Global Information Assurance Certification Paper

GIAC Enterprises

GCFW Practical Assignment
Version 2.0
By Andrew Walker

1.1 Abstract

GIAC Enterprises is a ".com" based out of San Francisco, California. A University of Wisconsin – Madison student, who graduated with a B.S. in Computer Science and a business idea, founded GIAC Enterprises in 1998.

GIAC Enterprises specializes in the redistribution of fortune cookie saying. GIAC receives their sayings from several different suppliers, then reformats these sayings and redistributes the finished product to the maker of the actual cookie and GIAC's international partners. This finished product is a text document with the saying ready to be cut into pieces and inserted into the cookies.

The original network infrastructure was started with a Hewitt Packard PC and an externally hosted web page. Over the years this company has survived the ".com" crash and expanded its fortune cookie saying business into an enterprise. With the companies expansion the network infrastructure has expanded as well. GIAC is still a privately held company and thus has a tight budget for its IT needs.

GIAC's owner/founder is a visionary man and realizes that his company needs to take its first steps into the global market. With this expansion, he also realizes there will be additional IT needs that cannot be facilitated with GIAC's current IT network. The scale of this project was too large for the owner/founded to take on himself, therefore he hired Secure Consulting to design, implement and test his new enterprise network.

1.2 Current Architecture

Currently, GIAC has a small, but semi-functional network. The major problem is security. Function was GIAC's number one priority and security was always an afterthought. Recently, due to global viruses and cyber-terrorism, customers and suppliers have been concerned about the security of their orders and assets. Credit cards are not being processed in a secure manner, which is causing loss of market credibility. Also, fortunes are being transmitted in the clear. This means that anybody with a packet-sniffing tool can steal these valuable fortunes. Currently, this is Dell workstation/server environment with a Cisco 3745 router. The new architecture will use all of the old technology with the addition of new equipment.

1.3 Phase One Meeting

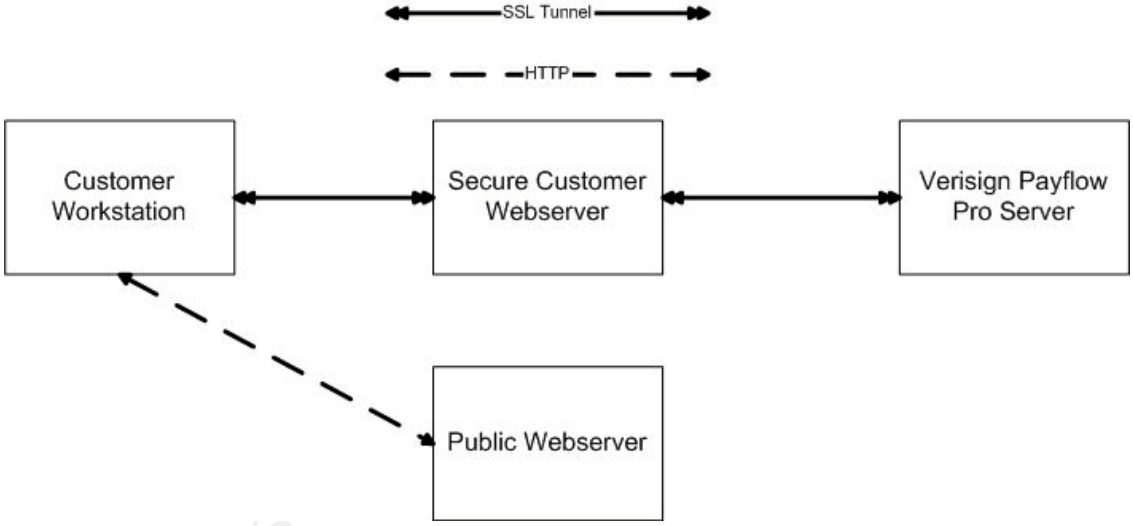
This meeting was created by Secure Consulting to better understand their customers' needs. During this meeting five network user groups were defined. These user groups included: customer, suppliers, international partners, internal employees, and mobile sales force/teleworkers. Secure Consulting noted each group's specific network needs. Down time for the new networks integration was

also determined at this meeting. Because of a limited budget redundancy will not be incorporated into the first instantiation of the update. This limited budget also forces the network to be managed by the current network team. This team consists of two engineers. One engineer will focus on internal system administration and the other will focus on server and hardware security.

1.4 Infrastructure User Group Definitions

1.4.1 Customers:
This group of people will make initial contact to GIAC via the public web, http over port 80. Once an order is initiated customers will connect to a secure customer web server (CustSecWeb.giac.com), via SSL over port 443, where the credit card will be processed. This credit card processing will be done using VeriSign Playflow Pro. This software package connects to VeriSign credit card processing servers, 216.168.255.0/22, using SOCKSv5 over port 443. Once the credit card is deemed valid the customer will be able to download the SSL secured fortunes. The diagram below depicts the customer's traffic flow. [13]

Figure 1.4.1.1 Customer Payment Workflow Diagram



Customer may also have the need to email GIAC employees thus they will need access the mail server using SMTP. Lastly, customers will need access to our DNS information which will be registered on the global DNS server.

1.4.2 Suppliers:
Suppliers in this scenario are very similar to customers. The major difference between the two groups is the direction of their traffic. Suppliers will be uploading fortune cookie sayings, opposed to customers downloading them. To accomplish this the supplier would go to public web page and request access to the secure supplier web server (SuppSecWeb.giac.com). This would again take place through an SSL tunnel. Once the sayings have been uploaded to the secure supplier server and reviewed by a GIAC employee for integrity and quality GIAC Enterprises will pay that supplier by individually predetermined means.

There isn't an automated payment system because of quality control. Payment will only be sent once fortunes have been screened. Payment to suppliers will normally be done manually at the conclusion of each month.

Again, suppliers may need to send emails to GIAC employees, thus they will need access to the mail server. Also, they will be accessing the external web interface, which means they need access to the external DNS information.

1.4.3 Partners:
Partners provide the global aspect of GIAC Enterprises. These are the international companies that translated and resell GIAC Enterprise's fortunes. These companies will connect to GIAC through an IPSEC VPN tunnel ending at GAIC's CyberGuard Firestar 500. The VPN tunnel that is being used for this connection will only give these international partners access to the FTP staging server, which holds the fortune sayings as strings. These partners will also need access to the public web server and GIAC's SMTP server.

1.4.4 GIAC Enterprises employees (located on GIAC Enterprise's internal network):
Internal employees will need different access depending on their job function. All employees will need access to the internal mail server and the external web. Thus, they will need access to such protocols as SMTP, HTTP, FTP and DNS. Some employees will need access to the supplier's web server to confirm supplier's fortune saying submissions. Other employees that will need special access will include system administrators and possibly executives.

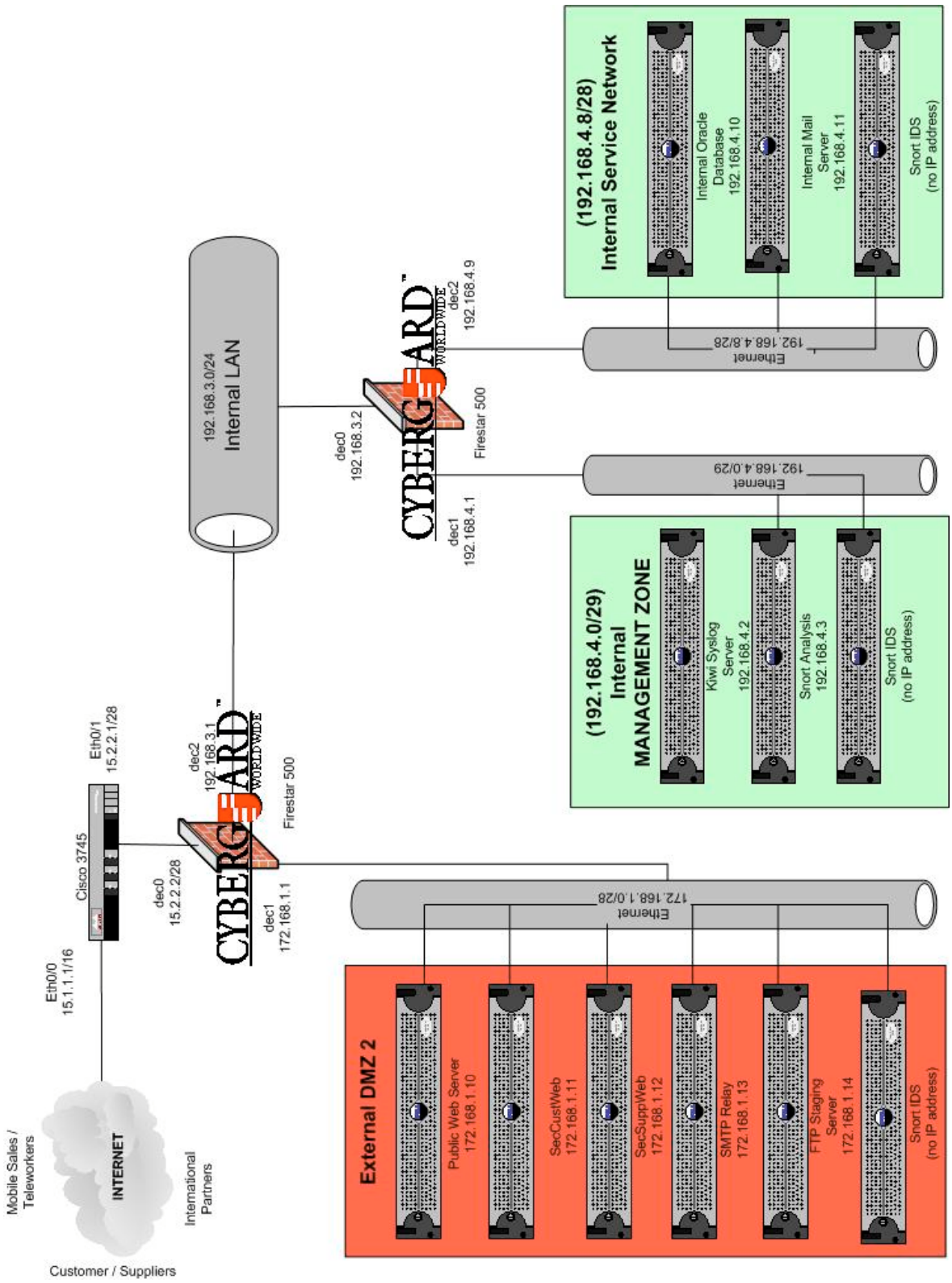
1.4.5 GIAC Enterprises employees (mobile sales force and teleworkers):
This mobile sales force will be accessing the same networks as the internal employees. The difference is that these employees will be connecting through an external SSL tunnel. This tunnel will use the CyberGuard's Passport One application. This application allows the mobile sales force to connect from any IP address, restricting only by authentication. Initially, authentication will be done with a simple username and password. In the future GIAC will request that all employees receive PKI certificates and authentication will be done via PKI. Once the tunnel connects the mobile sales force to GIAC headquarters they will have access to all of the same services that internal employees use.

