Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.7

Kent Stout
September 16, 2002

Table of Contents

1. Assignment 1 – Security Architecture 4
   1.1 Background 4
   1.2 Business Relationships and Requirements 4
   1.3 The Network 7
      1.3.1 External Network 9
      1.3.2 Customer Service Network 9
      1.3.3 Partners/Suppliers Network 10
      1.3.4 Internal Network 10
2. Assignment 2 – Security Policy and Tutorial 12
   2.1 Border Router 12
      2.1.1 General Configuration 12
      2.1.2 Access Control Lists (ACLs) 14
   2.2 Firewall Policy 16
   2.3 VPN policy and tutorial 21
      2.3.1 VPN description and rule set 21
      2.3.2 VPN Tutorial 24
3. Assignment 3 – Verify the Firewall Policy 30
   3.1 Plan the audit 30
   3.2 Audit Results and Analysis 34
   3.3 Audit Summary 38
4. Assignment 4 – Design Under Fire 39
   4.1 Attack Against the Firewall 41
   4.2 Denial of Service (DoS) Attack 42
   4.3 Attack Against an Internal System 43
5. Resources 45
6. Appendix A – Certificate Generation Script 47

Abstract

This paper describes the Security Architecture and Firewall Policy for an imaginary company named GIAC Enterprises that deals in the sale of fortune cookie sayings. The Firewall Policy of GIAC Enterprises is also audited and analyzed within this paper. Finally, three attacks on previous GCFW practical assignment are proposed and discussed.

1. Assignment 1 – Security Architecture

1.1 Background

GIAC Enterprises is an internet-based company which deals in the online sale of fortune cookie sayings. GIAC is located in the US, but its supplying entities and customer base are worldwide. Since the company's inception, GIAC has dealt exclusively in an English-based market. In the interest of expanding business, GIAC has recently formed a partnership with China Fortunes Enterprises(CFE). The agreement states that CFE will supply translations for GIAC's various fortunes in return for a share of the profit in the sell of these translated fortunes.

GIAC itself is a small company with approximately fifty employees, but has sustained relatively high profits despite the collapse of many internet-based companies. Keeping the workforce small has allowed them to invest a substantial amount of money into the equipment that makes up their physical network. This has paid dividends in the areas of scalability and performance.

1.2 Business Relationships and Requirements

The next few sections describe the requirements needed for GIAC to operate properly. This includes defining the relationships between GIAC and the entities with which it interacts.

Customers

Customers gain access to GIAC and its fortunes through the web server located in the customer service network. This web server provides Internet customers with company information, purchasing instructions, contact information, and it handles all purchase transactions. Customers can browse the GIAC home page via HTTP, but all transactions are handled via HTTPS. Access to the web server is handled by the firewall's HTTP proxy, which prevents operations such as PUT, DELETE, and POST. Only GIAC's internal employees on site are able to perform these actions. Before any transactions are made, a customer is required to create a personal account on the web server, which then gets stored in the directory server located on the same machine. Once an account has been created, the customer can then log in via HTTPS. All subsequent browsing and transactions are done via HTTPS until the customer logs out. Once logged in, the customer can browse through GIAC's fortune sayings and make purchases via credit card. The customer can also change personal account information and passwords. Customers are never in direct contact with the company's internal fortunes database. All requests made by the customer are relayed by the web server via the SQL*Net proxy on the firewall to the internal database. The web server is only allowed to make read-only requests to the internal database. The list below describe the steps a customer would take for a first time transaction:

1) Customer accesses the web server via HTTP
2) Customer creates an account on web server
3) Customer logs in via HTTPS
4) Customer browses through fortune sayings and selects a package for purchase
5) Customer enters credit card information
6) Once the credit card has been validated, the customer is free to download the purchased fortunes
7) Customer logs out

Customers are also allowed to email GIAC with any questions, comments, or complaints. Links to these email addresses can be found on the company web site.

Suppliers

Suppliers provide GIAC with many of their fortune cookie sayings and are located around the world. They are paid per transaction. There is a special account on the web server that allows them to perform the following actions:

- Update their company information
- View official contract agreements with GIAC
- Track payments for services provided
- View previously supplied fortunes
- Email GIAC employees

Suppliers do not use the web server for uploading new fortunes. This would be considered very insecure in that the confidentiality of the provided data would be very difficult to ensure given that the web server is located in the only publicly accessible area of GIAC's overall network. For this purpose, GIAC has created a partners/suppliers network, which is only accessible using Cyberguard's VPN technology. All suppliers are required to have and employ Cyberguard VPN client software in order to upload fortunes. Once a host-to-gateway VPN connection has been established suppliers can upload fortunes to the database located in the partners/suppliers network via FTP. In order to establish the VPN connection, suppliers must first authenticate at the firewall's external interface using Cyberguard's Passport One (https/3443) mechanism. Currently this only requires a supplier username and strong password (which is changed monthly by one of GIAC's firewall administrators), but thought has been given to requiring the use of SecureNet Keys for authentication with Passport One since this method is already in place for remote employees. The drawback to this approach is requiring each and every supplier to possess a SecureNet Key. This added hassle could cause GIAC to lose some of its suppliers. Passport One allows different sets of filtering rules to be associated with the various user profiles enabled on the firewall, while simultaneously supporting the VPN connection. Once they have logged in and their Passport One session is

running, the VPN client software must then be activated on their workstation to establish a VPN connection. Suppliers must then authenticate to the FTP server running on the database machine. The low trust level given to suppliers dictates that defense in depth should be practiced. Through the VPN tunnel, suppliers can now upload fortunes to the database server via the firewall's FTP proxy. The supplier profile on the firewall grants suppliers the ability to perform only certain FTP operations through the FTP proxy. Suppliers are not permitted to delete, overwrite, rename, or retrieve any of the files already located on the database server. They are allowed to upload files and create new directories on the database server only. These same restrictions are reinforced by the database itself. The exact rules associated with the supplier profile are given later in the VPN security policy section.

Partners

GIAC has recently partnered with China Fortunes Enterprises (CFE) in an effort to expand into foreign language markets. Their contractual agreement states that CFE will provide translations for GIAC's fortunes in return for a share of the profit resulting from the sale of these translated fortunes. CFE partners are much more trusted than both the suppliers and customers. Even so, they are only given access to the database server in the partners/suppliers network. This access is only permitted through a gateway-to-gateway VPN connection established between CFE's firewall and GIAC's firewall. This database contains only a subset of the fortunes located on the internal database at any given time. The subset is updated periodically to meet working demands. This database is running Oracle iFS (Internet File Server), which supports many standard Internet protocols. The only ones that are permitted by the database are FTP, HTTP, and SMTP. Partners are forced to have user accounts on the database, which restrict the extent to which they can use these protocols, but sufficient access privileges are granted so that work is not inhibited. They are able to download and upload fortunes and translations.

GIAC Internal Employees

GIAC's internal employees that are on site are permitted to browse the Internet via HTTP and HTTPS through the given firewall proxies. They are also allowed to FTP through the firewall using the application proxy. Employees are also able to send and receive email through the internal mail server, which in turn forwards mail to and receives mail from the external mail server. This is done to limit the number of connections originating from the internal network to the Internet. Both mail servers have antiviral software running on them. As stated above, internal employees have access to the machines in the customer service network in order to perform maintenance when needed. The internal database, which houses GIAC's fortunes, is also running Oracle iFS. Each employee has a user account on this database, which restricts access abilities. Employees are able to communicate with the database using only the HTTP and FTP protocols. CFE

has established a gateway-to-gateway VPN connection that allows GIAC's internal employees to work on an assigned part of CFE's private network. Internal employees are not given access to the database in the partners/suppliers network except on request (for maintenance) because it is not needed. Every night between 1:00am and 2:00am, the partners/suppliers database replicates to the internal database using the firewall's SQL*Net proxy. Thus, all information needed by employees can be found on the internal database.

Mobile Sales Force and Teleworkers

All remote work performed by employees is done over a VPN connection. This requires that all remote employees have Cyberguard VPN client software installed on their laptops. Remote employees authenticate to the firewall using the Passport One (https/3443) mechanism as described above. Employees are required to use a SecureNet Key to authenticate through Passport One. Once they have a Passport One session established and running, they must activate the VPN Client Software in order to secure a connection. After the VPN connection has been established, employees are allowed to connect to the Telnet Server located in the internal network via the generic Port Guard proxy offered by Cyberguard. Once they have logged into the Telnet Server through their user account, they can enjoy most of the same privileges that an internal user on site has.

1.3 The Network

GIAC's network is shown below in Figure 1. As you can see there are three internal networks:

- Customer Service Network
- Partners/Suppliers Network
- Internal Network

There is only one external network. The firewall dynamically NATs all internal IP addresses, except for the syslog server, to c.c.c.2. The syslog server statically NATs to c.c.c.3 in order to allow the border router to pass syslog messages through the firewall. All machines are running Solaris 8 (02/02) with the recommended patches applied from http://sunsolve.sun.com/, and all servers, excluding the two databases, are Sun Fire V120 Servers. All machines are running Command Antivirus for Solaris for protection against viruses and other types of malware. Signature files are updated immediately upon availability. All machines syslog all log messages to the central syslog server on the internal network. Below is a further description of each machine in GIAC's network.

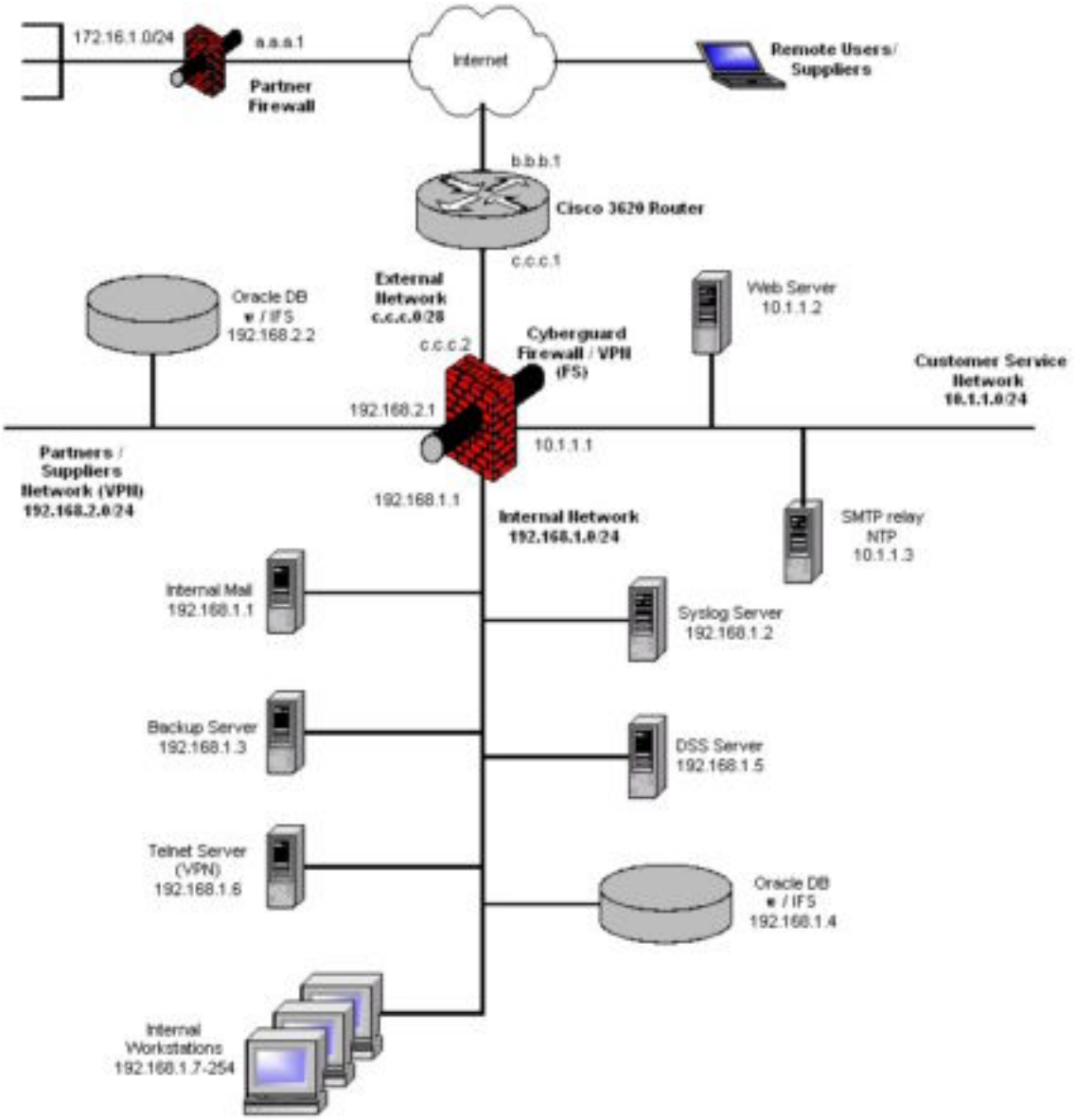


Figure 1.
GIAC's Network

1.3.1 External Network

- **Border Router**

The border router is a Cisco 3620 running IOS release 12.2. This is a mid-range router that offers sufficient bandwidth and is relatively inexpensive. Cisco offers excellent support documentation for all of its products[10]. The border router syslogs all of its log messages using udp/514 to c.c.c.3, which statically NATs to the syslog server on the internal network.

