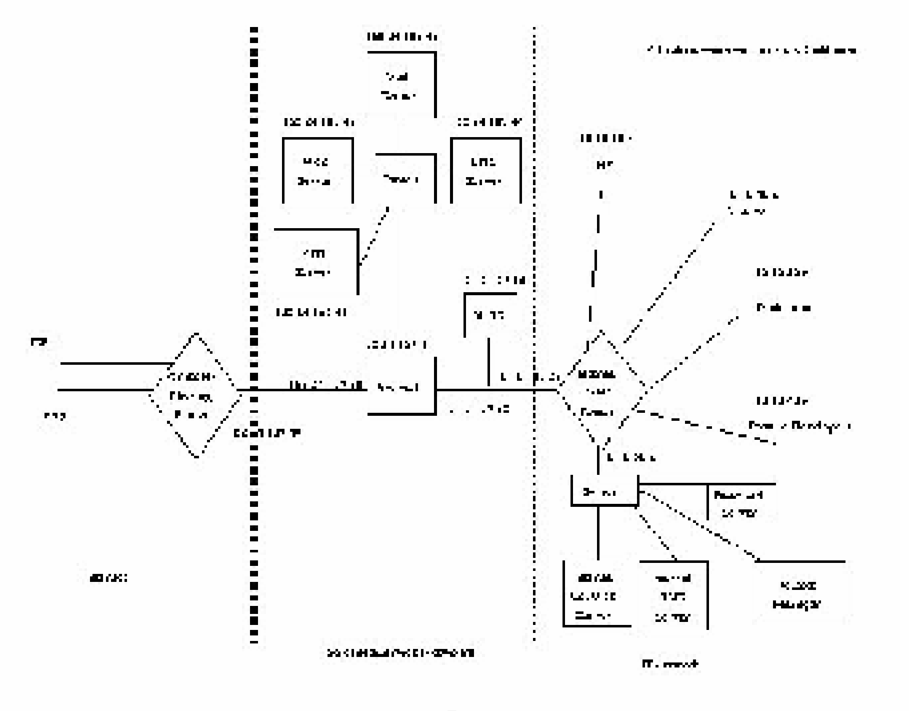
Additional recommendations

- Recommend future audits of the perimeter performed every year and vulnerability assessments every six months and after any change to the firewall rulesets.
- Subscribe to an advisory/alert bulletin board such as CERT or bugtraq as well as keep up on platform specific security advisory bulletin boards.

Assignment IV - Design Under Fire

4.1 An attack against the firewall itself

This attack is taken from Heather Bard practical. It is located at
http://www.sans.org/y2k/practical/Heather_Bard_GCFW.doc



She is using an Axent Raptor firewall. The platform is not mentioned so I went to bugtraq to find out vulnerabilities on the Raptor firewalls. I discovered bugtraq #2517. This vulnerability is based on ver.6.5 and taken directly from bugtraq:

Raptor Firewall HTTP Request Proxying Vulnerability

Raptor Firewall is a product distributed and maintained by Axent Technologies, Inc. Raptor is an Enterprise-level firewall, providing a mixture of features and performance.

A problem in the software package could allow intruders access to private web resources. By using the nearest interface of the firewall as a proxy, it is possible to access a system connected to the other interface of the firewall within TCP ports 79-99, and 200-65535. The firewall will only permit connections to the other side on ports in this range, excluding port 80, and using HTTP. This affects firewall rules that permit HTTP traffic.

Therefore, it is possible for a malicious user to access internal web assets, and potentially gain access to sensitive information. It is also possible for an internal user to gain access to external web resources through the firewall, providing the resources are not running on the default port 80. < http://www.securityfocus.com/bid/2517 >

An attacker could configure a browser to use IP address of Raptor firewall as an HTTP Proxy, then begins probing internal network. Probes can reveal vital information about the company. We could do port scans of the internal network and obtain ip addresses of internal servers, crack internal passwords using password cracking tools, plant virus' or trojans, etc.