1.4.6 The General Public:
Must have access to the public web server. This web server will redirect a customer who is purchasing fortune sayings to a secure server. These people will also need access to SMTP server to send email to employees.

1.5 Preludes to Design Review

Secure Consulting made GIAC Enterprises fully aware of this architecture's shortcomings. First, there is a single ISP providing external access to this network. After analyzing the risk-to-reward ratio of getting a second ISP GIAC Enterprises decided to stay with a single ISP, Verizon, providing a T1. Following this idea of redundancy Secure Consulting also made GIAC Enterprises aware of the each chokepoint. These chokepoints include having a single router or firewall at any point on this network. Once again, GIAC Enterprises decided to rely on the response time of IT Team instead of purchasing resources to create proper redundancy.

1.6 Network Upgrade Diagram



1.7 Border Router

In an attempt to reuse any equipment that GIAC already owned a Cisco 3745 running IOS version 12.2 was used as the border router and first line of defense. After analyzing this product and discussing its use with Cisco this router was deemed suitable for today and near future plans. To stay as up-to-date as possible the IOS on this router was updated to Cisco IOS 12.3.

This router has two specific functions. First, and most obvious, this router will interface with the ISP using a static IP address given to us from Verizon, and perform routing. Secondly, this box will provide a base level of security by filtering larger amounts of unwanted packets. This router will filter based on protocol and port. Filtering this traffic at the router will increase the speed and efficiently of our next line of defense, the firewall. This approach displays a defense-in-depth model that was requested by GIAC Enterprises. Once basic packet filtering is done the remaining traffic will be routed to the external firewall.

This router will not be managed remotely. This is a small network with one room housing all of the major networking components. Thus, the router will be managed via console cable. This provides a more secure box when all remote connections can be turned off.

Sending syslog data, via UDP 514, back the Internal Management DMZ will be the means to monitor this router. Once the syslog data enters the management zone it will then be picked up by a Kiwi Syslog server.

1.8 External Firewall

Supporting the defense-in-depth theory the external firewall is a CyberGuard Firestar 500. This firewall was chosen because of flexibility and customizable GUI. Another reason for choosing this firewall was because of its VPN ability. Instead of buying another box to act as the corporate endpoint for the IPSEC tunnels this box will cost effectively assume several roles. After proper training, the existing GIAC IT support team will administer this firewall, thus a firewall with an easy to use GUI was the best idea.

The Firestar will filter all traffic going to and from the border router. This includes:

- HTTP → TCP over port 80.
- HTTPS→TCP over port 443.
- FTP→TCP over port 21.
- SMTP → TCP over port 25.
- DNS → UDP over port 53
- Syslog →UDP over port 514
- Passport One → TCP over port 3443

1.8.1 External DMZ

SMTP Relay:
This server is the external interface for email. When an email request enters the external firewall from the Internet the message will be sent to the SMTP Relay machine. A dirty word search and a virus scan will take place on this server by Trend's Virus Wall package. Once these scans are done the email will be forwarded to the internal firewall. This firewall will proxy email to the internal mail server if, and only if, the source IP address is that of the external SMTP Relay. Mail that is exiting GIAC Enterprises and going to the Internet will go through a reverse process. Once again, these emails will be scanned at the external interface and quarantined if anything abnormal is detected.

Public Web Server:
This web server will hold the public web page for GIAC Enterprise. This web page will be the initial starting page for customer, suppliers and the general public. If a customer would like to initiate an order they will have to click on the "Place Order Now" button. This button is a link to the Customer Secure Web server. If you are a supplier you would choose the "Supplier Entry" button which will redirect you to Secure Supplier Web server

Customer Secure Web Server:
This web server will initiate the SSL connect to the customer's computer and itself. The customer will then be able to browse the external database for the fortune of their choice and select the fortunes to purchase. This will initiate the customer's credit processing, which is done with Verisign's Payflow Pro. Payflow Pro uses SSL to connect to Verisign's processing server, which handles all credit checks and return either an approval or denial code. This is great way to alleviate some of the credit card liability issues. Once the approval code is received the secure customer web server will start uploading fortunes to the customer.

Suppliers Secure Web Server:
This web server will prompt you for a username and password immediately upon entry. The username and password are given to the supplier via sealed envelope once a purchase contract has been signed. This process is not automated for legal reasons given to Secure Consulting during the phase one meeting. Once the supplier logs into the secure web server they have to opportunity to upload fortunes to this server. Employees then review these fortunes before payment is issued to the supplier. Employee review will consist of remotely connecting to the secure server using HTTPS. Once again this process is not automated for legal and quality assurance reasons. Finally, once these fortunes have been scrubbed by GIAC employees, they are moved to the internal Oracle database.

Snort IDS Box:

This box will provide IDS protection for this subnet and send its logs back to the internal management subnet for review.

1.8.2 Internal Network

The internal network will house the internal work force of GIAC Enterprises. Although these are trusted employees of GIAC, for network design purposes they will only be considered *semi-trusted* users. Currently, GIAC employs about 180 on their internal work force. A class C subnet was assigned to this network to allow room for growth. The internal workforce is using Dell Desktops with a hardened version of Windows 2000 as an operating system. These workstations were hardened according to the NSA's Configuration Guide.[12]

1.9 Internal Firewall

Another CyberGuard Firestar 500 will provide the internal network protection of GIAC Enterprise.

This Firestar will filter all traffic going to and from the internal network. This includes:

- SMTP → TCP over port 25.
- DNS → TCP over port 53.
- SYSLOG → UDP over port 514.
- FTP → TCP over port 21.

This firewall will be connected to the internal network of GIAC's Enterprises. The external firewall and the internal firewall will be connected with another IPSEC tunnel in order to transfer data securely through a semi-trusted employee network.

1.9.1 Internal Management Network

Snort IDS Box:
This box will provide IDS protection for this subnet and send its logs back to the Snort Log Analysis server.

Snort Log Analysis:
The second box in this subnet will be a Snort Log Analysis box. All of the Snort IDS servers on GIAC's network will send their log files to this server. From this analysis machine several scripts and GREPs will be done to sort through the log to find potential problems.

Kiwi Syslog Server:
This will be the machine that listens on port 514 for UDP packets. These will be syslog packets from systems throughout the network. These packets will then be analyzed and stored for later use.

1.9.2 Internal Server Network

Internal Database (Crown Jewels): This will be an Oracle 9i database holding the crown jewels of GIAC Enterprises. This server will only by accepting connections from the internal network and the secure web servers. These rules will be enforced by the internal CyberGuard firewall.

Internal Mail Server:
This server will control the internal mail of GIAC Enterprises. Any exiting mail will route through this box to the internal firewall. From there the SMTP traffic will be routed to the external firewall, which will forward it to the external mail relay. This external relay will scan the exiting mail for viruses and perform a dirty word search, finally sending the mail to the outside world. Any incoming mail will route from the external firewall, to the external mail relay. Then, the server will send the scan the email and send this on to internal mail firewall, which will proxy that mail the internal mail server.

Snort IDS Box:
This box will provide IDS protection for this subnet and send its logs back to the internal management subnet for review.

1.10 IP Addressing Scheme

IP Addressing Scheme For Security Components

Machine	Interface	IP Address/Subnet
Cisco 3745 Router	Eth0	15.1.1.1/16
Cisco 3745 Router	Eth1	15.2.2.1/24
CyberGuard Firestar 500 (External)	Dec0 (External Int.)	15.2.2.2/24
CyberGuard Firestar 500 (External)	Dec1 (Internal Int.)	172.168.1.1/28
CyberGuard Firestar 500 (External)	Dec2 (Internal Int.)	192.168.3.1/24
Internal Network	N/A	192.168.3.0/24
CyberGuard Firestar 500 (Internal)	Dec0 (External Int.)	192.168.3.2/24
CyberGuard Firestar 500 (Internal)	Dec1 (Internal Int.)	192.168.4.1/29
CyberGuard Firestar 500 (Internal)	Dec2 (Internal Int.)	192.168.4.9/28

2.1 Security Policies Introduction

This section will discuss the step-by-step process for configuring the security components of this architecture. The filtering policies for the border router and the CyberGuard Firewalls will also be discussed.

2.2 – Cisco 3745 Border Router

This router will be GIAC's only connection to the Internet. This solo connection to the Internet has some pros and cons. Because there is no other entry or exit a successful DoS against this router could render GIAC with no contact to the outside world. This will obviously cut GIAC's connection with customers, partners, and outside sales force, which will result in a loss of income and productivity. A positive side of having a single connection point to the Internet is increased security. With a single router GIAC will know the exact path that any attack will, or has, come through to gain access to any internal servers or workstations. This will also allow GIAC to focus on specific security points when new vulnerabilities are discovered.

This router's primary function is to screen any initial incoming traffic in order to decrease some of the external CyberGuard's filterable traffic. GIAC internal System Administration workforce will be managing this router onsite. Thus, all external services for managing, such as Telnet, will be disabled. If these services were enabled it would increase the box's risk of being breached.

The following configurations of the Cisco 3745 were done in accordance with the Cisco Router Guide.[11]

2.2.1 – Hardening the Cisco Border Router

Before any access-lists can be created the router needs to be locked down. There are several steps to locking down a router including physical security of the area. The following is a step-by-step guide to hardening the configuration of the Cisco 3745 router.