- **Cyberguard Firewall High Availability (HA) Cluster**

As with any Internet-based company, GIAC cannot afford downtime. It was decided that the expense and risk of downtime far outweighed that of purchasing a second firewall to ensure high availability. Both firewalls are Cyberguard FS models running release 5.0 for Unixware PSU 2. The Cyberguard FS model is a proxy-based firewall appliance that offers integrated VPN technology, built-in split DNS capability, and built-in high availability software. It boasts 200Mbps performance with up to 550 thousand simultaneous connections[11]. Each appliance has six 10/100 Ethernet ports. Cyberguard has achieved a Common Criteria Evaluation Assurance Level 4 (EAL4) certification as defined by the Common Criteria for Information Technology Security Evaluation (CCITSE), which is a set of evaluation criteria agreed to by the National Security Agency(NSA)/National Institute of Standards and Technologies(NIST) and similar entities around the world[12]. Cyberguard FS provides application proxies (or smartproxies as labeled by Cyberguard) for several common protocols including: HTTP, FTP, SMTP, SSL, and SQL.

GAIC is employing the split DNS capabilities of the Cyberguard firewall as well as the integrated VPN technology. No zone transfers are allowed to either of the DNS servers running on the firewall. In addition to the five smartproxies listed above, GIAC is also utilizing a generic (Port Guard) proxy for remote employees, which are allowed to telnet into the internal network over a VPN connection.

1.3.2 Customer Service Network

This is the only network that is publicly accessible.

- **Web Server**

The web server is running Apache 2.0.40, and has been configured to return bogus replies to any version queries or OS fingerprinting attempts. This machine has been hardened by YASSP[4] (Yet Another Solaris Security Package) to allow only the specific services needed by the web server to function properly. YASSP is a free hardening tool (actually a tarball of various packages) that can be

downloaded at http://www.yassp.org/. The web server is also running OpenLDAP 2.0.25, in order to store and authenticate usernames and passwords. Apache has been configured to use auth_ldap 1.6.0 in order authenticate users with OpenLDAP.

- **SMTP relay (External Mail) and NTP Server**

This machine serves as both a mail relay and the NTP server for the GIAC network. This machine has also been hardened by YASSP to allow only the necessary services to run. This machine is running sendmail 8.12.6 and XNTPD version 4.1.1a. All mail from the Internet is received by this server, scanned for viruses, and then forwarded to the internal mail server. It also receives all mail from the internal mail server, which it then forwards to the Internet. The NTP server running on this machine is allowed to query three public NTP servers once a day from 1:00am to 2:00am in order to synchronize its time. In turn, all other machines in GIAC's network query this server in order to synchronize their times.

1.3.3 Partners/Suppliers Network

This network is only accessible via a VPN connection.

- **Oracle Database Server**

GIAC administration decided that it was too risky to allow non-GIAC persons to have access to the internal network. This prompted GIAC to provide a separate network for cooperative development. The only machine currently on the network is a Sun Fire 280R Server, which hosts an Oracle9i Database. Oracle Internet File Server (iFS), which comes bundled with the Oracle Database, is also running on this machine. Oracle iFS supports several access protocols, but only HTTP, FTP, and SMTP are activated. Both suppliers and partners access this machine to provide GIAC with vital products. Suppliers are only allowed to FTP fortunes to the database through the firewall's FTP smartproxy via a host-to-gateway VPN connection. Partners, which are much more trusted, are allowed to take advantage of all three protocols mentioned above to retrieve fortunes and provide translations. They access the machine via a gateway-to-gateway VPN connection. At any given time, only a subset of GIAC's fortunes reside on this database. In case of compromise, only a portion of the fortunes would be vulnerable. This machine replicates to the internal database nightly (1:00am-2:00am) through the firewall's SQL*Net smartproxy.

1.3.4 Internal Network

- **Internal Mail Server**

This server is also running sendmail 8.12.6. Internal employees are only allowed to connect to this server for mail services. This server is not allowed to make any connections to the Internet. It sends all outgoing mail to the external mail server where it is then relayed to the Internet, and it receives all incoming mail from the external mail server also. To support defense in depth, the internal mail server also scans all outgoing and incoming mail for viruses and other malware.

- **Internal Syslog Server**

This is the central log server for GIAC's network. All machines including the firewall and border router forward log messages using udp/514 to the log server. This server requires maximum security because it contains the history of all actions that take place on GIAC's network. To ensure security, this box has also been hardened using YASSP such that the only listening service still running on the machine is syslogd. The only other service it is allowed to perform is a query to the NTP server in the customer service network in order to synchronize its time. A custom set of perl scripts, which run as daemons, have been written to parse incoming log messages in order to aid administrators in reviewing logs.

- **Backup Server**

This server holds snapshots of the internal database for emergency recovery. It also stores the configurations for each of the internal servers as well as the servers in the customer service network. No communication is allowed with this server except for the periodic backups of the internal database, and any configuration changes to the other servers. It is also allowed to query the NTP server in the customer service network for time synchronization. Only administrators are allowed to login into this machine.

- **Defender Security Server (DSS)**

This server provides two-factor authentication for remote employees trying to connect using the Passport One mechanism on the Cyberguard firewall. Remote employees must have a SecureNet Key, which is a small challenge-and-response token card that provides one-time passwords. Once authenticated by this server, the firewall establishes a Passport One session. Remote employees can then activate their VPN client software to establish a host-to-gateway VPN connection with the firewall.

- **Telnet Server**

Rather than give remote employees unrestricted access to all internal machines, it was decided that a single point of access would be a better solution. This makes security monitoring and permission restrictions much easier to maintain for GIAC's administrators. Given that this is the only way to externally access GIAC's internal network, its security is of paramount importance. That is why this

server is only accessible through a VPN connection. Once a host-to-gateway VPN connection has been established for a remote employee, they are allowed to telnet through the VPN tunnel to this server via the generic Port Guard smartproxy on the firewall. After logging in to the telnet server, employees can access their personal workstations, check internal email, and perform general tasks.

- **Internal Database Server**

This is a Sun Fire V480 Server hosting an Oracle9i Database, which is also running Oracle iFS. This is the main database, which holds all of GIAC's fortunes. Each internal employee has a personal account on this server. Strong passwords are enforced and changed monthly. Employees are only allowed to work in a designated development area of the database. Fortunes are thoroughly reviewed before being put in the production area of the database, which is the area that is queried by the customer web server. Requests from the web server are read only. The only two protocols activated for employees to work in the development area by the iFS software are HTTP and FTP. This server periodically pushes a subset of its fortunes to the database server located on the partners/suppliers network, and it also allows backup snapshots to be sent to the backup server.

2. Assignment 2 – Security Policy and Tutorial

2.1 Border Router

The border router is GIAC's first line of defense. It has been decided that the most efficient way to utilize the combined processing power and filtering capabilities of the border router and firewall is to assign the router to be a static packet filterer and allow the firewall to perform stateful filtering. GIAC configured the border router using the NSA Router Security Configuration Guide[8]. A brief description is given for each of the following configuration commands. For a complete description refer to the NSA guides listed in the resources section at the end of this document.

2.1.1 General Configuration

Disable all servers that are not needed on the router such as echo, discard, chargen, bootp, finger, http, snmp, etc.

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

All services that are not needed on the router are explicitly shut down including Cisco Discovery Protocol(CDP), remote configuration, source routing, and classless routing.

```
no cdp run
no service config
no ip source-route
no ip classless
```

These commands are applied to all interfaces of the router in the configure interface mode in order to disable directed broadcasts (can be used for DOS attack), proxy ARP, and NTP.

```
no ip directed-broadcast
no ip proxy-arp
ntp disable
```

The following commands are also applied to each interface on the router in order to prevent IP unreachables, redirects, and mask replies from being sent. These ICMP messages can aid attackers in mapping a network.

```
no ip unreachable
no ip redirect
no ip mask-reply
```

The following commands are executed in the configure line mode in order to secure the console and virtual terminal lines and disable the auxiliary line because it is not being used.

```
line con 0
exec-timeout 5 0
login
transport input telnet

line vty 0 4
exec-timeout 5 0
transport input telnet

line aux 0
no exec
exec-timeout 0 10
transport input none
```

The enable secret password has been set, as well as the passwords for both the console and virtual terminal lines. The router has been enabled to use basic encryption (MD5 hash) to protect all passwords.

```
service password-encryption

enable secret <strong password>
```

```
line con 0
password <strong password>

line vty 0 4
password <strong password>
```

The router has been enabled to send logs to the central log server on the internal network using syslog. Messages are sent from the internal interface of the router using the local7 facility.

```
logging on
no logging console
logging c.c.c.3
logging facility local7
logging source-interface eth 0/1
```

2.1.2 Access Control Lists (ACLs)

GIAC's router employs the use of extended ACLs as opposed to standard ACLs because they offer a greater variety of filtering options. Standard ACLs filter by examining the source IP address of a packet only. In addition to examining the source IP address, extended ACLs can also examine the destination IP address, source and destination ports, protocol, and ICMP message types. Standard ACLs are numbered from 1-99, while extended ALCs are numbered from 100-199.

There are two ACLs employed on the router. The first is applied to inbound traffic on the external interface of the router, and the second is applied to inbound traffic on the internal interface of the router. This method was chosen, rather than filtering outbound traffic on either interface, in an effort to optimize CPU and memory usage on the router itself. This prevents any packets destined for denial from passing through the router.