4.2 Design a Denial of Service Attack Against the Network Design

TCP is a connection-oriented protocol that maintains state. A SYN packet sent to a open port causes a RTS-ACK packet to be sent to the spoofed IP address. If it exists, the spoofed ip address responds to this unexpected SYN-ACK with a RST back to the victim's machine. If the spoofed address is not reachable, the router would send an ICMP Destination unreachable message. The victim's machine continues to send SYN-ACKs and continues to ignore the ICMP error message. The victim's machine ignores the ICMP messages because it thinks there is a temporary network problem. It will continues its attempt to complete the three-way handshake until its TCP timer times out. This type of attack eats up the bandwidth and slows down traffic or eventually stops traffic until the TCP timer times out.

4.2.1 Counter Measure – Cisco Router

* On the Cisco router, use ip verify unicast reverse-path interface command. This command will check each packet routed into the router. If the source ip doesn't have a route in the CEPF tables which points to the same interface the packet was received on, the router will drop the packet. This will stop SMURF attacks and other attacks that depend on source ip address spoofing. It is important for CEF to be turned on in the router.

* Filter all RFC1918 address space using access control lists.

```
Interface xy
    ip access-group 101 in
            Access-list 101 deny ip 10.0.0.0 0.255.255.255 any
            Access-list 101 deny ip 192.168.0.0 0.0.255.255 any
            Access-list 101 deny ip 172.16.0.0 0.15.255.255 any
            Access-list 101 permit ip any any
```

* Apply ingress and egress filtering using ACL's. (based on RFC2267)
Use CAR to rate limit ICMP packets

* Configure rate limiting for SYN packets

Compromise an internal system through the perimeter system, select target, why target, process to compromise the target

The target selected for this paper is the Internal DNS Server. I have selected that target because it would give me the most information on servers on the internal network. The process would require to gain access the internal network. Utilizing the attack against the primary Raptor firewall, I could configure a browser set to the ip address of the firewall. The firewall will allow access through to the other side and into the internal network. Once inside, I can probe the network to get the internal ip address of the server I wanted, run a password cracking tool against it to gain root access and establish a backdoor for future use.

References:

Albitz, Paul, Liu, Cricket. DNS and BIND. 3'rd ed. O'Reilly, 1999

Northcutt, Stephen, Mark Cooper, Matt Fearnow, Karen Frederick. Intrusion Signature and Analysis. New Riders, 2001

Tiso, John. Securing Your Cisco Router, SysAdmin Magazine, July 2001, Vol.10, Nu.7

Brenton, Chris. Firewalls 101: Perimeter Protection with Firewalls, Sans Institute, May, 2001

Additional references:
Cisco Strategies to Protect Against DDoS Attacks
http://www.cisco.com/warp/public/707/newsflash.html

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

Improving Security on Cisco Routers
http://www.cisco.com/warp/public/707/21html#encryption

Securing Your Internet Router
http://www.sans.org/infosecFAQ/firewall/router.htm

Silvia, Tara "Firewall and Perimeter Protection" Practical Assignment SANS, March 2001
http://www.sans.org/y2k/practical/Tara_Silvia.doc

Firewall Failover Using Nokia Firewalls and VRRP
http://www.hanetworks.com/networkds/nokia/vrrp/Jason-Mogavero-VRRP.html

ICSA Firewall Policy Guide http://2cobbs.com/firewalls/index.html

Bugtraq http://www.securityfocus.com

Assignment 1 - Security Architecture (25points)
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, VPN's 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).

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 the 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!

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:

- The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
- Any relevant information about the behavior of the service or protocol on the network.
- The syntax of the ACL, filter, rule, etc.
- A description of each of the parts of the filter.
- An explanation of how to apply the filter.

  If the filter is order-dependant, 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.)
- Explain how to test the ACL/filter/rule.

-

Be certain to point out any tips, tricks, or “gotchas”.

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 hare 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.

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

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 our 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.