Before anything can be done the router should be given a hostname. Following the theme of 1970's and 1980's metal bands this router was named KISS.

```
Router# config t
Enter configure commands, one per line.  End with
CNTL/Z.
Router(config)#hostname KISS
KISS(config)#
```

Once the machine is named properly a virtual "No Trespassing" sign was added to the router's configuration. This sign is called a banner, which is displayed to whomever gains access to the router before they login.

```
KISS(config)#banner motd %
```

```
Enter TEXT Message.  End with character '%'.
-------------------Warning---------------------
This box is property of GIAC Enterprises.  Any
unauthorized entry is prohibited.  Violators will be
prosecuted to the full extent of the law.
-------------------Warning---------------------%
KISS(config)#
```

Next, user accounts need to be set up for the two network engineers that GIAC employs. These people will have individual accounts with different permission levels. Having separate accounts for each person will provide accountability for any changes made to the equipment. The log file will show who made what changes. Once the user accounts are created the console port can be locked down to only allow login from known users. Before any user accounts are setup the password for the box should be remove and changed to a secret password. The secret command on a Cisco box will type 7 encrypt passwords in the configuration file. Type 7 is a default Cisco level of encryption. Higher levels can be chosen with the proper parameter.

```
KISS(config)#no enable password
KISS(config)#enable secret KISS_RULES
KISS(config)#username jsmith privilege 15 secret
pa55Word
KISS(config)#username jdoe privilege 1 secret
pa55Word2
KISS(config)#line con 0
KISS(config)#transport input none
KISS(config)#login local
KISS(config)#exec-timeout 5 0
KISS(config)#
```

Configuration of this box will only be done from the console port, thus the auxiliary port can be disabled. This follows the theory of anything not being used; whether it is services or ports needs to be disabled.

```
KISS(config)#line aux 0
KISS(config)#transport input none
KISS(config)#login local
KISS(config)#exec-timeout 5 0
KISS(config)#no exec
KISS(config)#
```

The next step in locking down the box includes removing any remote administration ability. Tying a “deny all” access-list to the five VTYs (Virtual Terminal Lines) will disable remote access.

```
KISS(config)#no access-list 90
```

```
KISS(config)#access-list 90 deny any log
KISS(config)#line vty 0 4
KISS(config)#access-list 90 in
KISS(config)#transport input none
KISS(config)#login local
KISS(config)#exec-timeout 0 1
KISS(config)#no exec
KISS(config)#
```

With the default IOS 12.3 load, Cisco has provided a few commands to a level 1 user that are more appropriate for a higher level user. Thus, these commands need to be moved from the level one command pool to the level 15-command pool. The last line is used to move the show command back to level 1.

```
KISS(config)#privilege exec level 15 connect
KISS(config)#privilege exec level 15 telnet
KISS(config)#privilege exec level 15 rlogin
KISS(config)#privilege exec level 15 show ip access-
lists
KISS(config)#privilege exec level 15 show access-lists
KISS(config)#privilege exec level 15 show logging
KISS(config)#privilege exec level 1 show ip
```

Several common vulnerabilities are caused by unused or unneeded services enabled on a box. The easiest way to eliminate these vulnerabilities is to disable any unused services. The first service that NSA[11] points out is the Cisco Discovery Protocol. Cisco products use this service to identify each other on a LAN. This service could allow a hacker to map the network for future attacks. The following line will shut this service down.

```
KISS(config)#no cdp run
```

TCP and UDP have a recommended list of services, hosts should provide. In this network configuration these services are not needed. Thus, they are disabled using the following commands.

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

Unix finger protocol is support by Cisco IOS finger server. These services allow machines to query each other about its logged in users. Once again, in this network this service is considered a security threat and should be turned off with the following command.

```
KISS(config)#no ip finger
KISS(config)#no service finger
```

Some of the newer Cisco IOS releases support a web based remote administration service called http server. Because our network is managed locally this service should be turned off using the following command.

```
KISS(config)#no ip http server
```

Bootp is a protocol that is used on some hosts to load operating systems over the network. Typing the following disables this protocol:

```
KISS(config)#no ip bootp server
```

Cisco routers have the ability to load these configurations from onboard memory or from over the network. Our configurations will be loaded on the NVRAM thus auto-loading can be disabled.

```
KISS(config)#no ip boot network
KISS(config)#no service config
```

IP source routing is another potential problem. Source routing allows a packet to specify it's own route. For security reasons this is not desirable. This service is disabled with the following command.

```
KISS(config)#no ip source-route
```

SNMP can be a useful protocol for health and status checks of network equipment. Unfortunately, there are two problems with SNMP. First, if you are not familiar with SNMP it can be difficult to administer properly. In this case the GIAC SA's that will be managing the day-to-day functions of this network have no SMTP knowledge. The second problem with SNMP is that there have been security flaws brought to light in the past couple of years that could leave GIAC Enterprises vulnerable. For these reasons Secure Consulting, along with GIAC's management, decided to disable SNMP services on all network equipment. Once again, the networking components of this architecture will be residing in one room for ease of monitoring and administrating. The following command will disable SNMP on the router.

```
KISS(config)#no snmp-server
```

By default each interface on a Cisco router supports proxy ARP. This protocol allows ARP to act transparently across two LAN thus breaking the security perimeter between segments. This is seen as security problem in the GIAC architecture and is disabled. Directed broadcast is also a service that needs to be disabled per interface. This service "allows a host on one LAN segment to initiate a physical broadcast on a different LAN segment," according to NSA[11]. In an attempt to make this a difficult network to map some ICMP messages will be turned off per interface as well. Finally, each interface by default has NTP enabled. We will not have a Network Time Protocol Hierarchy included in this

architecture thus this service is disabled. The following commands will disable all the aforementioned services and protocols. The last command on this list will disable a router's ability to forward a packet with no default network route.

```
KISS(config)#int e0/0
KISS(config-if)#no ip proxy-arp
KISS(config-if)#no ip directed-broadcast
KISS(config-if)#no ip unreachable
KISS(config-if)#no ip redirect
KISS(config-if)#no ip mask-reply
KISS(config-if)#ntp disable
KISS(config-if)#int e0/1
KISS(config-if)#no ip proxy-arp
KISS(config-if)#no ip directed-broadcast
KISS(config-if)#no ip unreachable
KISS(config-if)#no ip redirect
KISS(config-if)#no ip mask-reply
KISS(config-if)#ntp disable
KISS(config-if)#exit
KISS(config)#no ip classless
```

2.2.2 Packet Filtering Rules for Cisco Border Router

GIAC's border router will have two extended access-lists. The first access-list will be entitled "InboundTraffic." This list will hold rules dealing with traffic coming from the Internet and entering the router on Ethernet0/0. The second list will be entitled "OuboundTraffic." This list will hold the filter rules for outbound traffic from the firewall to the internal interface, Ethernet0/1, of the router.

2.2.2.1 InboundTraffic

Once in config mode the access-list list can be created and given a name or list number. For ease of use we will use name instead of numbers for our lists.

```
KISS(config)#ip access-list extended InboundTraffic
```

The first rule in the list will block all packets entering the router from the Internet that have an internal IP address. No packet should be entering GIAC's network with an IP address from inside their network. These packets could have malicious intent or could have error causing affects.

```
KISS(config-ext-nacl)# remark -->deny packets w/source IP of
internal network
KISS(config-ext-nacl)# deny   ip host 15.1.1.1 any log
KISS(config-ext-nacl)# deny   ip 15.2.2.0 0.0.0.15any log
```

Next, we will block packets that have a source address from one of the private address spaces defined by RFC 1918. These could be crafted packets that would leave GIAC with no means of tracing their origin.

```
KISS(config-ext-nacl)#remark -->deny packets w/source IP of RFC
                        1918 Private Blocks
KISS(config-ext-nacl)#deny   ip 198.168.0.0 0.0.255.255 any log
KISS(config-ext-nacl)#deny   ip 172.16.0.0 0.7.255.255 any log
KISS(config-ext-nacl)#deny   ip 10.0.0.0 0.255.255.255 any log
```

Any packet using the loopback address as its source will also be blocked. This type of packet can be used in denial of service attacks.

```
KISS(config-ext-nacl)#remark -->deny packets w/source IP of
loopback address
KISS(config-ext-nacl)#deny   ip 127.0.0.0 0.255.255.255 any log
```

This address space is used by the IANA as an experimental zone. These packets should never be allowed into our network because they are most like crafted malicious packets.

```
KISS(config-ext-nacl)#remark -->deny packets w/source IP of IANA
     Experimental Zone
KISS(config-ext-nacl)#deny   ip 240.0.0.0 7.255.255.255 any log
```

This rule will filter incoming traffic from multicast addresses 224.0.0.0 to 239.255.255.255. These packets are unwanted traffic on this network.

```
KISS(config-ext-nacl)#remark -->deny packets w/source IP of
multicast address bloc
KISS(config-ext-nacl)#deny   ip 224.0.0.0 15.255.255.255 any log
```

Next, because our external firewall is also our DNS server, we must allow UDP 53 traffic through the router to the firewall. The following line will permit this traffic.

```
KISS(config-ext-nacl)#permit udp any 15.2.2.2 0.0.0.0 eq 53
```

Because everything will be NATed behind our firewall all exceptable traffic should originate from the firewall's public address of 15.2.2.2. Thus, these packets are permitted.

```
KISS(config-ext-nacl)#remark -->permit only traffic destined for
     internal network
KISS(config-ext-nacl)#permit ip any 15.2.2.0 0.0.0.15
```

Final deny all statement.

```
KISS(config-ext-nacl)#remark -->deny all
KISS(config-ext-nacl)#deny   ip any any log
KISS(config-ext-nacl)#exit
```

2.2.2.2 OutboundTraffic

Once again we must create the extended access-list first. Then add the rules to the list in the order that are to be executed.

```
KISS(config)#ip access-list extended InboundTraffic
```

The first outbound traffic that will be blocked is that of prohibited traffic. This traffic is prohibited because of its inherent security flaws. These two destination

IP addresses are those of AOL instant messenger and GoToMyPC.com respectively.

```
KISS(config-ext-nacl)#remark -->deny prohibited destination IP
     addresses
KISS(config-ext-nacl)#deny   ip any 205.188.6.0 0.0.1.255 log
KISS(config-ext-nacl)#deny   ip any host 63.251.244.169 log
```

The next traffic that is filtered is any packet with a destination of a private address specificied by RCF 1918.

```
KISS(config-ext-nacl)#deny   ip any 192.168.0.0 0.0.255.255 log
KISS(config-ext-nacl)#deny   ip any 172.16.0.0 0.7.255.255 log
KISS(config-ext-nacl)#deny   ip any 10.0.0.0 0.255.255.255 log
```

Any traffic that has a destination of the loopback address will be filtered before exiting the router. This traffic will also be filtered at the firewall, thus this rule is created as a precaution

```
KISS(config-ext-nacl)#remark --> deny packets w/destination of
                        loopback address
KISS(config-ext-nacl)#deny   ip any 127.0.0.0 0.255.255.255 log
```

Block any traffic that is destined for the experimental address block of the IANA.

```
KISS(config-ext-nacl)#remark --> deny packets w/destination of
                     Experimental Block
KISS(config-ext-nacl)#deny   ip any 240.0.0.0 7.255.255.255 log
```

Filter any packets that are destined for a multicast address.

```
KISS(config-ext-nacl)#remark --> deny packets w/destination of
                     Multicast address
KISS(config-ext-nacl)#deny   ip any 224.0.0.0 15.255.255.255 log
```

The following rules are inserted to permit certain types of ICMP traffic to exit this network. These rules are needed to allow certain utilities to run such as ping and tracert.

```
KISS(config-ext-nacl)#remark -->permit outgoing ICMP Traffic
KISS(config-ext-nacl)#permit icmp any any echo
KISS(config-ext-nacl)#permit icmp any any parameter-problem
KISS(config-ext-nacl)#permit icmp any any packet-too-big
KISS(config-ext-nacl)#deny   icmp any any log
```

The last statements will only allow traffic that comes from the firewall to exit this network. Then it will deny everything else.

```
KISS(config-ext-nacl)#remark -->only permit traffic from GIAC's
network
KISS(config-ext-nacl)#permit ip host 15.2.2.2 any
KISS(config-ext-nacl)#deny ip any any log
KISS(config-ext-nacl)#exit
```

2.2.2.3 Binding Access-Lists to Interfaces

Lastly he access-lists must be bound to an interface and the traffics direction. For instance, the extended access-list “InboundTraffic” is bound to Ethernet0/0’s

inbound traffic. It is important to insert all filter rules for an interface per direction into one access-list. Cisco's IOS releases will only allow one access-group to be defined per interface per direction. Thus, current IOS releases can only support one "out" access-group and one "in" access-group per interface.

```
KISS(config)#int eth0/0
KISS(config-if)#ip access-group InboundTraffic in
KISS(config)#int eth0/1
KISS(config-if)#ip access-group OutboundTraffic in
KISS(config-if)#end
```

2.3 External CyberGuard Configuration

This firewall was selected because of its versatility. It will act as the VPN gateway, DNS server, web proxy, and network NAT device. Although, it is better practice to have each box on a network perform one specific task, this is not always the most cost efficient. The CyberGuard allowed GIAC's to keep their initial investment low, but at same time allowing them the flexibility to upgrade the network with minimal headache.