- **External Interface ACL**

The following command creates a new access-list if it doesn't already exist, or clears any previous information that was contained in it.

```
no access-list 101
```

The following commands actually construct the ACL. Lines beginning with a "!" are comments. The "log" keyword at the end of each line instructs the router to generate a log message when that rule is matched.

```
! Block all packets with internal addresses as source ip
access-list 101 deny ip c.c.c.0 0.0.0.15 any log

! Block all loopback and reserved addresses
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

! Block multicast and broadcast
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log

! Block ICMP redirects even though we have disabled them
access-list 101 deny icmp any any redirect log

! Block Land attacks
access-list 101 deny ip host b.b.b.1 host b.b.b.1 log

! Block incoming syslog traffic
access-list 101 deny udp any any eq syslog log

! Block incoming snmp traffic
access-list 101 deny udp any any eq 161 log
access-list 101 deny udp any any eq 162 log
access-list 101 deny tcp any any eq 161 log
access-list 101 deny tcp any any eq 162 log

! Block TFTP traffic
access-list 101 deny udp any any eq 69 log

! Permit only traffic destined for firewall's external interface
access-list 101 permit ip any host c.c.c.2

! Deny everything else
access-list 101 deny ip any any log
```

This access-list is applied to inbound traffic on the external interface of the router executing the following command in the interface configuration mode.

```
ip access-group 101 in
```

- **Internal Interface ACL**

This access-list is much simpler. The ACL denies several types of ICMP traffic that could be used to map GIAC's network, and provides egress filtering to ensure that no spoofed addresses are allowed to originate from within GIAC's network.

```
no access-list 102

! Block network revealing ICMP traffic
access-list 102 deny icmp any any host-unreachable
access-list 102 deny icmp any any echo-reply
access-list 102 deny icmp any any time exceeded

! Permit traffic coming from external interface of the firewall only
access-list 102 permit ip host c.c.c.2 any
```

```
! Deny everything else
access-list 102 deny ip any any
```

By executing the following command in the interface configuration mode, the access-list above is applied to inbound traffic on the internal interface of the router.

```
ip access-group 102 in
```

After saving the current configuration, the router needs to be rebooted to work properly.

2.2 Firewall Policy

As stated earlier, GIAC is using a pair of Cyberguard FS model firewalls to provide high availability for GIAC's overall network. The high availability cluster is an active/standby pair that is governed by built-in software. The software ensures that all policies and configuration files are replicated from the active node to the standby node. The firewall policy described in this section is resident on both firewalls. GIAC designed their firewall policy with a "deny all" mentality. Administration was adamant in allowing only those services vital to the operation of the company to traverse the firewall. The active firewall protects three private networks:

- Customer Service Network
- Partners/Suppliers Network
- Internal Network

Below is a table for each private network summarizing the access requirements enforced by the firewall. Redundant connections amongst the three private networks will not be repeated in every table.

Customer Service Network

Service/Protocol	Source	Destination	Description
http/tcp 80	Internet	Web Server 10.1.1.2	Allow customer access to the web server
https/tcp 443	Internet	Web Server 101.1.2	Allow customer SSL encrypted access
smtp/tcp 25	Internet	External Mail Server 10.1.1.3	Allow incoming email for employees
http/tcp 80	Internal Network	Web Server 10.1.1.2	Allow employee access to the web server
https/tcp 443	Internal Network	Web Server 10.1.1.2	Allow employee SSL encrypted access

smtp/tcp 25	Internal Mail Server 192.168.1.1	External Mail Server 10.1.1.3	Allow internal mail server to retrieve/send internal employee email
ntp/udp 123	NTP Server 10.1.1.3	Public NTP Servers ntppub.tamu.edu ntp.cox.smu.edu ntp.fnbhs.com	Allow GIAC's NTP server to query public time servers
ntp/udp 123	Internal Network Partner/Suppliers Network	NTP Server 10.1.1.3	Allow all internal machines to query the NTP server
syslog/udp 514	Customer Service Network	Syslog Server 192.168.1.2	Allow all machines in customer service network to send syslog messages
sqlnet/tcp 1521	Web Server 10.1.1.2	Internal Database 192.168.1.4	Allow web server to query database for fortunes

Partners/Suppliers Network (Non VPN)

Service/Protocol	Source	Destination	Description
sqlnet/tcp 1521	Partners/Suppliers(PS) Database 192.168.2.2	Internal Database 192.168.1.4	Allow PS database to replicate to internal database
sqlnet/tcp 1521	Internal Database 192.168.1.4	Partners/Suppliers(PS) Database 192.168.2.2	Allow internal database to push subset of fortunes to PS database
syslog/udp 514	Partners/Suppliers(PS) Database 192.168.2.2	Syslog Server 192.168.1.2	Allow PS database to send syslog messages to syslog server

Internal Network (Non VPN)

Service/Protocol	Source	Destination	Description
http/tcp 80	Internal Network	Internet	Allow internal employees to browse the internet
https/tcp 443	Internal Network	Internet	Allow internal employees to browse the internet via SSL
ftp/tcp 21	Internal Network	Internet	Allow internal employees to ftp to the Internet

Firewall Rule Set

The following is the actively relevant excerpt from the actual rule configuration file (netguard.conf) taken from the **/etc/security/firewall/ng_inet** directory on the firewall appliance. The application proxies provided by the firewall add another layer of security, but they can consume large amounts of memory and CPU, which can lead to serious drops in performance. This is why the application proxies are only used in crucial situations such as the traversal of a packet over the external interface of the firewall or packets directed at critical machines on GIAC's network. Cyberguard offers a defense against TCP SYN flood attacks, which allows the firewall administrator to set the period of time that the firewall waits for the return ACK from the client initiating the TPC three-way handshake. This defense is enabled with a 10 second wait period for every TCP port listening on the external interface of the firewall. It is denoted in the rules below with the TCPSYNFLD keyword. The ENABLE_REPLY keyword allows the firewall to keep state for the UDP protocol such that UDP replies will be permitted if requested. Rules with time constraints are denoted with the "tbr:<day>:<time window>" string.

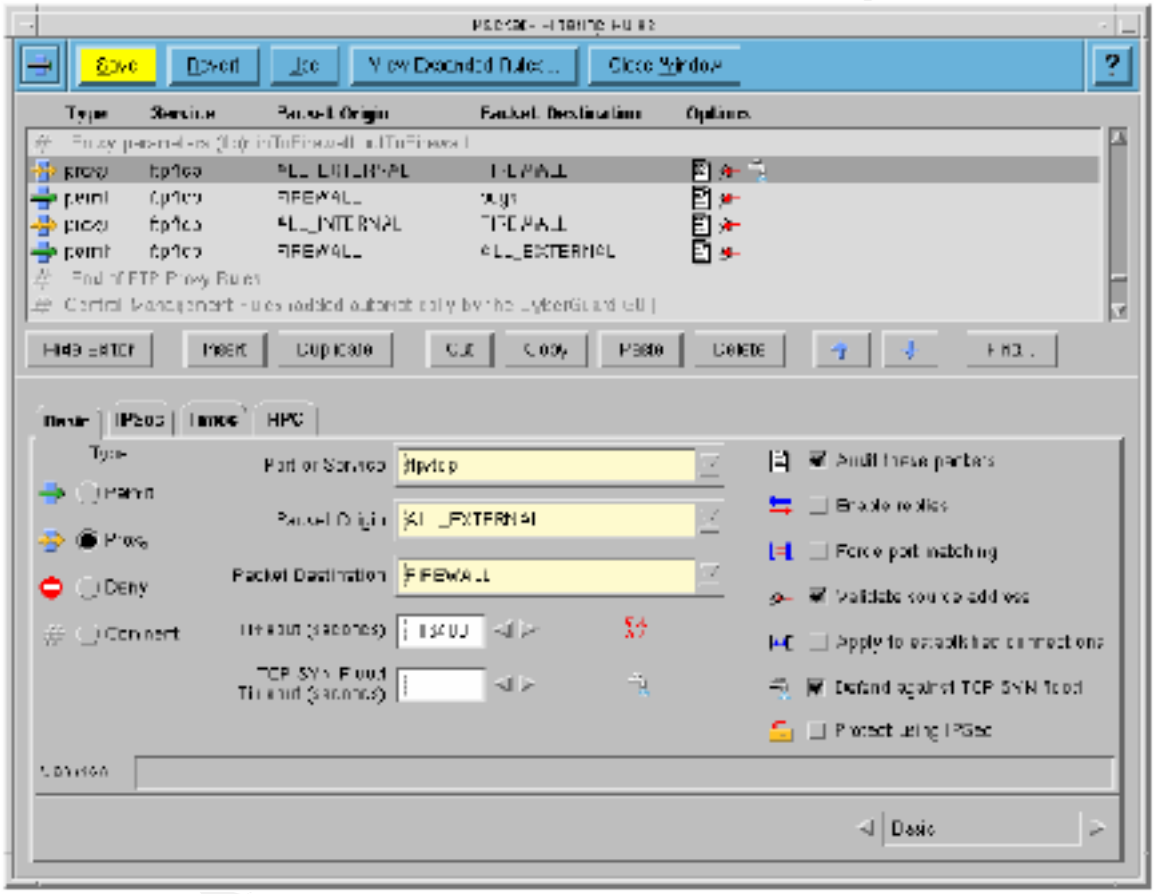
```
################################################################################
#
#       Internet Protocol Packet Filter Rules Configuration File
#
################################################################################
#
################################################################################
#
# Select any alternative from each column.
#
# Action service/protocol Frm host/subnetmask To host/subnetmask  Options
# ====== ===============  ================== ==================  ===========
#
# PERMIT service/protocol INTERNAL_NETWORK    INTERNAL_NETWORK    ENABLE_REPLY
# DENY   service          EXTERNAL_NETWORK    EXTERNAL_NETWORK    DONT_AUDIT
# PROXY  ALL              LOCAL_HOST          LOCAL_HOST          TIME_OUT=nnn
#        ALL/protocol     EVERYONE            EVERYONE            NO_IF_CHECK
#                         if_NETWORK          if_NETWORK          TCPSYNFLD
#                         nnn.nnn.nnn.nnn     nnn.nnn.nnn.nnn     TCPSYNFLD_TIMEOUT=nnn
#                         nnn.nnn.nnn.nnn/subnet nnn.nnn.nnn.nnn/subnet
#
################################################################################
################################################################################
#
#
# EXAMPLES
#
# Allow ping / echo packets
#
#permit echo/icmp      EVERYONE       EVERYONE       ENABLE_REPLY
#permit echo/udp       EVERYONE       EVERYONE       ENABLE_REPLY
#
#
include /etc/security/firewall/ng_inet/netguard.include
########################################################################
# The following line is used to locate the end of the header comments.
# DO NOT DELETE OR MODIFY THIS LINE.
# Place site-specific rules here, above the rules that are generated
# automatically by the firewall administrative interface.
########################################################################

# The following rules were added to allow all machines on the internal network
```

```
# the ability to connect to the web server using http and/or https.
proxy   http/tcp       192.168.1.0/28 10.1.1.2
proxy   https/tcp      192.168.1.0/28 10.1.1.2

# These rules allow machines from both the customer service network and the
# partners/suppliers network to send syslog messages to the syslog server.
permit  514/udp 10.1.1.0/28    192.168.1.2
permit  514/udp 192.168.2.0/28 192.168.1.2


# This rule allows the border router to send syslog
# messages to the syslog server.
permit  514/udp c.c.c.1  c.c.c.3

# These rules allow the NTP Server on the customer service network to
# query three public stratum-2 NTP Servers.
permit  123/udp 10.1.1.3       ntppub.tamu.edu        ENABLE_REPLY   tbr=0:0100-
0200+1:0100-0200+2:0100-0200+3:0100-0200+4:0100-0200+5:0100-0200+6:0100-0200
permit  123/udp 10.1.1.3       ntp.cox.smu.edu        ENABLE_REPLY   tbr=0:0100-
0200+1:0100-0200+2:0100-0200+3:0100-0200+4:0100-0200+5:0100-0200+6:0100-0200
permit  123/udp 10.1.1.3       ntp.fnbhs.com          ENABLE_REPLY   tbr=0:0100-
0200+1:0100-0200+2:0100-0200+3:0100-0200+4:0100-0200+5:0100-0200+6:0100-0200

# These rules allow all machines from both the internal network and
# the partners/suppliers network to send NTP queries to the NTP server.
permit  123/udp 192.168.1.0/28 10.1.1.3       ENABLE_REPLY
permit  123/udp dec3_NETWORK   10.1.1.3       ENABLE_REPLY

# These rules allow CFE's internal network to communicate to GIAC's
# partners/suppliers network and vice versa using all protocols.  These two rules are
# only enabled through the gateway-to-gateway VPN established between
# GIAC's firewall and CFE's firewall.
permit  ALL     172.16.1.0/24  192.168.2.0/24  ENABLE_REPLY ipsec=HighSecurity:sa-per-
net:0x2:auto:auto
permit  ALL     192.168.2.0/24 172.16.1.0/24   ENABLE_REPLY ipsec=HighSecurity:sa-per-
net:0x2:auto:auto

# The first rule allows the partners/suppliers database to replicate to the internal
# database, but only from 1:00am-2:00am each night.  The second rule allows the
# internal database to update the subset of fortunes on the partners/suppliers database,
# but only from 1:00am-2:00am each night.
permit  sqlnet/tcp     192.168.2.2   192.168.1.4     tbr=0:0100-0200+1:0100-0200+2:0100-
0200+3:0100-0200+4:0100-0200+5:0100-0200+6:0100-0200
permit  sqlnet/tcp     192.168.1.4    192.168.2.2     tbr=0:0100-0200+1:0100-0200+2:0100-
0200+3:0100-0200+4:0100-0200+5:0100-0200+6:0100-0200

#
# DO NOT DELETE OR MODIFY THE FOLLOWING LINE.
# DO NOT DELETE: The following rules are added during initial boot.
# These rules allow any internal machine to ping the internal interface
# of the firewall available from to its respective network.  They are only
# uncommented for network troubleshooting situations.
# permit       echo/icmp      ALL_INTERNAL   FIREWALL        ENABLE_REPLY
# permit       echo/icmp      FIREWALL       ALL_INTERNAL    ENABLE_REPLY
# DO NOT DELETE: The above rules are added during initial boot.

# Automatically-generated rules added here.

# SqlNet proxy rules (added automatically)
# Proxy parameters (sqlnet): outToFirewall
# This rule allows the customer web server to send requests to the internal database
# using the sqlnet smartproxy
proxy   sqlnet/tcp     10.1.1.2       192.168.1.4
# End of SqlNet proxy rules

# SMTP proxy rules (added automatically)
# Proxy parameters (smtp): inToFirewall outThruFirewall
# These two rules allow external mail to be sent to the external mail server via
# the smtp proxy.  TCP SYN FLOOD protection is enabled for this connection.
proxy   smtp/tcp       ALL_EXTERNAL   FIREWALL        TCPSYNFLD TCPSYNFLD_TIMEOUT=10
permit  smtp/tcp       FIREWALL       10.1.1.3
```

```
# This rule allows the external mail server to connect to the internet
# to send email using the smtp proxy.
proxy   smtp/tcp       10.1.1.3       ALL_EXTERNAL

# These two rules allow the internal mail server to send and receive mail from the
# external mail server using the smtp proxy.
proxy   smtp/tcp       192.168.1.1    10.1.1.3
proxy   smtp/tcp       10.1.1.3       192.168.1.1
# End of SMTP proxy rules

# Passport One rules (added automatically)
# This rule anyone from the internet to connect to the Passport One facility
# on the firewall for authentication.  This is the mechanism that allows
# host-to-gateway VPN connections to be established.  TCP SYN FLOOD protection is
# enabled for this rule.
permit  3443/tcp       ALL_EXTERNAL   FIREWALL        TCPSYNFLD TCPSYNFLD_TIMEOUT=10

# This rule allows the firewall to communicate with the DSS server for
# authentication of remote employees.
permit  2626/tcp       FIREWALL       192.168.1.5
# End of Passport One rules

# FTP proxy rules (added automatically)
# Proxy parameters (ftp): inToFirewall outThruFirewall
# This rule allows all internal employees to ftp to the internet using
# the ftp proxy.
proxy   ftp/tcp 192.168.1.0/28 ALL_EXTERNAL
# End of FTP proxy rules

# Auditlogd Syslog rules (added automatically)
# This rule allows the firewall to send syslog messages to the
# syslog server.
permit  514/udp FIREWALL 192.168.1.2
# End of Auditlogd Syslog rules

# Split DNS rules (added automatically)
# This rules enable the functionality of the built-in split-DNS software
# on the firewall.  No zone transfers are allowed, and TCP SYN FLOOD defense
# is enabled for all dns requests coming from the internet.
permit  domain/tcp     ALL_EXTERNAL   EXTERNAL_INTERFACES     TCPSYNFLD
TCPSYNFLD_TIMEOUT=10
permit  domain/tcp     EXTERNAL_INTERFACES    ALL_EXTERNAL
permit  domain/udp     ALL_EXTERNAL   EXTERNAL_INTERFACES     ENABLE_REPLY
permit  domain/udp     EXTERNAL_INTERFACES    ALL_EXTERNAL    ENABLE_REPLY
permit  domain/tcp     ALL_INTERNAL   INTERNAL_INTERFACES
permit  domain/tcp     INTERNAL_INTERFACES    ALL_INTERNAL
permit  domain/udp     ALL_INTERNAL   INTERNAL_INTERFACES     ENABLE_REPLY
permit  domain/udp     INTERNAL_INTERFACES    ALL_INTERNAL    ENABLE_REPLY
deny    domain/tcp     EVERYONE       EVERYONE
deny    domain/udp     EVERYONE       EVERYONE
# End of Split DNS rules

# SSL proxy rules (added automatically)
# Proxy parameters (ssl): inToFirewall outToFirewall outThruFirewall
# These two rules allow ssl traffic to reach the customer web server
# using the ssl proxy. TCP SYN Flood defense is enabled.
proxy   https/tcp      ALL_EXTERNAL   FIREWALL        TCPSYNFLD TCPSYNFLD_TIMEOUT=10
permit  https/tcp      FIREWALL       10.1.1.2

# This rule allows internal employees to establish ssl connections to
# the internet using the ssl proxy.
proxy   https/tcp      192.168.1.0/28 ALL_EXTERNAL
# End of SSL proxy rules

# HTTP proxy rules (added automatically)
# Proxy parameters (http): inToFirewall outThruFirewall
# These two rules allow http traffic to reach the customer web server
# from the internet using the http proxy.
proxy   80/tcp  ALL_EXTERNAL   FIREWALL        TCPSYNFLD TCPSYNFLD_TIMEOUT=10
permit  80/tcp  FIREWALL       10.1.1.2
```

```
# This rule allows internal employees to browse the internet
# using the http proxy.
proxy   80/tcp  192.168.1.0/28 ALL_EXTERNAL
# End of HTTP proxy rules

# End of automatically generated rules.
#
# This deny rule should always be the last rule.
#
deny    ALL     EVERYONE        EVERYONE        ENABLE_REPLY
```

Below is screen shot of the window used to enter packet filtering rules on the Cyberguard firewall. The screen shot does not reflect the rules listed above.



Packet Filtering Rules Window

2.3 VPN policy and tutorial

2.3.1 VPN description and rule set

A VPN, which stands for Virtual Private Network, provides a secure connection between distant networks and nodes. It ensures origin authentication, confidentiality, and integrity for data that travels through unsecured networks such as those found on the Internet[1]. A VPN is an excellent way to share data

with a company partner, allow employees to work remotely, and grant access to internal resources by other trusted entities.

The Cyberguard VPN is based on IPSEC (IP Security), which secures data at the network level through protocols such as Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). To learn more about IPSEC and its protocol suite see the Resources section at the end of this paper.

The Cyberguard VPN offers two types of connections, host-to-gateway and gateway-to-gateway, both of which are employed by GIAC. A gateway-to-gateway VPN connection is one that is formed between two gateway devices such as two Cyberguard firewalls and is usually persistent. This type of connection is best suited for company partnerships in which there are known static IP addresses for both entities. This is the type of VPN connection that GIAC uses in conjunction with CFE. A host-to-gateway connection is one in which a host entity running VPN client software connects to a VPN gateway on a temporary basis. This type of connection is best suited for teleworkers and remote employees who need access to internal resources on a periodic basis. It is also useful for temporarily trusted relationships between separate corporate entities. GIAC employs this type of VPN connection for remote employees and suppliers. This type of connection was chosen for suppliers because they frequently change and are not as trusted as partners. The Passport One mechanism on the firewall allows host-to-gateway VPN connections to be established from any valid IP address on the Internet.

The Passport One mechanism can be configured to use any of the following three protocols: http, https, or telnet. GIAC decided it was best to use only https because both http and telnet would send the username and password of any person authenticating in clear text over the Internet. In order to configure Passport One to use https, a server-side SSL certificate has to be placed on the firewall in the **/etc/security/firewall** directory. If this certificate cannot be found by Passport One, it will not open up the default port of 3443 to receive connections via https. A script provided by Cyberguard that generates this certificate can be found in Appendix A.

As stated above, GIAC uses host-to-gateway VPN connections for both suppliers and remote employees. In order to enable this, two Passport One profiles were created: supplier_prof and rmusers_prof. Through these profiles certain packet filtering rules can be enforced. This provides the unique capability of using the same VPN channel for both suppliers and remote employees, but enforcing different rule sets for each. These rule sets are only enabled after suppliers or remote employees have authenticated to their respective Passport One profile and a proper VPN connection has been established. The files containing the rule sets for both the supplier_prof and rmusers_prof profiles are displayed below.

These files can be found under the **/etc/security/firewall/clas/profiles/local** directory on the firewall.

- **rmusers_prof profile rule set**

```
# This rule gives remote employees the ability to telnet to the internal telnet server
# using the generic Port Guard proxy over the VPN channel.
proxy   telnet/tcp     %USER   FIREWALL       ipsec=HighSecurity:sa-per-
net:0x3:remote:auto

# This rule permits the firewall to communicate with the internal telnet server.
permit  telnet/tcp     FIREWALL       192.168.1.6
```

- **supplier_prof profile rule set**

```
# This rule allows suppliers to ftp to the partners/suppliers database using
# the FTP proxy over the VPN channel.
proxy   ftp/tcp %USER   FIREWALL        ipsec=HighSecurity:sa-per-net:0x3:remote:auto

# This rule allows the firewall to communicate with the partners/suppliers database.
permit  ftp/tcp FIREWALL       192.168.2.2
```

The rules for the gateway-to-gateway VPN connection between GIAC and CFE were given in the firewall rule set section above. Figure 2 below gives a graphical representation of the services permitted through the two VPN connections employed by GIAC.

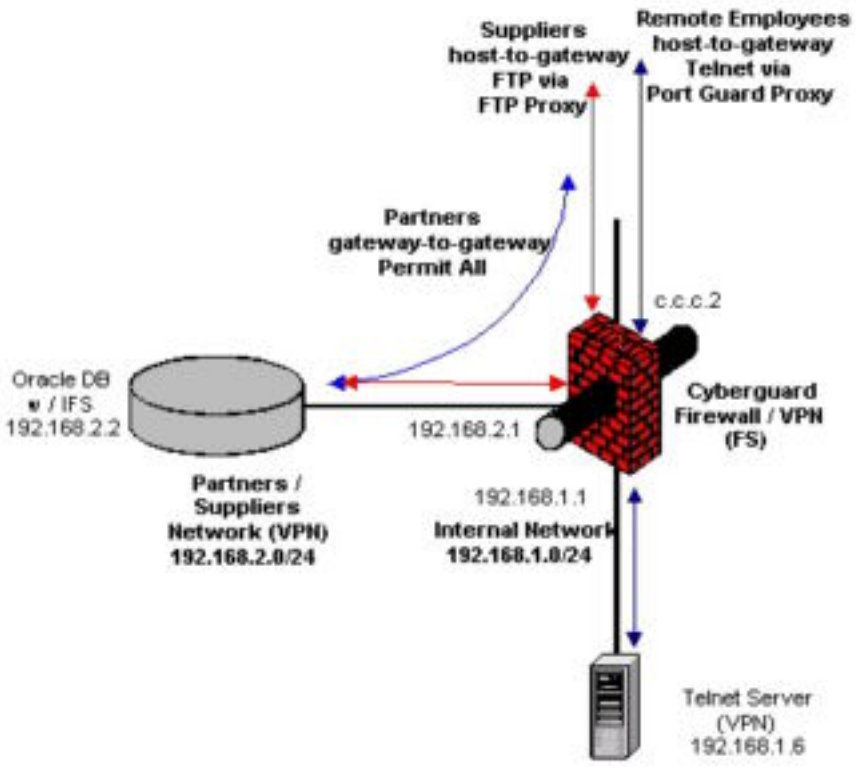


Figure 2.
Services Permitted through VPN Connections

2.3.2 VPN Tutorial

This section describes the steps taken to create the two VPN connections employed by GIAC. The first connection described is gateway-to-gateway, and the second connection is host-to-gateway. Cyberguard refers to VPN connections as secure channels. Most of this tutorial was taken directly from Cyberguard's Firewall Manual[1].