2.3.1 Network Interfaces Configuration

The CyberGuard Firestar comes with six network interface connections. Four of these connections are referred to as 'dec0 – dec3' and the other two will be referred to as 'eeE0 – eeE1.' The eeE ports are "Exempt External Ports" and will not be used in this architecture. To configure the network connection click on System→Network Interfaces. This will open a Network Interfaces window.

Network Interfaces (JeffersonAirplane)					
System Node Name:	JeffersonAirplane				
Registered Domain Name:	giac.com				
Interface	**Type**	**Host Name**	**IP Address**	**Sub-Network Mask**	**Speed/Duplex**
Dec0	External	Public	15.2.2.2	255.255.255.240	Default
Dec1	Internal	ExternalDMZ	172.168.1.1	255.255.255.240	Default
Dec2	Internal	InternalLAN	192.168.3.1	255.255.255.0	Default
Dec3	Disabled				
EeE0	Disabled				
EeE1	Disabled				

For security reasons any interface that is not being used was disabled. Dec0 was configured as an external interface and Dec1-Dec2 were configured as internal interfaces. Setting the 'Type' appropriately is important when creating Packet-Filtering Rules. The speed was set to default for all interfaces; this acts as 'auto' would on a Cisco device.

2.3.2 Host Names Configuration

This is a feature of the CyberGuard firewalls that allow you attach a name with an IP address. This is needed for DNS lookup and easier configuration of Packet-Filtering Rules. Once these host names are entered, Packet-Filtering rules can be created in reference to a name instead of an IP address. This will make the rules easier to read, and thus debug. The following hosts were entered in the firewall configuration.

Host Names (JeffersonAirplane)			
Host Name	**IP Address**	**Aliases**	**Comment**
Localhost	127.0.0.1		Loopback address
Public	15.2.2.2	PublicInt	
ExternalDMZ	172.168.1.1	DMZ	
WebServer	172.168.1.10	WebServer	
SMTPRelay	172.168.1.13	SMTPRelay	
CustSecWeb	172.168.1.11	CustWeb	
SuppSecWeb	172.168.1.12	SuppWeb	
InternalLAN	192.168.3.1	InternalLAN	
BorderRouter	15.2.2.1	Router	
DeepPurple	192.168.3.2	DeepPurple	
StagingServer	172.168.1.14	StagingServer	ftp server for internal partners

2.3.3 VPN Configuration

The external CyberGuard in GIAC's new network architecture will provide a VPN gateway to the mobile sales force, international partners, and the internal firewall. CyberGuard supports two types of VPN's, both of which GIAC will use. The first type of VPN is a gateway-to-gateway connection, which will be used between GAIC, and its international partners, and between the two corporate firewalls. The second VPN type is a host-to-gateway connection, which will be used between GIAC and its mobile sales force. Passport One will facilitate this encrypted path.

We will be using IKE as a method of establishing authentication keys. CyberGuard offers the ability to customize on a per-channel basis. Thus, we can select different IKE parameters for each international partner. IKE parameters consist of two separate parameters, authentication data and IKE data. The authentication data will eventually be configured to use PKI certificates, but until the international partners start using certificates all VPN connections will use pre-shared keys.

IKE data consists of parameter used in the initial IKE negotiation between the two endpoints. The parameters are IKE Protection Strategy, IKE Mode, and a Diffie-Hellman group number used to provide perfect forward secrecy. We will be

using the default values for the IKE Protection Strategy. These values consist of 3des encryption, SHA-1 hashing, and DH group 5, 2, or 1 in that order.[4]

When using CyberGuard's VPN creation tools, the rules are automatically generated, to allow IKE traffic to pass between the two endpoints. The rules that are create will look similar to the following (EndpointA = xxx.xxx.xxx.xxx; EndpointB = yyy.yyy.yyy.yyy) [4]:

```
Permit ike/udp xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy ipsec=default
Permit ike/udp yyy.yyy.yyy.yyy xxx.xxx.xxx.xxx ipsec=default
```

Tutorial: VPN Creation for International Partners (Gateway-to-Gateway)

- Click on Configuration → VPN Secure Channels
- Click on Show Editor
- Channel Name: Paris Supplier
- Peer Type: Gateway
- Hostname: IP address of Paris Supplier (i.e. yyy.yyy.yyy.yyy)
- Establish Key Using: IKE
- Preshared Secret: G1@C_RULE$
- Click on the 'Peer Protected Networks' tab
- Selected Paris Supplier under the VPN Secure Channels
- Click on 'StagingServer' in the 'Choices List' window
    - By doing this we have limited our international partners to the StagingFTP server. This will be a front-end portal to the Oracle database.
- This will configure the connection between EndpointA and EndpointB. Once this is completed any allowed traffic through this tunnel must be specified in the Netguard.conf
    - Click on Configuration→Packet-Filtering Rules
    - At the top of the list insert the following two rules:
        - Permit ftp/tcp yyy.yyy.yyy.yyy xxx.xxx.xxx.xxx ipsec=default
        - Permit ftp/tcp xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy ipsec=default

The host-to-gateway connection, facilitated by Passport One, will be an SSL tunnel. This type of connection will be created differently in the CyberGuard GUI. Passport One will work well for GIAC's mobile sales force because it allows VPN connections from any IP address. For instance, if a sales person was at a Wi-Fi café in the airport he/she could create a connection back to headquarters and conduct business as usual. Their only authentication initially will be a username and password. To setup Passport One follow the instructions below.

Tutorial: VPN Creation for Mobile Sales Force (Host-to-Gateway)

- Click on Configure-->Passport One
- Click on the 'Setup' tab
- Check 'Enable'
- Check 'giac.com (15.2.2.2)' in the external interfaces window.

- Check 'HTTPS' as authentication ports. Use default port 3443.
- Click on the 'Profiles' tab.
- Click 'Show Editor' and insert a name for this profile in the 'Profile Name' field.
- Click the 'Rules' tab.
- Create two rules:

Type	Service	Origin	Destination
Permit	ALL	Firewall	%USER
Permit	ALL	%USER	FIREWALL

- Click Save and close the window.
- Click 'Configure→Users'
- Insert User into table and enable password as external authentication method.

2.3.4 Split DNS Configuration

Domain Name Service is a necessary evil in any company's network and GIAC Enterprises is no exception to this rule. CyberGuard was a good choice for GAIC Enterprises because the Firestar 500 has a built in DNS system. To mitigate traditional DNS vulnerabilities CyberGuard uses two DNS servers on a box. One name server is for the external interfaces and one name server is for in the internal interfaces. The name server information on the external interface is considered public information and the information on the internal interfaces is considered private. The firewall then disallows anything from the outside to view private or internal information. Packet-filtering rules must be setup to allow only the internal DNS to send its information only to the external DNS. This is called Split DNS or Dual DNS and a tutorial on how GIAC Enterprises used CyberGuard's Split DNS functionality is provided below.

Configuring Split DNS

- Click Configure→Split DNS. This will open the 'Split Domain Name Server' window.
- Select 'Enable split Domain Name System' and 'Update packet-filtering rules.'
- Select the 'Servers' tab.
- In the Public Name Server section of the window check the external interface to be used by the public DNS server
- In the 'Forwarder Addresses' in the public section enter the DNS servers of the ISP.
- Select 'None' in the public section's 'Privileged Addresses.' These addresses will be allowed to do zone transfers to DNS.
- In the 'Private Name Server' section select both internal interfaces.
- Enter the IP address of the external interface in the 'Forwarder Addresses' section.
- Enter the IP address of the internal firewall in the 'Privileged Addresses' field. This will allow the internal firewalls DNS to perform zone transfers.

- Leave Default information in the 'Zones' field and add hosts as needed in the 'Hosts' tab.

2.3.5 Smart Proxy Setup (HTTP, HTTPS, FTP, SMTP)

Both firewalls will utilize the Smart Proxy feature provided with the CyberGuard Firestar. The external firewall will act as a web proxy for all HTTP and HTTPS going to the web server and the secure web server. This server will also proxy email, SMTP traffic, to the SMTP relay. Some traffic will then be forwarded to the internal firewall. Once this traffic reaches the internal firewall it will be proxied into the appropriate area. The benefit of the Smart Proxy feature is the automatic creation of the firewall rules. To create the automatic rules set you must select the "Update Packet-Filter Rules" check box.

2.3.5.1 SmartProxies Tutorial (i.e. HTTP Proxy)

- Click 'Configure→SmartProxies'
- Click 'Enable Proxy Service'
- Select 'Inbound to Firewall' and 'Outbound To Firewall'
- In the configuration window below select the 'Setup' tab.
- Check the 'Enable https Throughput' and leave the default port at 443
- Select 'Independent' and the web server handler
- Click on the servers tab and insert IP address or host name of the Web Server.
    - Make sure the above host name is listed in the host file on the CyberGuard.
- Leave the remaining configurations as default.

Once 'Save' and 'Use' are clicked these proxies will be translated into Packet-Filtering Rules and inserted into the netguard.conf file. Below are the rules generated by the above proxy tutorial.

Type	Service	Packet Origin	Packet Destination	Options
Permit	https/tcp	FIREWALL	ALL_EXTERNAL	VSA=true
Permit	ftp/tcp	FIREWALL	ALL_EXTERNAL	VSA=true
Proxy	80/tcp	ALL_EXTERNAL	FIREWALL	VSA=true
Permit	80/tcp	FIREWALL	172.168.1.10	VSA=true
Proxy	80/tcp	ALL_INTERNAL	FIREWALL	VSA=true
Permit	80/tcp	FIREWALL	ALL_EXTERNAL	VSA=true

2.3.6 Final Packet-Filtering Rule Set Analysis

All packet-filtering rules are stored in the Netguard.conf file. These rules are added in the order they are created, which is an important note. When a packet enters the firewall it is compared to the rule set from top to bottom. This packet is then dealt with based on the first rule it matches. TIf no rule matches the packet it will be dropped. In the packet-filtering page each rule has five columns to configure. Table 2.3.6 lists the columns and the options for each column.