- **How to configure GIAC's gateway-to-gateway connection**

Step 1 – Create a Channel to the IPSec Peer Network (CFE)

1) Select **Configuration** from the Control Panel.

2) Select **VPN Secure Channels**. The VPN Secure Channels window appears.

3) Click on the **Channel Information** tab. The Channel Information page appears.
4) Click on **Show Editor**. The expanded Channel Information page appears.

5) Click on **Insert** to begin creating a new secure channel.

6) Type **CFE** (for China Fortunes Enterprises) in the **Channel Name** field.

7) Select **Gateway** as the **Peer Type**.

8) Type **a.a.a.1** (CFE's external firewall interface) in the **Host Name** field.

9) Select **IKE** (Internet Key Exchange) as the **Establish Keys Using** selection.

10) Type a <secret phrase> in the **Preshared Secret** field. Firewall administrators from GIAC and CFE have agreed upon this secret phrase, which must be configured the same on both gateways.

11) Click on the **Advanced** button next to the **Preshared Secret** field.

12) Check the **Use Identity** checkbox under the **Preshared Secret**.

13) Under **IKE Data**, select **HighSecurity** in the **IKE Protection Strategy** list box. This enforces the use of only the most secure encryption algorithms such as 3des, aes, and twofish.

Step 2 - Identify Networks Protected by CFE's Firewall

1) Click on the **Peer Protected Networks** tab of the VPN Secure Channels window.

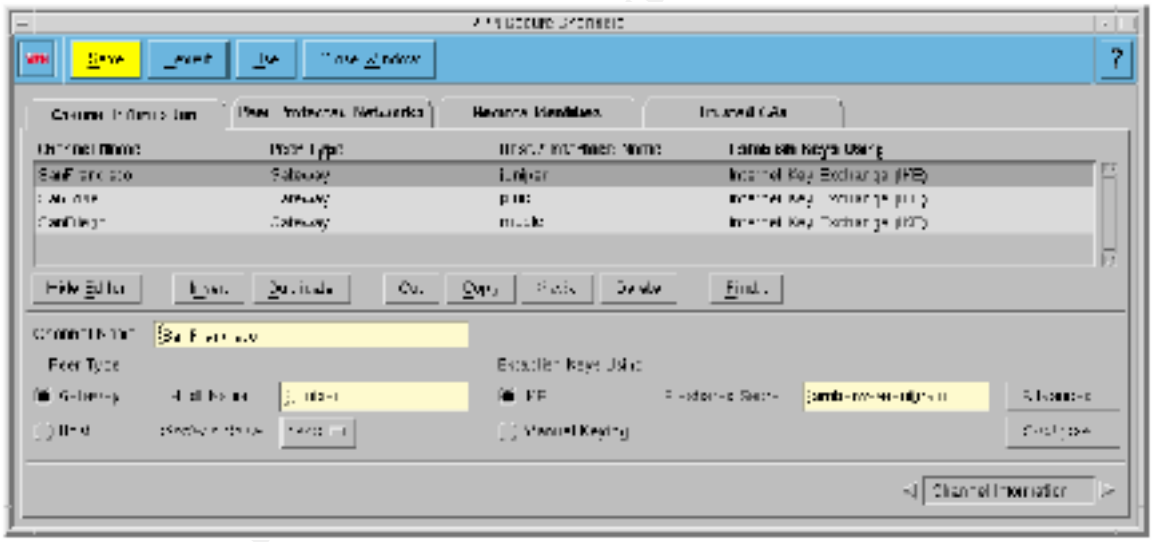
2) In the **VPN Secure Channels** list on the left side of the page, select **CFE**.

3) Click on **Show Editor**.

4) Click on **Insert**.

5) In the **Network Address** field, type **172.16.1.0/255.255.255.0**.

Below is a screen shot of the window used to configure VPN Secure Channels on the Cyberguard firewall. It does not reflect the configuration described in this paper.



VPN Secure Channels Window

Step 3 - Define Packet-Filtering Rules

1) Select **Configuration** from the Control Panel.

2) Select **Packet-Filtering Rules**. The Packet-Filtering Rules window appears.
3) Click on **Show Editor**. The expanded window appears.

4) Click on the **Basic** tab. The Basic page appears.

5) Enter the following rules:

```
permit ALL 172.16.1.0/24 192.168.2.0/24
permit ALL 192.168.2.0/24 172.16.1.0/24
```

6) For both rules, select the rule and check the **Protect using IPSec** option.

7) Select the **IPSec** tab.

8) Select **HighSecurity** in the **IPSec Protection Strategy** list box.

9) Click on **Save**. Your changes take effect at the next system reboot.

10)(Optional) Click on **Use**. Your changes take effect immediately.

- **How to configure GIAC's host-to-gateway VPN connection (dynamic address)**

Step 1 - Define a Channel to the IPSec Peer (host)

1) Select **Configuration** from the Control Panel.

2) Select **VPN Secure Channels**. The VPN Secure Channels window appears.

3) Click on the **Channel Information** tab. The Channel Information page appears.

4) Click on **Show Editor**. The expanded Channel Information page appears.

5) Click on **Insert**.

6) Type **remote** in the **Channel Name** field.

7) Select **Host** as the **Peer Type**. An example of a host is a single end-user machine, known as a VPN client.

8) Select **dec0**, which is the external interface of the firewall, in the **Interface Name** list box. This is the interface to which the peer (VPN client) will connect.

9) Select **IKE** (Internet Key Exchange) as the **Establish Keys Using** selection.

10)Type a <secret phrase> in the **Preshared Secret** field. GIAC's firewall administrator has communicated this secret phrase to both remote

employees and suppliers. This secret phrase must be configured in the VPN client software that is used by both groups.

Note: When the IPSec peer type is a host with an unknown IP address, the host cannot be specified on the Peer Protected Networks page. This limits the information the firewall has in attempting to automatically select an VPN Secure Channel for a particular packet-filter rule. Therefore, **Enable Manual Selection of VPN Secure Channel** will need to be configured for each applicable packet-filtering rule, on the IPSec page of the Packet-Filtering Rules window. Described below.

Step 2 - Define Packet-Filtering Rules

Because the IP address of the client is not known, the Passport One mechanism is used to set up the packet-filtering rules. This allows use of the %USER construct so that the source IP address of the system from which the user made the authenticating connection is substituted into the packet-filtering rules.

1) Select **Configuration** from the Control Panel.

2) Select **Passport One**. The Passport One window appears.

3) Click on the **Setup** tab. The Setup page appears.

4) Check **Enable**.

5) Under **Enabled Interfaces**, check the firewall interface that corresponds to the interface selected in Step 1, which is **dec0**.

6) Under **Authentication Ports** check the **HTTPS** checkbox, and uncheck the **HTTP** and **Telnet** checkboxes. Accept the defaults for **Maximum Number of Sessions**, and **Refresh Interval**.

7) Click on the **Profiles** tab. The Profiles page appears.

8) Click on **Insert**.

9) Type **supplier_prof** in the **Profile Name** field.

10) Click on the **Rules** tab. The Rules page appears.

11) Click on **Insert**.

12) Enter the following packet filter rules:

```
proxy     ftp/tcp   %USER     FIREWALL
permit    ftp/tcp   FIREWALL  192.168.2.2
```

13)For the proxy rule above, check the option **Protect using IPSec**.

14)Click on the **IPSec** tab.

15)Select **HighSecurity** in the **IPSec Protection Strategy** list box.

16)Because the **%USER** is in the Packet Origin field of the packet-filtering rule, click on the **To Packet Origin** box in the **Enable Manual Selection of VPN Secure Channel** section. Then select **remote** from the list box.

17)Check the **Allow NAT to Translate Addresses** checkbox.

18)Click on the **Profiles** tab. The Profiles page appears.

19)Click on **Insert**.

20)Type **rmusers_prof** in the **Profile Name** field.

21)Click on the **Rules** tab. The Rules page appears.

22)Select **rmusers_prof** in the **Profile Name** list box. **Click** on **Insert**.

23)Enter the following packet filter rules:

```
proxy     telnet/tcp     %USER      FIREWALL
permit    telnet/tcp     FIREWALL   192.168.1.6
```

24)For the proxy rule above, check the option **Protect using IPSec**.

25)Click on the **IPSec** tab.

26)Select **HighSecurity** in the **IPSec Protection Strategy** list box.

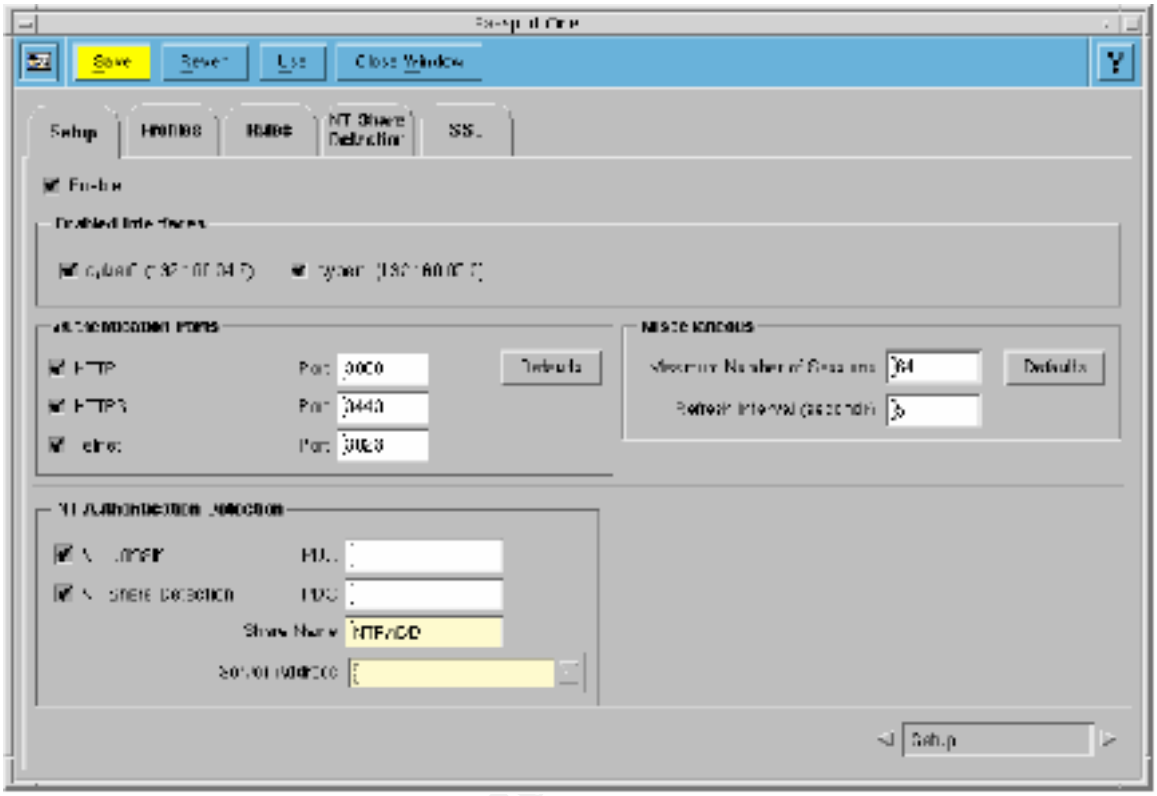
27)Because the **%USER** is in the Packet Origin field of the packet-filtering rule, click on the **To Packet Origin** box in the **Enable Manual Selection of VPN Secure Channel** section. Then select **remote** from the list box.

28)Check the **Allow NAT to Translate Addresses** checkbox.

29)Click on **Save**. Your changes take effect at the next system reboot.

30)(Optional) Click on **Use**. Your changes take effect immediately.

Below is a screen shot of the window used to configure the Passport One mechanism on the Cyberguard firewall. The screen shot does not reflect the configuration described above.



Passport One Window

Step 3 - Associate Remote Users and Suppliers with their Passport One Profiles

1) Select **Configuration** from the Control Panel.

2) Select **Users**. The Users window appears.

3) Click on **Show Editor**. The expanded Users window appears.

4) Click on **Insert**. The list is scrolled to the end. An incomplete new line appears.

5) Type **supplier** in the **Login ID** field. Type **GIAC suppliers** in the **Full Name** field.

6) Click on the **Authentication** tab. The Authentication page appears.

7) Select **Disabled** in the **Internal Method** list box. Select **Password** in the **External Method** list box.

8) Click the **Generate** button to generate a strong password for the supplier user. Check the **Age password** checkbox, and enter 30 in the **Maximum Age (days)** field.

9) Click on the **Passport One Rules** tab. The Passport One Rules page appears.

10) Click on **Insert**. Select **supplier_prof** from the **Profile** list box and type a * in the **Source Address** field because the address of the host is unknown. Type **0** in the **Duration** field. A **0** specifies an unlimited session.

11) Click on the **User Information** tab.

12) Click on **Insert**. The list is scrolled to the end. An incomplete new line appears.

13) Type **rmtuser** in the **Login ID** field. Type **GIAC remote employees** in the **Full Name** field.

14) Click on the **Authentication** tab. The Authentication page appears.

15) Select **Disabled** in the **Internal Method** list box. Select **SecureNetKey** in the **External Method** list box.

16) Click on the **Passport One Rules** tab. The Passport One Rules page appears.

17) Click on **Insert**. Select **rmusers_prof** from the **Profile** list box and type a * in the **Source Address** field because the address of the host is unknown. Type **0** in the **Duration** field. A **0** specifies an unlimited session.

18) Click on **Save**.

3. Assignment 3 – Verify the Firewall Policy

3.1 Plan the audit

As part of the contract agreement established between China Fortunes Enterprises(CFE) and GIAC, it was agreed upon that both companies would send a group of its firewall administrators to audit the others' firewall. This was beneficial for both companies. In GIAC's case it:

- Provided an unbiased evaluation of their firewall
- Saved the money of having to hire a third party auditor

- Allowed the firewall administrators from interact and get to know one another
- Allowed GIAC to gauge the amount of trust that it should be give to the gateway-to-gateway VPN connection shared with CFE

It was decided that CFE's administrators would audit GIAC's firewall first. GIAC and CFE administrators worked together to come up with the best and most efficient plan for the audit. It was decided that the standby firewall in GIAC's network would be used for testing. Before removing the standby firewall from the network GIAC had to send out several notifications. All remote employees and suppliers were notified by email of the upcoming tests. The email stated that the standby firewall of the high availability cluster was going to be removed for auditing on a certain date, and barring any unforeseen problems with the active firewall, the tests would go unnoticed by network users. The plan was that the audit would take at most one full work day to complete. A message was also posted on the GIAC home page notifying customers of the upcoming tests, but no detail was given.

A test network using just three machines was set up and fully configured in GIAC's development lab before the standby firewall was removed from the real network. Each of the three machines was connected to a different interface of the firewall to represent all servers for that given network as shown in Figure 3 below.

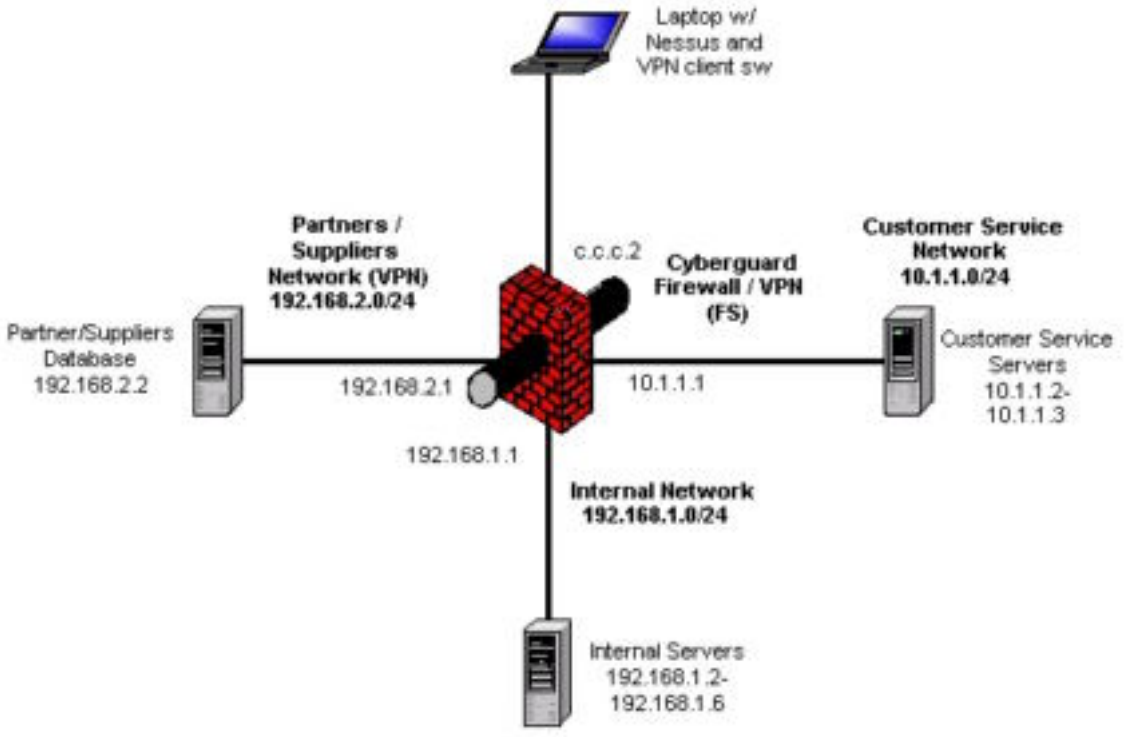


Figure 3.
Test Network

A standard Apache web server has been set up on the machine representing the customer service network. The machine representing the internal network has been configured to receive telnet connections, and an FTP server has been set up on the machine representing the partners/suppliers network. Nessus[15] has been downloaded and compiled on a laptop in the test lab, and it is going to serve as the primary auditing tool to verify GIAC's firewall policy. Nessus version 1.2.2 was chosen as the auditing tool for several reasons including:

- It is widely accepted and supported.
- It is extremely easy of use.
- It is free.
- It offers a non-destructive mode.
- It has a wide range of configurations.
- It has excellent reporting options.
- It is very powerful and employs nmap for scanning

The following is the test procedure that is going to be used to audit the firewall and verify GIAC's policy.

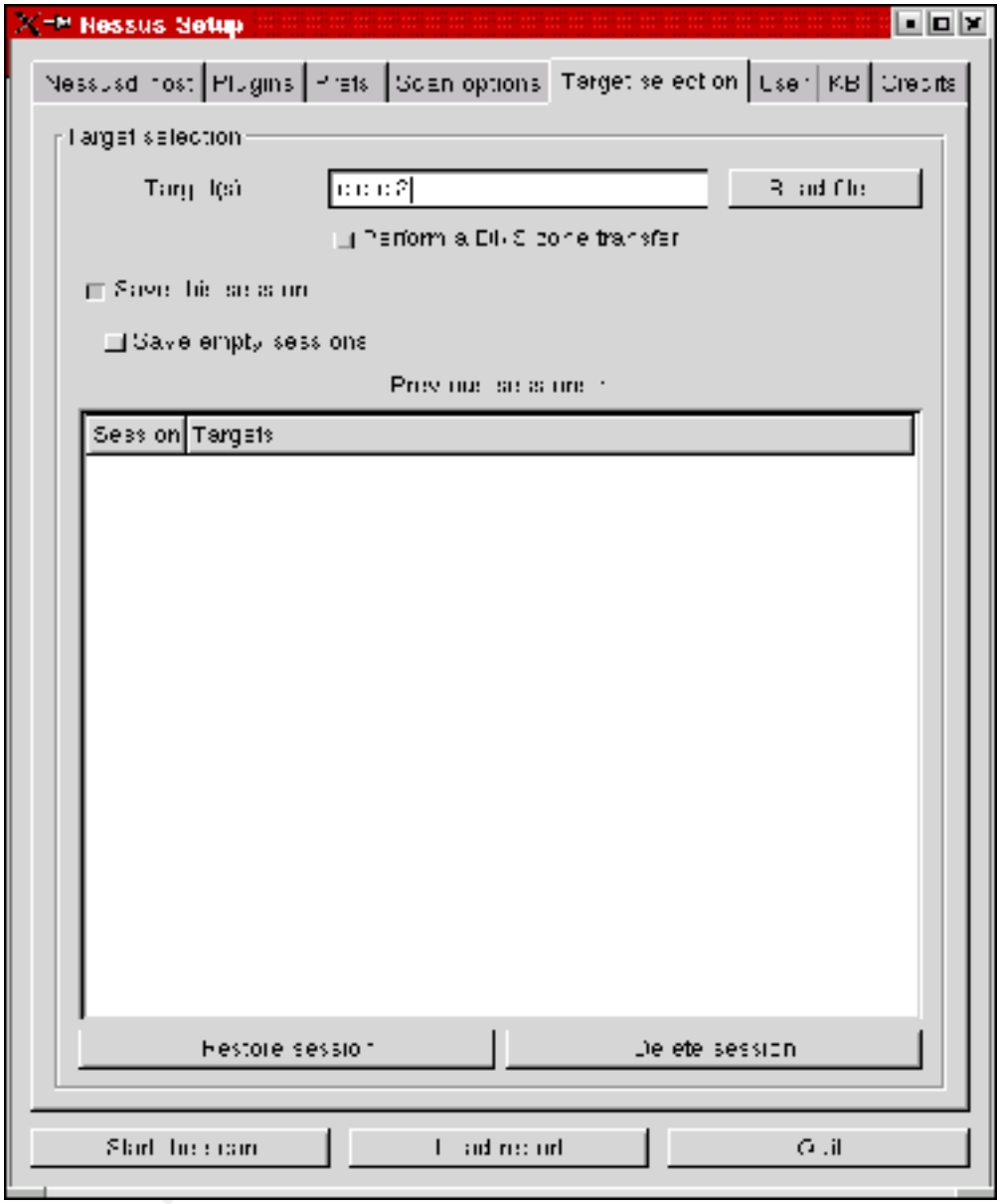
1. Connect the laptop running nessusd (standard configuration file) to the external interface of the firewall as shown in Figure 3 above.

2. Configure the Nessus client in the following manner:

    a. Under the **Plugins** tab, enable all but the dangerous plugins and denial of service (DoS) attacks.

    b. Under the **Scan Options** tab, input a full port range of 1-65535, select **Optimize the test**, and select **Nmap tcp connect() scan** as the port scanner(it runs the fastest).

    c. Under the **Target selection** tab, input **c.c.c.2** (external interface of firewall) as the target for the scan.