Table 2.3.6: Packet Creation Criteria/Options

Action	Service	Packet Origin	Packet Destination	Options
Permit	Service/ protocal	INTERNAL_NETWORK	INTERNAL_NETWORK	ENABLE_REPLY
Deny	Service	EXTERNAL_NETWORK	EXTERNAL_NETWORK	DON'T AUDIT
Proxy	ALL	LOCAL_HOST	LOCAL_HOST	TIME_OUT=nnn
	ALL/protocal	EVERYONE	EVERYONE	NO_IF_CHECK
		if_network nnn.nnn.nnn.nnn	if_network nnn.nnn.nnn.nnn	TCPSYNFLD
				TCPSYNFLD_TIMEOUT=nnn
		Nnn.nnn.nnn.nnn/ subnet	Nnn.nnn.nnn.nnn/ subnet	

The following rules send all traffic destined for the internal firewall through an IPSEC tunnel. These rules are mimicked for each International Partner as these relationships are developed by GIAC. The System's Administrator will insert the appropriate rules into this section when a new VPN link is established. Only the IP address will change.

```
Permit   ALL        FIREWALL       192.168.3.2    ENABLE_REPLY
Permit   ALL        192.168.3.2    FIREWALL       ENABLE_REPLY
```

The only modification to the International Partner VPN's is that these tunnels will only allow HTTP and HTTPS traffic pass. FTP can also easily be enabled if needed.

These next two rules allow Verisigns Credit Card Servers to connect via SSL. These rules have used fake IP addresses and will need to be update with the actual IP addresses from Verisign. The second rule can be modified to allow other connects to the firewall via SSL.

```
Permit  Socks/tcp  216.168.255.0/443  FIREWALL   ENABLE_REPLY
Permit  443/tcp    192.168.3.2        Dec0       ENABLE_REPLY
```

Passport One automatically generated one rule that allows anyone to attempt an SSL connection to the box. It is up to the firewall to authenticate the user at this point. This authentication will initially be done using username and password until PKI certificates are distributed to all employees. The rule associated with this VPN connection does add a level of risk by allowing ALL_EXTERNAL the ability to attempt an SSL connection to our firewall. This risk will be mitigated by locking down a user account after three incorrect password guesses.

```
Permit   3443/tcp   ALL_EXTERNAL   FIREWALL       ENABLE_REPLY
```

Split DNS also created its packet-filtering rule set. These rule sets allow this external box to provide DNS service to the outside DNS machines and DNS lookup for internal users. This rules look redundant because TCP and UDP DNS was allowed.

```
Permit   Domain/tcp  ALL_EXTERNAL   EXTERNAL_INT
permit   domain/tcp  EXTERNAL_INT   ALL_EXTERNAL
permit   domain/udp  ALL_EXTERNAL   EXTERNAL_INT  ENABLE_REPLY
permit   domain/udp  EXTERNAL_INT   ALL_EXTERNAL  ENABLE_REPLY
permit   domain/tcp  ALL_INTERNAL   INTERNAL_INT
permit   domain/tcp  INTERNAL_INT   ALL_INTERNAL
permit   domain/udp  ALL_INTERNAL   INTERNAL_INT  ENABLE_REPLY
permit   domain/udp  INTERNAL_INT   ALL_INTERNAL  ENABLE_REPLY
Deny     domain/tcp  EVERYONE       EVERYONE
Deny     domain/udp  EVERYONE       EVERYONE
```

The following rules address all the various protocols that the external firewall will proxy. These protocols are https, smtp, http respectively.

```
Proxy    https/tcp      ALL_EXTERNAL  FIREWALL
permit   https/tcp      FIREWALL      172.168.1.4
Proxy    https/tcp      ALL_INTERNAL  ALL_EXTERNAL
Proxy    smtp/tcp       ALL_EXTERNAL  FIREWALL
permit   smtp/tcp       FIREWALL      172.168.1.3
permit   smtp/tcp       FIREALL       192.168.3.1
Proxy    smtp/tcp       ALL_INTERNAL  ALL_EXTERNAL
Proxy    80/tcp         ALL_EXTERNAL  FIREWALL
permit   80/tcp         FIREWALL      172.168.3.2
Proxy    80/tcp         ALL_INTERNAL  FIREWALL
permit   80/tcp         FIREWALL      ALL_EXTERNAL
```

Finally, the static routes that the firewall must keep generated the following rules.

```
permit   route/udp      FIREWALL      Dec0_NETWORK
permit   route/udp      Dec0_NETWORK  FIREWALL
permit   route/udp      FIREWALL      Dec1_NETWORK
permit   route/udp      Dec1_Network  FIREWALL
permit   route/udp      FIREWALL      Dec2_NETWORK
permit   route/udp      Dec2_NETWORK  FIREWALL
```

Lastly, we deny anything that is not explicitly allowed.

```
Deny     Any            Everyone      Everyone
```

2.4 Internal CyberGuard Configuration

Adding an internal firewall creates a secondary line of defense for the “crown jewels” of the network. Behind this firewall exists GIAC’s fortunes database, internal mail server, and management network. This firewall will also provide a barrier between the semi-trusted internal network and GIAC’s internal servers.

2.4.1 Network Interfaces Configuration

Three of the six network interfaces on this appliance are being used. Dec0 will be the external interface, which is connected to the internal network. The other enabled interfaces will be internal interfaces that are NAT enabled.

Network Interfaces (DeepPurple)					
System Node Name:	DeepPurple				
Registered Domain Name:	Internal.giac.com				
Interface	**Type**	**Host Name**	**IP Address**	**Sub-Network Mask**	**Speed/Duplex**
Dec0	External	EXT	192.168.3.2	255.255.255.0	Default
Dec1	Internal	ManZone	192.168.4.1	255.255.255.248	Default
Dec2	Internal	ISZone	192.168.4.9	255.255.255.240	Default
Dec3	Disabled				
EeE0	Disabled				
EeE1	Disabled				

Once again, all interfaces not being used will be disabled.

2.4.2 Host Names Configuration

Host Names (DeepPurple)			
Host Name	**IP Address**	**Aliases**	**Comment**
Localhost	127.0.0.1		Loopback address
EXT	192.168.3.2		
ManZone	192.168.4.1		
KiwiSyslog	192.168.4.2		
SnortAnalysis	192.168.4.3		
ISZone	192.168.4.9		
OracleDB	192.168.4.10		
InternalMail	192.168.4.11		

2.4.3 Internal Firewall Split DNS

Similar to the external firewall split DNS is configured on the internal CyberGuard. The only major difference between the configurations of these two boxes is that no privileged users are defined on either the public or private DNS interfaces. This means that no zone transfers can be done to this DNS box. The

basic concept is that in the internal DNS box can communicate out, but the outside DNS box cannot communicate in.

3.1 Network Audit

Before the new network architecture can be transitioned to GIAC's system administrators for life-cycle support a network audit must be performed. By request of GIAC executives a penetration test will not be part of the audit. This audit will only confirm that each security components rule set is performing as expected. The three components that will be audited are:

- Border Router
- VPN
- External Firewall

In an attempt to save money Secure Consulting will not audit the internal firewall. The internal firewall is only needed for added peace-of-mind. The VPN associated with this firewall was already tested as an endpoint for the external firewalls IPSEC tunnel. The FTP and SMTP proxies are the same as the external firewalls, thus should work identically.

Each of these audited components will be tested with two laptops. One laptop will act as the external machine and one will act as the internal machine. The external laptop will run programs such as Nmap[10]. The internal laptop will act as packet sniffer by running Ethereal[9].

Another tool that will be used in this network audit is a simple java program, TestServer.java, which listens for http traffic on a specific port. This tool will be used to test the http proxy rules on the external CyberGuard. Mark Goss wrote this program and source code is provided in Appendix B.

Secure Consulting has coordinated with the GIAC executives and their employees to start the network audit at 6:00 p.m. Pacific Time on Friday. By conducting the audit at this time of day there will be less of an impact on the employees. Another benefit of conducting the audit at this time is that any down time will be tolerated well over the weekend when sales are lower and employees are not working.

3.1.1 Audit Costs

The audit will not require any additional equipment or software. The audit team owns the laptops being used and the tools used for the audit are freeware. The consultant's time will be the main expense for part of the project. Three consultants will perform the audit. Two people actually perform the technical audit and one person will document the process and create an Audit Review Document. A cost analysis is provided below in table 3.1.1.1.

Audit Process	Number of people	Hours/Person	(Cost/Person)/hour	Total
Study security requirements documentation	2	8	$50.00	$800.00
Plan security audit	2	4	$50.00	$400.00
Equipment Setup and Configuration	2	4	$50.00	$400.00
Router Scan	3	6	$50.00	$900.00
VPN Scan	3	6	$50.00	$900.00
External Firewall Scan	3	6	$50.00	$900.00
Evaluate Results	3	4	$50.00	$600.00
Compose Security Profile Document	1	8	$50.00	$400.00
Total				$5,300.00

Table 3.1.1.1

3.2 Cisco 3745 Border Router Audit

The two main purposes of the 3745 router are to filter basic unwanted traffic, entering and exit the network, and to route traffic. This portion of the audit will test the access-lists of the router and static routes insert into the configuration file. For this test the router will first be scanned from the outside of the network to test for proper filtering of incoming traffic.

The first scan that I did against the 3745 was a standard TCP connect port scan. This scan was done with Nmap using the following command:

```
C:\NMAP>nmap -sT -v -O 15.1.1.1

Starting nmap 3.48 ( http://www.insecure.org.namp ) at
2003-10-19 09:30 Eastern Daylight Time
Host 15.1.1.1 appears to be down, skipping it.
Note: Host seems down.  IF it is really up, but
blocking our ping probes, try -P0

Nmap run complete - 1 IP address (0 hosts up) scanned
in 12.508 seconds
```

This output was expected because the Ethernet0/0 on the Cisco router does not except ICMP requests from any IP address. If the inside employees want to test their connectivity they can only ping the inside of the border router, Ethernet0/1.

The next step in the router audit was to scan the router without pinging it. This is a much more stealth means of probing a router. This scan was also recommended by the above Nmap[10] command line output. This type of scan can be initiated in Nmap[10] using the following command.

```
C:\NMAP>nmap -P0 -v 15.1.1.1
```

This type of scan takes much longer to complete then the simple ping scan. While this scan was running I watch the router, via console cable, and noted the following log messages. These log entries are recognizing and blocking notable traffic from 15.1.1.100, which is the attacking machine.

```
%SEC-6-IPACCESSLOGP: list InboundTraffic denied udp
15.1.1.100(0) -> 15.1.255.25
5(0), 1 packet
%SEC-6-IPACCESSLOGP: list InboundTraffic denied tcp
15.1.1.100(0) -> 15.1.1.1(0)
, 1471 packets
%SEC-6-IPACCESSLOGP: list InboundTraffic denied udp
15.1.1.100(0) -> 15.1.255.25
5(0), 4 packets
%SEC-6-IPACCESSLOGP: list InboundTraffic denied tcp
15.1.1.100(0) -> 15.1.1.1(0)
, 1454 packets
%SEC-6-IPACCESSLOGP: list InboundTraffic denied udp
15.1.1.100(0) -> 15.1.255.25
5(0), 4 packets
%SEC-6-IPACCESSLOGP: list InboundTraffic denied tcp
15.1.1.100(0) -> 15.1.1.1(0)
, 1471 packets
%SEC-6-IPACCESSLOGP: list InboundTraffic denied udp
15.1.1.100(0) -> 15.1.255.25
5(0), 4 packets
%SEC-6-IPACCESSLOGP: list InboundTraffic denied tcp
15.1.1.100(0) -> 15.1.1.1(0)
, 614 packets
```

At the completion of the Nmap[10] scan the following output was noted from the command line.

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at
2003-10-19 09:40 Eastern Daylight Time
Host 15.1.1.1 appears to be up … good.
```

```
Initiating SYN Stealth Scan against 15.1.1.1 at 09:40
The SYN Stealth Scan took 1358 seconds to scan 1657 ports.
All 1657 scanned ports on 15.1.1.1 are: filtered

nmap run complete – 1 IP address (1 host up) scanned in
1362.639 seconds.
```

The above command line output combined with Cisco logging message shows that this router is properly filtering unwanted traffic. The auditing the firewall will show that wanted traffic is getting through the router an on to the firewall.

Nmap was also not able to fingerprint the OS running at the IP address of 15.1.1.1. This is because all ports were filtered, which doesn't give Nmap any data to create an OS profile. The following output was recorded when trying to fingerprint the routers OS.

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at
2003-10-19 10:19 Eastern Daylight Time
Host 15.1.1.1 appears to be up … good.
Initiating SYN Stealth Scan against 15.1.1.1 at 10:19
The SYN Stealth Scan took 1358 seconds to scan 1657 ports.
Warning:  OS detection will be MUCH less reliable because
we did not find at least 1 open and 1 closed TCP port
All 1657 scanned ports on 15.1.1.1 are: filtered
Too many fingerprints match this host to give specific OS
details TCP/IP fingerprint:
Sinfo(V=3.48%P=i686-pc-windows-
windows%D=10/19%Time=3F92A37F%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

Nmap run complete – 1 IP address (1 host up) scanned in
1546.724 seconds
```

To confirm what Nmap had outputted and what the router was logging Tcpdump[16] was run inside the router. Tcpdump[16] acts as a packet sniffer running in promiscuous mode. I then ran 'grep' on the output of Tcpdump[16] to show anything that wasn't DNS lookups of my own laptop. Once I did this, all Nmap[10] packets were filtered. The router was successfully blocking the unwanted traffic of the SYN Stealth scan, ping sweep, FIN Stealth scan, and ACK scan.

3.3 External Firewall Audit

The initial firewall scans were run similar to the router scans. First, the attack machine was inserted into the network as an external attacker, which would reside on the Internet. Next, the detection machine was placed in external DMZ. This machine was running Ethereal[10] in an attempt to detect unwanted traffic. This machine was also running Mark Goss's TestServer.java program, which

acts as a mock web server to confirm that wanted http traffic is getting proxied correctly. First, Ethereal was run on the internal laptop and sniffed from traffic as the external laptop ran nmap. During this phase of the test no traffic was detected by Ethereal inside the external DMZ. TestServer.java was then started on the laptop to test for wanted http traffic. IE was then opened on the external laptop to send http traffic the firewall (http://15.2.2.2). Confirming our proxy rule set TestServer.java received http traffic from the firewall. The same proxy rules were used for https and smtp, thus no confirmation will be needed for these rules.

On a negative note Nmap was able to confirm that the firewall had four open ports and was listening for 4 types of traffic. These ports and service are listed below.

- http → port 80
- https → port 443
- DNS → port 53
- SMTP → port 25

Because these are all services that will be needed by GIAC there is no mediation for this. Nmap's output is below.

```
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at
2003-10-19 10:19 Eastern Daylight Time
Host 15.1.1.1 appears to be up … good.
Warning:  OS detection will be MUCH less reliable because
we did find at least 1 open and 1 closed TCP port
Interesting ports on (15.2.2.2):
(The 1597 ports scanned but not shown below are in state:
filtered)
Port       State      Service
25/tcp     open       smtp
53/tcp     open       domain
80/tcp     open       http
443/tcp    open       https
Remote OS guesses: Gauntlet 4.0a firewall on Solaris
2.5.1, Linux 1.3.20 (X86), Siemens 300E Release 6.5,
Raptor Firewall 6 on Solaris 2.6, Solaris 2.5, 2.5.1,
Solaris 2.6- 7 X86.
Nmap run completed – 1 IP address (1 host up) scanned
in 305 seconds.
```

When the OS detection was enabled NMAP was once again not able to confirm OS and offered guesses such as Gauntlet 4.0a firewall, Siemens 300E, and Raptor Firewall 6. Other guesses were various Linux and Solaris OS. Thus, there was no helpful information releases by this firewall for a potential attack on the underlying OS.

The internal monitoring machine was then moved from the external DMZ to the internal network of GIAC Enterprises. The IP address of this laptop was then changed from the address of the web server to 192.168.3.4, which is a valid internal employee address. At this point all the previous Nmap scans were run another time. From inside this network no traffic was detected from Ethereal[10]. Also, TestServer.java picked up no http traffic. These were expected results, thus confirming firewall rule set.

3.4 VPN Audit

The VPN audit will need to be performed slightly different. Ethereal[10] will be used as a packet sniffer, which will watch the packets following the VPN tunnel creation and confirm that the payload of these packets is encrypted. There are several VPN's in this network. First, there is a tunnel established between GIAC and each of its mobile employees. Second, there is a tunnel created between GIAC and each of its international partners. Lastly, there is a tunnel between the external and internal firewalls crossing the internal network. This breaks down into two site-to-site tunnels and one client-to-site tunnel. The same rule sets are used for the two site-to-site tunnels. Thus, only one audit was performed to confirm the creation of both tunnel site-to-site tunnels. All traffic between the two endpoints in this IPSEC tunnel will be encrypted. Thus, a ping test was used to generate traffic, which initiated the tunnel creation. The following Ethereal[10] output verifies that two ping test, and their replies where encrypted between the two endpoints.

No.	Time	Source	Destination	Protocol	Info.
1	.855430	192.168.3.1	192.168.3.2	ESP	ESP(SPI=0xbcb7426)
2	.855641	192.168.3.2	192.168.3.1	ESP	ESP(SPI=0x33cd37b7)
3	1.828506	192.168.3.1	192.168.3.2	ESP	ESP(SPI=0xbcb7426)
4	1.828694	192.168.3.2	192.168.3.1	ESP	ESP(SPI=0x33cd37b7)

The client-to-site connection, to facilitate the mobile sales force, was created with Passport One. Passport One has the ability to create a connection to a mobile user with http, https, or telnet. Because of the sensitive nature of our data we opted to use https. Running Ethereal[10] on the same machine that initiated the tunnel creation, IP=15.1.1.100, found the following traffic. This traffic shows the use of port 443 on the firewall, IP=15.2.2.2, and various encrypted packets sent to authenticate the user. These packet header don't show the encrypted payload, but no user information was sent in the clear during user authentication.

No.	Time	Source	Destination	Protocol	Info
4	3.375996	15.1.1.100	15.2.2.2	TCP	1031 > 443 [SYN] Seq=4162292507 Ack=0 Win=65535 Len=0
5	3.376172	15.2.2.2	15.1.1.100	TCP	443 > 1031 [SYN, ACK] Seq=2680133664 Ack=4162292508 Win=17520 Len=0
6	3.376198	15.1.1.100	15.2.2.2	TCP	1031 > 443 [ACK] Seq=4162292508 Ack=2680133665 Win=65535 Len=0

```
    22 23.457591   15.2.2.2        15.1.1.100      TCP     443 > 1031 [PSH,
ACK] Seq=2680133665 Ack=4162292508 Win=17520 Len=50
    23 23.459313   15.1.1.100      15.2.2.2        TCP     1031 > 443 [PSH,
ACK] Seq=4162292508 Ack=2680133715 Win=65485 Len=44
    24 23.462086   15.2.2.2        15.1.1.100      TCP     443 > 1031 [PSH,
ACK] Seq=2680133715 Ack=4162292552 Win=17476 Len=488
    25 23.476207   15.1.1.100      15.2.2.2        TCP     1031 > 443 [PSH,
ACK] Seq=4162292552 Ack=2680134203 Win=64997 Len=336
    26 23.607763   15.2.2.2        15.1.1.100      TCP     443 > 1031 [ACK]
Seq=2680134203 Ack=4162292888 Win=17140 Len=0
```

3.5 Audit Analysis

Finally, once the data has been gathered the third member of the audit crew begins writing the audit analysis. This analysis will attempt to summarize all the data previously gathered and provide a security assessment.

Finding #1:

First, the audit proved that the border routers configuration was properly filtering traffic. All ports were filtered and no services were left open. The route is using static routes, which eliminates the danger of dynamic routing. Basically, this router is extremely basic; its beauty lays in its simplicity. The only major finding with router was its lack of redundancy. This router should be load balanced with another router and preferably another ISP. This security risk was one that GIAC Enterprises was willing to accept based on the cost difference between solutions. Figure 3.4.1 depicts a properly redundant connection to the Internet. Also, it should be noted that each of the two power sources on the Cisco 3745's should be on different circuits. GIAC is in the process of adding another circuit to their server room to facilitate this requirement.

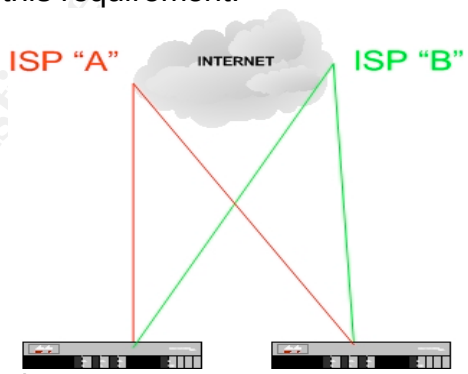


Figure 3.4.1

Finding #2:

The second finding was uncovered at the secondary line of defense, the firewall. When nmap scanned this device four open ports were found. These ports were open for HTTP, HTTPS, FTP, and SMTP services. These services cannot be turned off and this risk was once again accepted. Secure consulting did recommend another firewall approach for better mitigating risk at the firewall. The recommendation was to have a stateful firewall, possibly the Cisco PIX, in

front of a proxy firewall, still using CyberGuard, to act as a single line of defense. This one-two punch at the firewall depth will provide the benefits of both the stateful and proxy firewalls. Figure 3.4.2 shows a generic depiction of this architecture. To make this type of redundancy feasible dynamic routing would be added to the network configuration.