3. Perform the scan.

4. Log in as a **supplier** user using the Passport One mechanism on the firewall, and enable the client VPN software on the laptop to establish a VPN connection.

5. Verify the ability to ftp to the partners/suppliers database (192.168.2.2) via the FTP smartproxy.

6. Log in as a **rmtuser** user using the Passport One mechanism on the firewall, and enable the client VPN software on the laptop to establish a VPN connection.

7. Verify the ability to telnet to the internal telnet server (192.168.1.6) via the generic Port Guard smartproxy.

8. Connect the laptop to the customer service network on the firewall, and configure Nessus as described above. Make sure to change the target IP address to 10.1.1.1. Perform the scan.

9. Connect the laptop to the partners/suppliers network on the firewall, and configure Nessus as described above. Make sure to change the target IP address to 192.168.2.1. Perform the scan.

10. Connect the laptop to the internal network on the firewall, and configure Nessus as described above. Make sure to change the target IP address to 192.168.1.1. Perform the scan.

3.2 Audit Results and Analysis

- **External Interface Audit**

Nessus provided the following output from the scan of the firewall's external interface as described above. Addresses have been sanitized.

```
results|c.c.c|c.c.c.2|general/tcp|10336|Security Note|"Default scan"
set. nmap will ignore the user specified port range and scan only the
1024 first ports and those declared in nmap-services
```

These lines show ports that are expected to be open. The Passport One port (3443) was not identified as open because nmap only scanned the first 1024 ports. There were no unexpected ports found open.

```
results|c.c.c|c.c.c.2|smtp (25/tcp)
results|c.c.c|c.c.c.2|domain (53/tcp)
results|c.c.c|c.c.c.2|http (80/tcp)
results|c.c.c|c.c.c.2|https (443/tcp)
```

These lines show how proficient Nessus can be in identifying the exact version of a web server and/or operating system. The fact that Nessus correctly identified the test web server and its operating system reaffirms the need for GIAC's customer web server to purposefully send bogus replies for any such queries.

```
results|c.c.c|c.c.c.2|http (80/tcp)|10330|Security Note|a web server is
running on this port
results|c.c.c|c.c.c.2|https (443/tcp)|10330|Security Note|A TLSv1
server answered on this port\n
results|c.c.c|c.c.c.2|https (443/tcp)|10330|Security Note|a web server
is running on this port through SSL
results|c.c.c|c.c.c.2|http (80/tcp)|10107|Security Note|The remote web
server type is :\n\nApache-AdvancedExtranetServer/1.3.20 (Mandrake
Linux/3mdk) mod_ssl/2.8.4 OpenSSL/0.9.6b PHP/4.0.6\r\n\nWe recommend
```

```
that you configure your web server to return\nbogus versions in order
to not leak information\n
results|c.c.c|c.c.c.2|https (443/tcp)|10107|Security Note|The remote
web server type is :\n\nApache-AdvancedExtranetServer/1.3.20 (Mandrake
Linux/3mdk) mod_ssl/2.8.4 OpenSSL/0.9.6b PHP/4.0.6\r\n\nWe recommend
that you configure your web server to return\nbogus versions in order
to not leak information\n
results|c.c.c|c.c.c.2|smtp (25/tcp)|10263|Security Note|Remote SMTP
server banner :\n0\n0
```

GIAC is running mod_ssl version 2.8.10 on the customer web server so this buffer overflow vulnerability has been averted.

```
results|c.c.c|c.c.c.2|http (80/tcp)|10888|Security Hole|\nThe remote
host is using a version of mod_ssl which is\nolder than 2.8.7.\n\nThis
version is vulnerable to a buffer overflow which,\nalbeit difficult to
exploit, may allow an attacker\nto obtain a shell on this host.\n\n***
Some vendors patched older versions of mod_ssl, so this\n*** might be a
false positive. Check with your vendor to determine\n*** if you have a
version of mod_ssl that is patched for this \n***
vulnerability\n\n\nSolution : Upgrade to version 2.8.7 or newer\nRisk
factor : High\nCVE : CAN-2002-0082\n
results|c.c.c|c.c.c.2|https (443/tcp)|10888|Security Hole|\nThe remote
host is using a version of mod_ssl which is\nolder than 2.8.7.\n\nThis
version is vulnerable to a buffer overflow which,\nalbeit difficult to
exploit, may allow an attacker\nto obtain a shell on this host.\n\n***
Some vendors patched older versions of mod_ssl, so this\n*** might be a
false positive. Check with your vendor to determine\n*** if you have a
version of mod_ssl that is patched for this \n***
vulnerability\n\n\nSolution : Upgrade to version 2.8.7 or newer\nRisk
factor : High\nCVE : CAN-2002-0082\n
```

Nessus found that the Cyberguard firewall uses non-random IP IDs, which allows them to be predicted. Tools like HPING2 can use this vulnerability to do spoofed port scanning. GIAC needs to contact Cyberguard to see if there is a patch for this.

```
results|c.c.c|c.c.c.2|general/tcp|10201|Security Warning|\nThe remote
host uses non-random IP IDs, that is, it is\npossible to predict the
next value of the ip_id field of\nthe ip packets sent by this
host.\n\nAn attacker may use this feature to determine if the
remote\nhost sent a packet in reply to another request. This may
be\nused for portscanning and other things.\n\nSolution : Contact your
vendor for a patch\nRisk factor : Low
```

The weak and medium ciphers on GIAC's customer web server need to be disabled to ensure that they are not used.

```
results|c.c.c|c.c.c.2|https (443/tcp)|10863|Security Warning|The SSLv2
server offers 4 strong ciphers, but also\n2 medium strength and 2 weak
"export class" ciphers.\nThe weak/medium ciphers may be chosen by an
export-grade\nor badly configured client software. They only offer a
\nlimited protection against a brute force attack\n\nSolution: disable
those ciphers and upgrade your client\nsoftware if necessary
```

```
results|c.c.c|c.c.c.2|https (443/tcp)|10863|Security Warning|The TLSv1
server offers 18 strong ciphers, but also\n8 medium strength and 24
weak "export class" ciphers.\nThe weak/medium ciphers may be chosen by
an export-grade\nor badly configured client software. They only offer a
\nlimited protection against a brute force attack\n\nSolution: disable
those ciphers and upgrade your client\nsoftware if necessary
```

These lines display the various SSL versions accepted.

```
results|c.c.c|c.c.c.2|https (443/tcp)|10863|Security Note|This TLSv1
server also accepts SSLv2 connections
results|c.c.c|c.c.c.2|https (443/tcp)|10863|Security Note|This TLSv1
server also accepts SSLv3 connections
```

GIAC is using PHP version 4.2.3 on the customer web server so this vulnerability has been averted. The HTTP proxy employed by the firewall, which doesn't allow POST requests, also prevents this attack.

```
results|c.c.c|c.c.c.2|http (80/tcp)|10867|Security Hole|\nThe remote
host is running a version of PHP earlier\nthan 4.1.2.\n\nThere are
several flaws in how PHP handles\nmultipart/form-data POST requests,
any one of which can\nallow an attacker to gain remote acccess to the
system.\n\nSolution : Upgrade to PHP 4.1.2\nRisk factor : High\nCVE :
CAN-2002-0081\n
results|c.c.c|c.c.c.2|https (443/tcp)|10867|Security Hole|\nThe remote
host is running a version of PHP earlier\nthan 4.1.2.\n\nThere are
several flaws in how PHP handles\nmultipart/form-data POST requests,
any one of which can\nallow an attacker to gain remote acccess to the
system.\n\nSolution : Upgrade to PHP 4.1.2\nRisk factor : High\nCVE :
CAN-2002-0081\n
```

Testing of the VPN connection was also successful for both the supplier and rmtuser users. The supplier user was only able to ftp to the partners/suppliers database through the VPN connection, and the rmtuser user was only able to telnet to the internal telnet server through the VPN connection.

- **Internal Interface Audit (Customer Service Network)**

These are the results from the Nessus scan performed on the internal interface facing the customer service network (10.1.1.1).

```
results|10.1.1|10.1.1.1|general/tcp|10336|Security Note|"Default scan"
set. nmap will ignore the user specified port range and scan only the
1024 first ports and those declared in nmap-services
```

These lines show that port 25 is open for email traffic and that the split-DNS service (port 53) is running on the firewall. Sql port 1521, which used to send requests to the internal database server, was not found because only the first 1024 ports were scanned. Also, udp port scanning was not enabled so neither the syslog port (514) nor the NTP port (123) was found to be open. Udp port scanning was not enabled because it drastically increased scanning time.

```
results|10.1.1|10.1.1.1|smtp (25/tcp)
results|10.1.1|10.1.1.1|domain (53/tcp)
```

Nessus correctly identified the underlying operating system of the Cyberguard firewall appliance. GIAC has decided to notify Cyberguard and convey their test results involving this.

```
results|10.1.1|10.1.1.1|general/tcp|10336|Security Note|Nmap found that
this host is running SCO UnixWare 2.1.2\n
```

This was already discovered and addressed in the audit of the firewall's external interface.

```
results|10.1.1|10.1.1.1|general/tcp|10201|Security Warning|\nThe remote
host uses non-random IP IDs, that is, it is\npossible to predict the
next value of the ip_id field of\nthe ip packets sent by this
host.\n\nAn attacker may use this feature to determine if the
remote\nhost sent a packet in reply to another request. This may
be\nused for portscanning and other things.\n\nSolution : Contact your
vendor for a patch\nRisk factor : Low
```

- **Internal Interface Audit (Internal Network)**

These are the results from the Nessus scan performed on the internal interface facing the internal network (192.168.1.1).

```
results|192.168.1|192.168.1.1|general/tcp|10336|Security Note|"Default
scan" set. nmap will ignore the user specified port range and scan only
the 1024 first ports and those declared in nmap-services
```

These lines show that port 25 is open to allow the internal mail server to send email traffic to the external mail server. The split-DNS service (port 53) is running on the firewall. Sql port 1521, which used by the internal database server to push subsets of fortunes to the partners/suppliers database, was not found because only the first 1024 ports were scanned. Nessus did not find any of services allowing internal employees to connect to the Internet, which include HTTP, HTTPS, and FTP. Also, udp port scanning was not enabled so NTP port (123) was not found to be open. Udp port scanning was not enabled because it drastically increased scanning time.

```
results|192.168.1|192.168.1.1|smtp (25/tcp)
results|192.168.1|192.168.1.1|domain (53/tcp)
```

Nessus correctly identified the underlying operating system of the Cyberguard firewall appliance. This was addressed in the previous section.

```
results|192.168.1|192.168.1.1|general/tcp|10336|Security Note|Nmap
found that this host is running SCO UnixWare 2.1.2\n
```

This was already discovered and addressed in the audit of the firewall's external interface.

```
results|192.168.1|192.168.1.1|general/tcp|10201|Security Warning|\nThe
remote host uses non-random IP IDs, that is, it is\npossible to predict
the next value of the ip_id field of\nthe ip packets sent by this
host.\n\nAn attacker may use this feature to determine if the
remote\nhost sent a packet in reply to another request. This may
be\nused for portscanning and other things.\n\nSolution : Contact your
vendor for a patch\nRisk factor : Low
```

- **Internal Interface Audit (Partners/Suppliers Network)**

These are the results from the Nessus scan performed on the internal interface facing the partners/suppliers network (192.168.2.1).

```
results|192.168.2|192.168.2.1|general/tcp|10336|Security Note|"Default
scan" set. nmap will ignore the user specified port range and scan only
the 1024 first ports and those declared in nmap-services
```

These lines show the split-DNS service (port 53) is running on the firewall. Sql port 1521, which used by the partners/suppliers database server to replicate to the internal database, was not found because only the first 1024 ports were scanned. Also, udp port scanning was not enabled so NTP port (123) was not found to be open. Udp port scanning was not enabled because it drastically increased scanning time.

```
results|192.168.2|192.168.2.1|domain (53/tcp)
```

Nessus correctly identified the underlying operating system of the Cyberguard firewall appliance. This was addressed in the previous section.

```
results|192.168.2|192.168.2.1|general/tcp|10336|Security Note|Nmap
found that this host is running SCO UnixWare 2.1.2\n
```

This was already discovered and addressed in the audit of the firewall's external interface.

```
results|192.168.2|192.168.2.1|general/tcp|10201|Security Warning|\nThe
remote host uses non-random IP IDs, that is, it is\npossible to predict
the next value of the ip_id field of\nthe ip packets sent by this
host.\n\nAn attacker may use this feature to determine if the
remote\nhost sent a packet in reply to another request. This may
be\nused for portscanning and other things.\n\nSolution : Contact your
vendor for a patch\nRisk factor : Low
```

3.3 Audit Summary

The audit of GIAC's firewall went very well. They were able to complete the scans in a single workday as planned. No problems occurred with the active firewall protecting GIAC's production network while the standby firewall was absent, so no costs were incurred due to business outages. The only real costs incurred as a result of the audit will be that of sending two of GIAC's firewall

administrators to China for a few days in order to conduct an audit of CFE's firewall as part of the partnership agreement discussed earlier.