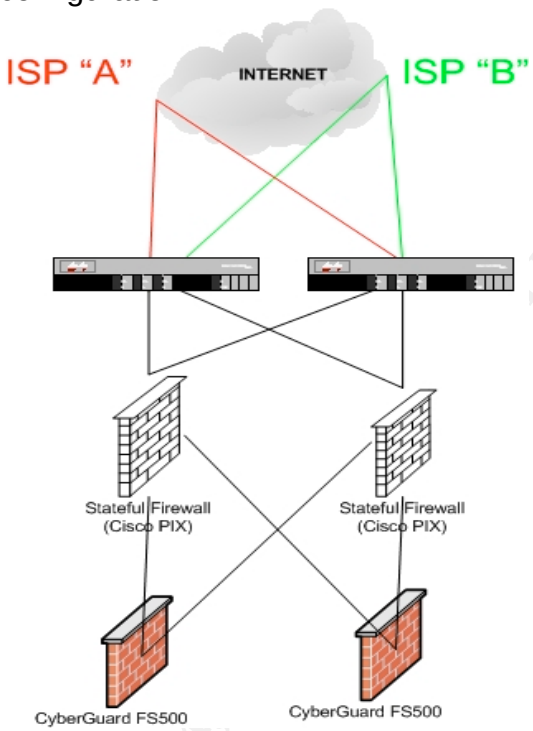


Figure 3.4.2

Finding #3:
The last finding dealt with the mobile sales force VPN connections. After reviewing Passport One's connection to the CyberGuard it was easy to see that any IP address could initiate the connection and then attempt to guess the user password. Granted Passport One will disconnect the attacker after three guesses, but more security could be implemented at this level. Ideally, one would like to be limiting the mobile sales force to specific IP addresses and then only allowing connection to the firewall from those addresses. This would create another barrier for a potential attacker. Unfortunately, it is not practical to have our mobile sales force use static IP addresses. Thus, GIAC will continue to use user authentication only.

Conclusion:
The audit analysis was presented to GIAC's management. All finding were then determined to be acceptable. To resolve the small security flaws would require funds that were not available in GIAC's IT budget. Management felt comfortable with their new defense-in-depth solution. Both parties signed a completion of work contract at this point.

4.0 Design Under Fire

This sections intent is to show security competency through the theoretical attack of another GIAC Enterprise network. The first step in this attack is the select of a passed GAIC practical assignment. The only criteria, as I understood it, is that the practical assignment selected must have been submit in the last six months. After narrowing down the practical to the most current I randomly selected Wolfgang Gottschalk's April 23, 2003 practical assignment.

http://www.giac.org/practical/GCFW/Wolfgang_Gottschalk_GCFW.pdf

Figure 4.1 shows the high-level network diagram created by Wolfgang. His border router is a Cisco 2610 Router running IOS C2600-JK9O3S-M version 12.2(13a). Behind that Wolfgang is using a Checkpoint FW-1 firewall. Wolfgang's corporate intranet uses IP address 10.0.0.1 – 10.0.0.200.

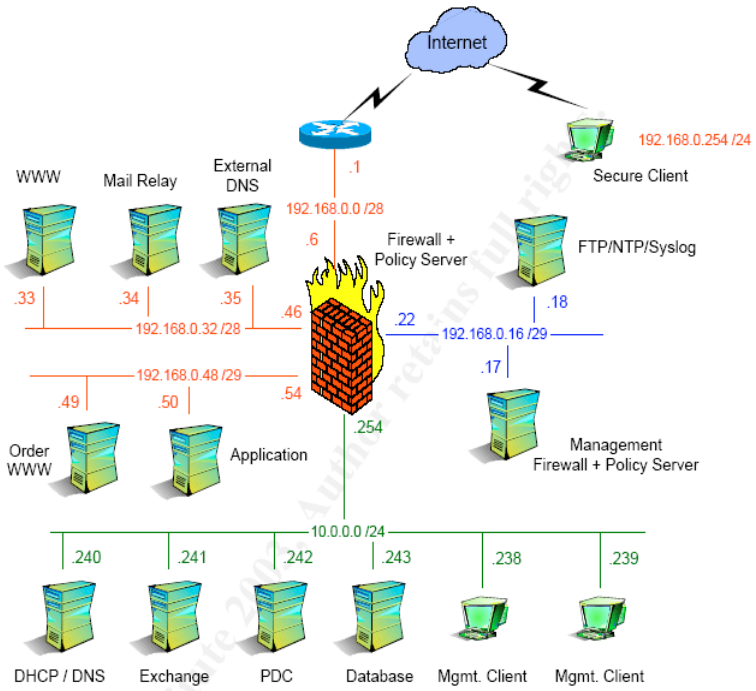


Figure 4.0.1

Three attacks will initiated against this network:

1. An attack against the firewall itself
2. An attack plan to compromise an internal system
3. Distributed Denial of Service attack (DDoS)

4.1 Network Reconnaissance

Before an attack can be successfully initiated critical information about a network must be gathered. To make this process more difficult this information must be gathered in a covert manner. If reconnaissance is performed in an obvious manner any IDS system, or simple log analysis will forewarn the network administrator that an attack is coming. Thus, I few simple techniques are used for reconnaissance.

First, simply going to the target's web page will provide some valuable information. A web page will give information such as email addresses of employees. These email addresses can later be used to send malicious emails or to perform social engineering. The victim's web page will also provide information needed to find IP address ranges. For instances, if I was going to attack www.giac.com, purely hypothetically, I would PING their URL. Although echo requests are not enabled on their border router a ping test will provide an IP address (there are other ways to get the IP address of a URL). I would then take this IP address and run a search against it at the American Registry for Internet Numbers[1]. This search would provide me with the IP address range, and contact information. For instance, I could get a technician phone number, email address, and mailing address through this process. All of this information can later be used for social engineering or as a variable in the actual attack.

Now I have an IP address range to perform more reconnaissance, or the actual attack. Another form of reconnaissance that I might do, once I have the IP range, is a stealth ports scan. The advantage of a stealth scan lies in its ability to space the individual port test out enough to go unrecognized in a log file.

Finally, I might run programs that do passive fingerprinting. Passive finger printing will try to use identifying characteristics of packets to identify the machine they were derived. This type of information could give the attacker the exact model of firewall or router a target is using. This information is invaluable when finding vulnerabilities to exploit.

4.2 An Attack Against the Firewall Itself

At this point I will be assuming that my attempts at gathering valuable network information were successful. I will hopefully have the any email addresses I need, IP addresses to focus attack, and even specific hardware being used on the network. Thus, I will now know that Wolfgang is using a Checkpoint FW-1 as his primary line of defense.

The next step in the attack is to gain vulnerability information about Checkpoint firewall. To do this I research the firewall at several web pages.

- CERT Coordination Center[8]
    - This web page posts known security vulnerabilities and general security practices. This is a great resource for any network security minded individual.

- Packet Storm Security[7]
  - More of a black hat site then CERT. This site not only provides security information, but also tools and scripts for exploiting vulnerabilities.
- SecurityFocus[6]
  - Valuable web page for general security notices. This page will also have specific methods for exploiting equipment such as Cisco routers.

After searching these web pages a notable vulnerability was found. This vulnerability was found at SecurityFocus, which lead me to a better description of the vulnerability at the following URL.

http://www.aerasec.de/security/advisories/txt/checkpoint-fw1-ng-fp3-syslog-crash.txt[5]

The vulnerabilities that where reported by this web page are as follows:

- ” Successful DoS from remote against syslog daemon of Check Point FW-1 NG before NG FP3 HF2, perhaps remote root exploit possible.”[5]

- ” Log flodding from remote against the logging mechanism by using the syslog daemon of Check Point FW-1 4.1”[5]

- “Syslog message containing escape sequences directed to syslog daemon of Check Point FW-1 up and including NG FP3 HF2 remain unfiltered and cause strange output behavior if the log is viewed on console.”[5]

This web page was also helpful enough to describe what the syslog packet must look like to exploit the vulnerability. This first syslog is a valid message to show an example of what the syslog daemon would expect

[evilhost]# echo "<189>19: 00:01:04: Test" | nc -u xxx.xxx.xxx.xxx 514[5]

- Where xxx.xxx.xxx.xxx is the valid ip address of the firewall.

This malicious syslog message with random escape sequences, as shown below, should cause the syslog daemon to crash. The syslog daemon cannot be restarted until the service is restarted.

[evilhost]# echo -e "<189>19: 00:01:04:
test\a\033[2J\033[2;5m\033[1;31mHACKER~
ATTACK\033[2; 25m\033[22;30m\033[3q" | nc -u firewall 514[5]

The results of such an attack are not completely documented. This type of attack can cause “strange output behavior” of the syslog daemon. A few most likely

events will happen. First, the syslog daemon crashes which causes the firewall to block all traffic. This is the standard Denial of Service reaction. Another, less likely, but more problematic, reaction is the ability of the attacker to execute malicious code or gain root access. This possibility arises because the syslog daemon runs at the root level. Thus, if a script could be created to exploit this vulnerability and execute code in the payload of the syslog message root level access could be given to the attacker. This is the worst-case scenario, which has yet to be publicly confirmed.

If you are running a Check Point firewall with the syslog daemon enabled there is hope. This vulnerability report also specifies means to mitigate the potential security flaws. The first notable workaround was to filter log output using "tr" like. An example rule is as follows.

> [firewall]# fw log -tfnl | tr '\000-\011\013-\037\200-\377' '*'
> (all chars with ASCII codes from decimal 0-31 and 128-255 except 10 for LF are replaced by an asterisk '*')[5]

The second workaround is to update this syslog daemon, once Check Point creates it. This patch will hopefully create a dynamic rule to filter this type of syslog data out.

4.3 An Attack Plan to Compromise an Internal System

The following attack would target workstations within the corporate LAN. This workstation would then become the slave for future attacks against the internal servers of GIAC Enterprises. This vulnerability assumes GIAC employees use Microsoft Internet Explorer as their default web browser.

4.3.1 IE Vulnerability Exploit

Wolfgang's GIAC Enterprises corporate LAN will most likely have Windows base workstations with Internet Explorer as the favorite web browser. It is the commonality of the corporate LAN that feeds this sections exploit. In the past several months SecurityFocus.com has posted several vulnerabilities in Microsoft's Internet Explorer web browser. Some of these vulnerabilities are so critical that there is a possibility of the execution of malicious code. The exploit I will be using is published at the following URL:

> http://www.securityfocus.com/bid/8565/info/[3]

SecurityFocus.com's explanation of the vulnerability stated that IE "does not properly handle object types, when rendering XML based web sites." The successful exploitation of this vulnerability would allow the attacker to install and executed malicious objects on the victim's machines. SecurityFocus.com also provided the following example code for the exploit:

```
<span datasrc="#oExec" datafld="exploit"
dataformatas="html"></span>
```

```
<xml id="oExec">
<security>
<exploit>
<![CDATA[
<object id="oFile" data="badnews.php"></object>
]]>
</exploit>
</security>
</xml>
```
[3]

The only contingency of this vulnerability is that the victim must visit the web page containing the malicious embedded object. The effectiveness of this exploit stems from the lack of user awareness. Because the malicious code is executing as part of the web page the user is not prompted with a warning about the object's install and execution. The process, start to finish, will happen in the background of the web page.

The malicious code executed by this vulnerability could range depending on the intent of the attacker. Personally, I would leave an agent behind that would embed itself into the machine at the users current permission level. This agent could then contact the host machine, on the outside of the network, to receive further instructions. This type of agent would most likely go undetected and the number of future exploits is only limited by the host's orders. I believe this type of attack would work extremely well with Wolfgang's architecture due to the placement of his server farm. He placed the company's internal servers on the same network as the employee workstations with no separating firewall to create a defense-in-depth solution.

Lastly, I would have to entice one, or many, of the internal employees to visit my hostile web page. This would be done through several steps. First, I would acquire as many email addresses of internal employees as possible. GIAC is a customer-based organization grounded on pleasing the customer, thus social engineering should provide the desired results. I would call GIAC and pose as a troubled customer requesting an email address of a customer service representative. I would then send an email to this person with a hyperlink to my web page. The email might also include some enticing text to lure the employee to the link.

4.4 Distributed Denial of Service Attack (DDoS)

This attack will require the use of slave machines. The general idea behind the DDoS is to create a means of rooting several UNIX bases boxes throughout the Internet. Once these boxes have been rooted you can install a script to attack specific IP address. This means that all of the slave machines will direct their fire onto one target machine.

The requirements of the attack specify that 50 cable/DSL machines must be used as slave machines for this attack. Thus, the first step is to root these 50 machines. This isn't that difficult when considering the typical cable/DSL user. These types of broadband connections have become popular for two reasons, fast speeds and constant connections. These two characteristics also make cable/DSL perfect connections for DDoS attacks. Most of the machines connected to a home cable/DSL connection do not have a firewall and many have no security at all. Lack of security combine with the fast connection will make these boxes ideal slave machines for a brute force DDoS attack. To find these machines I will determine what IP address ranges ISPs such as Comcast, Verizon, SBC Yahoo, etc use for their broadband customers. Then, scans of these IP blocks will be done to determine which machines are vulnerable. During this scan the attacking machine will compile a list of vulnerable machine founds. Finally, a script running the exploit for the vulnerability will run the attack against all predetermine machines. This root kit will then trigger another script, which will install the DDoS Master/Daemon in the background of the exploited machine.

The tool used to facilitate the DDoS is called "Trinoo" and can be found at the following web page:

http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt[2]

This script uses a standard hierarchal approach to over welling its victim. First, an attacker creates master machines. These machines control the daemons, the machines that actually carry out the attack. Finally, the attack ends with all the traffic generate by the daemons focused at the victim. This focus of traffic will overwhelm the bandwidth of the victim, thus causing a denial of service for all legitimate traffic.

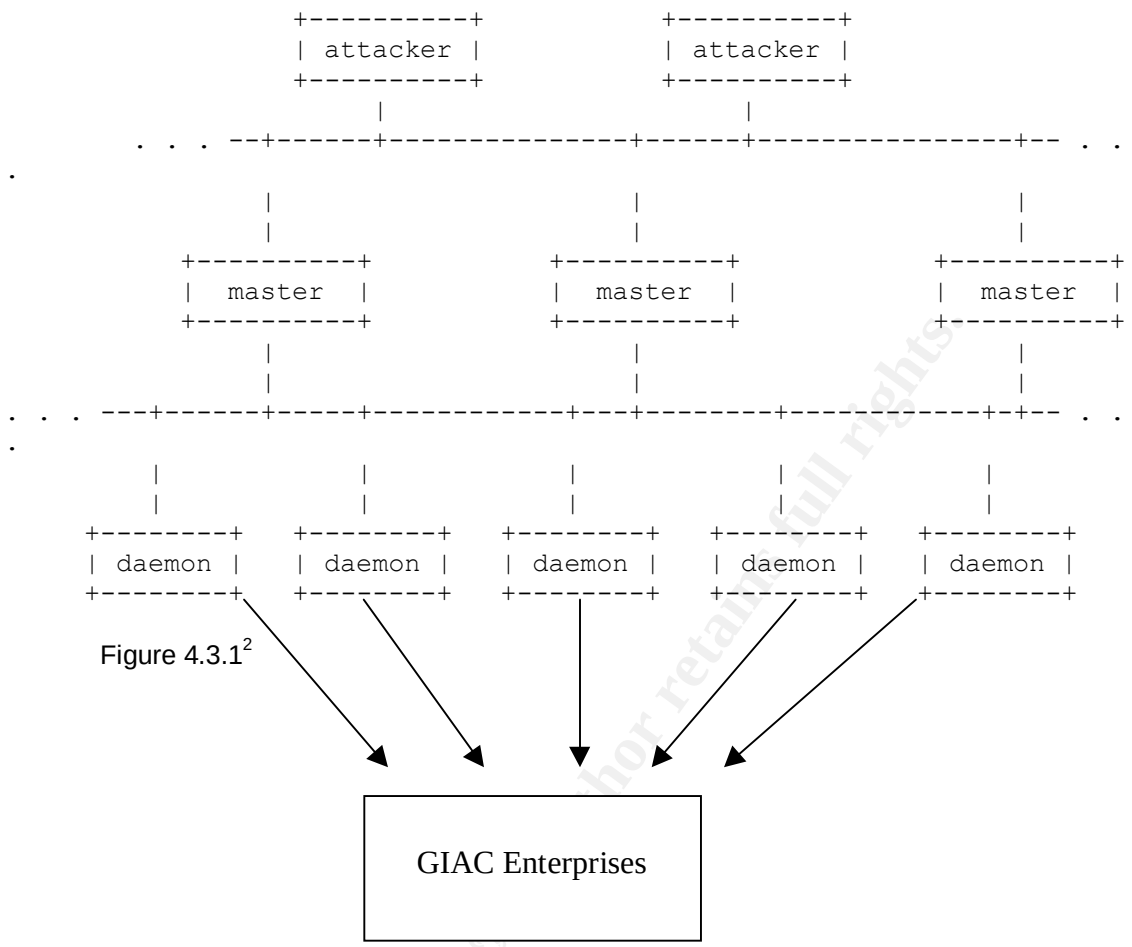


Figure 4.3.1[2]

With this tool the attacker will control one or more master agents, which in turn control several daemon agents each. With this approach the attacker is harder to identify since no traffic is directly coming from the attacker's machine. To further disguise the attacker all packets are sent with a spoofed IP address. This attack utilizes a UDP flood. Basically, the master will communicate to the daemon via UDP on high number ports. Then the daemons, once commanded, will flood the victims using UDP on port 4. [2]

References

1. www.arin.net
2. David Dittrich. "The DoS Project's "trinoo" distributed denial of service attack tool." http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt. (20 November 2003).
3. Micorsoft. "Microsoft Internet Explorer XML Page Object Type Validation Vulnerability." **http://www.securityfocus.com/bid/8565/info/.** (15 October 2003).
4. CyberGuard Corporation. Defend Your Domain Vol 1&2. U.S.A: Feb. 2002
5. "2003 AERAsec Network Services and Security GmbH (2003)." http://www.aerasec.de/security/advisories/txt/checkpoint-fw1-ng-fp3-syslog-crash.txt. (10 October 2003)
6. http://www.securityfocus.com/ (10 October 2003)
7. http://packetstormsecurity.nl/ (10 October 2003)
8. http://www.cert.org/ (10 October 2003)
9. http://www.ethereal.com/ (10 October 2003)
10. http://www.insecure.org/nmap/ (10 October 2003)
11. National Security Agency. "Cisco Router Guide (September 27, 2002)." http://www.nsa.gov/snac/cisco/index.html. (3 September, 2003)
12. National Security Agency. "Windows 2000 Guide." http://www.nsa.gov/snac/win2k/index.html. (10 September, 2003)
13. http://www.kiwisyslog.com/. (15 October 2003)
14. Verisign. "Payment Services: Payflow Pro." http://www.verisign.com/products/site/cs/index.html. (4 August, 2003)
15. B. Moskowitz, Y. Rekhter. "RFC 1918 – Address Alocation for Private Internets (February 1996)." http://www.faqs.org/rfcs/rfc1918.html. (4 August, 2003)

Appendix B: TestServer.java

```
import java.io.*;
import java.util.*;
import java.net.*;

public class TestServer {

	private int listenPort;
	private ServerSocket servSock;
	private DataInputStream in;
	private Socket inSock;
	private int ACCEPT_TIMEOUT =250;  //milliseconds

	public TestServer(int inListenPort){
		listenPort = inListenPort;
		initListenServer();
		listen();
	}

	private void initListenServer() {
		boolean successful = false;
		try {servSock.close();} catch (Exception
closeError) {}
		while (!successful){
			try{
				servSock = new
ServerSocket(listenPort);

	servSock.setSoTimeout(ACCEPT_TIMEOUT);
				System.out.println(new Date() + ":
Test Server listening on port " + listenPort);
				successful = true;
			}catch (BindException serverError){
				System.out.println("\n\n*** Error:
Port already in use ***\n");
				System.exit(1);
			}catch (Exception serveError){
				System.out.println(new Date() + ":
" + serveError.getMessage());
				try{
					Thread.sleep(1000);
```

```
                        }catch (Exception sleepError){}
                        successful = false;
                  }//CATCH
            }//WHILE LOOP
      }//PRIVATE VOID INITLISTENSERVER

      private void listen (){
            InetAddress ia;
            while (true) {
                  try {
                        inSock = servSock.accept();
                        inSock.setSoTimeout(50); //half a
second//
                        ia = inSock.getInetAddress();
//LEFT OFF HERE...//
                        System.out.print(new Date() + ":
Incoming connection: " + ia.getHostName());

      System.out.print("["+ia.getHostAddress() + "], port "
+ inSock.getPort());
                        System.out.println(", localport "
+ inSock.getLocalPort());
                        in = new
DataInputStream(inSock.getInputStream());
                        System.out.println("<START of
transmission>");
                        record();
                  }catch (InterruptedIOException iioe) {}
//times out//
                   catch (EOFException eofe){
                        closeConnection();
                        System.out.println("\n<END of
transmission>\n");
                  }
                  catch (Exception otherException) {
                        closeConnection();
                        System.out.println("\n<END of
transmission>");
                        System.out.println("\n"+new Date()
+ ": Encountered a "+otherException+", Ending
Transmission\n");
                  }//catch
            }//while
      }//private void listen

      private void closeConnection (){
            try {
```

```
                in.close();
            }catch (Exception closeError){}
            try {
                inSock.close();
            }catch (Exception closeError){}
        }//closeConnection

        private void record () throws Exception {
            while (true){
                try {

        System.out.print((char)in.readByte());
                }catch (InterruptedIOException iioe){}
            }//while
        }//private void record

        private static void warningMessage() {
            System.out.println("\n\nSYNTAX: java TestServer
<listenport>\n");
        }//private void warningMessage

        public static void main (String args[]){
            try {new TestServer(Integer.parseInt(args[0]));
            }catch (Exception argError){
                TestServer.warningMessage();
                return;
            }//catch
        }//main
}//TestServer
```