Major issues resulting from the audit include:

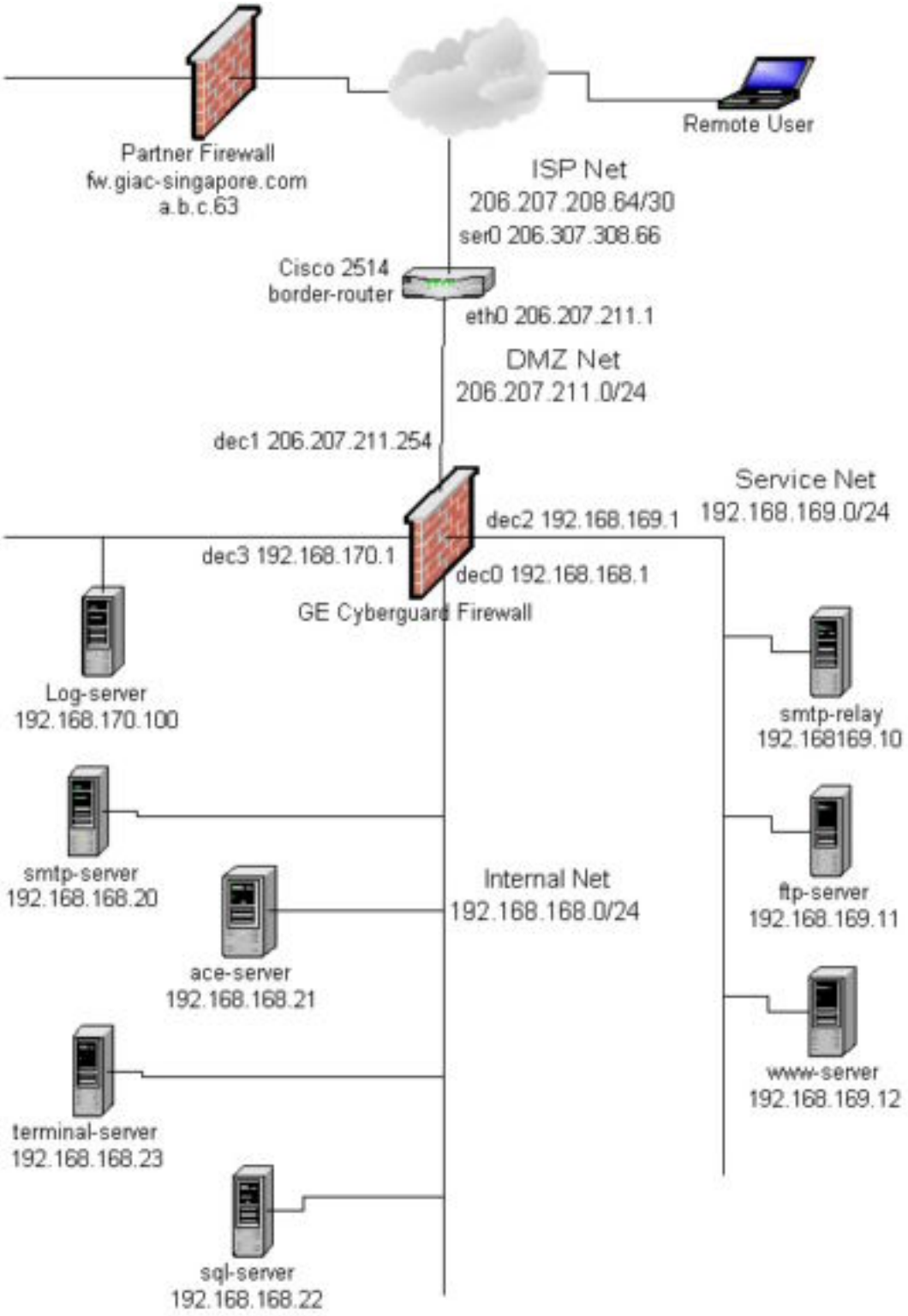
- Contacting Cyberguard to notify them of the non-random IP IDs issue and request a patch
- Contacting Cyberguard to notify them Nessus was able to correctly identify the underlying operating system of the Cyberguard FS model
- Disabling both the weak and medium ciphers on GIAC's customer web server

The audit also prompted GIAC's firewall administrators to:

- Reaffirm the configuration of the customer web server to return bogus replies to version and operating system queries.
- Check that the latest versions of both mod_ssl and PHP were being employed on the customer web server

4. Assignment 4 – Design Under Fire

I have chosen to attack the network constructed by Robert Wildt in his GCFW practical[16]. Below is the network diagram taken from his practical.



Network Diagram by Robert Wildt

Three separate attacks against this architecture are going to be proposed and discussed. The actual attacks could not be performed due to lack of the proper equipment. The three type of attacks that are going to be proposed are:

- An attack against the firewall itself.
- A denial of service (DoS) attack.
- An attack to compromise an internal system through the perimeter defense.

4.1 Attack Against the Firewall

After searching endlessly, only two possible vulnerabilities were found for the Cyberguard firewall. The first vulnerability was found only on several message boards and was not substantiated by any reliable source. Nevertheless, it was reported that a DoS (described in the next section) attack performed on the Cyberguard 4.0 line of firewalls could potentially cause it to crash[13]. Prerequisites were that the firewall had to be utilizing symmetric multi processing (SMP) and that the DoS attack had to force 50% utilization of the second processor. At that point the firewall would crash. It is also reported that Cyberguard has fixed this problem in all later releases of the firewall. The Cyberguard firewall employed by the diagram above is not susceptible to this vulnerability for two reasons:

- The Cyberguard FS model has only one processor, and thus does not utilize SMP.
- The software version is 5.0.

The second vulnerability is only pertinent is certain situations. It involves the permissions of certain system critical files located on the Cyberguard firewall. Below is a list of files and their permissions[14]:

```
drw-rw-rw- /etc/security/firewall/cm
drw-rw-rw- /etc/security/firewall/cm-defaults
-rw-rw-rw- /etc/.device.tab.lock
drwxrwxrw- /etc/conf/pack.d/ktrc
-rw-rw-rw- /etc/iaf/cr1/.kmpipe
-rw-rw-rw- /etc/scsi/dtab.out
-rw-rw-rw- /etc/wsinit.err
-rw-rw-rw- /usr/X/lib/fs/fs-errors
-rwxrwxrwx /usr/X/desktop/Help_Desk
-rw-rw-rw- /var/adm/log/routes
-rw-rw-rw- /var/adm/log/qhap.log
-rw-rw-rw- /var/adm/sa/*
-rw-rw-rw- /var/adm/spellhist
-rw-rw-rw- /var/adm/unixtsa.log
drwxrwxrwx /var/sadm/dist
drwxrwxrwx /var/content/*
-rw-rw-rw- /var/audit/1018_list
-rw-rw-rw- /dev/X/xfont.7000
-rw-rw-rw- /tmp/.scopty
-rw-rw-rw- /opt/QUALha/dev/ifs/*
```

As you can see from the list above, any user on the firewall can edit these files and affect certain aspects of system peformance. However, this potential

vulnerability can easily be averted by simply not allowing general user accounts on the firewall, which should be a requirement if possible in the first place. Cyberguard is an extremely secure firewall and boasts an excellent vulnerability track record.

4.2 Denial of Service (DoS) Attack

A DoS attack is one in which an attacker attempts to prevent legitimate users of a particular service from using that service[7]. One example of a DoS attack is a SYN flood. This type of attack is described in the section below.

- **SYN Flood**

When a client machine attempts to establish a TCP connection with a server machine, a series of messages are sent in a certain sequence between the two[7]. This sequence is often referred to as a TCP three-way handshake. The client starts this process by sending a SYN packet to the server. The server then replies to the client with SYN-ACK packet. The client then completes the connection by sending an ACK packet. To conduct a SYN flood attack a client machine starts sending multiple SYN packets to a given server. The SYN packets that are sent by the client spoof the IP address of another machine that is known not to be able to reply. In turn, the server sends its SYN-ACK packets to the machine that will not reply. This means that the server will never receive any ACK packets, and thus no connections will be established. The situation in which a server is waiting to receive the final ACK from a client is commonly called a half open connection. As the SYN flood attack progresses and more SYN packets are sent to the server, the data structure holding all of the half open connections will eventually become full. At this point, the server will no longer be able to accept any new incoming connection requests. There is almost always a timeout associated with half open connections, but it is usually so long that it cannot keep up with the amount of incoming SYN packets, especially if there is more than one attacking host sending them. An attack such as this, in which multiple attacking hosts are involved, is most commonly called a distributed denial of service (DDoS) attack.

I am going to perform a distributed TCP/SYN flood attack on the firewall above using 50 compromised cable modem/DSL systems. The tool that I have selected for the attack is Tribal Flood Network 2000 (TFN2K). TFN2K is based on a master-agent architecture. Each of my 50 compromised systems is running the TFN2K daemon agent, and I have control over them via a master machine. The agents can perform the following attacks[5]:

- TCP/SYN flood
- UDP flood
- ICMP/PING flood
- SMURF attack flood (BROADCAST PING)

For my attack, I instruct the agents to attack the external interface of the firewall above using the TCP/SYN flood option. Judging from the rule set for the firewall above, the attack should be extremely successful. It should deny the following services:

- DNS (53/tcp) to firewall external interface.
- Web access (80/tcp) to the public web server.
- SSH access (22/tcp) to the public ftp server.
- Web SSL access (443/tcp) to the public web server.
- Passport One access (3443/tcp).

- **Countermeasures**

Cyberguard offers a TCP SYN Flood Defense solution that can be enabled for any rule on the firewall. It basically allows the firewall administrator to modify the timeout period for half open connections. I believe the default timeout set by the Cyberguard software is 90 seconds. I suggest enabling the SYN flood defense for each of the services above, using a 10 second timeout period. The size of the connection queue should also be increased as much as possible without affecting other processes on the firewall. These two countermeasures should greatly increase the firewall's resistance to a DoS attack. However, there is no way to be totally impervious to a DoS attack. Given enough attacking hosts and the right amount of bandwidth, a DoS attack can always succeed.

4.3 Attack Against an Internal System

I have decided that the most vulnerable internal machine in the network above is the public ftp server. Based upon the rule set for the firewall, two groups are allowed to ftp to this server over ssh: suppliers and regular customers. Other than requiring an IP address, GIAC has no real stipulations to who can become a regular customer. The rule set allows regular customers to ftp over ssh, which nullifies the use of the FTP application proxy offered by Cyberguard. Thus the firewall has no protocol knowledge of the ftp traffic tunneling through ssh. Any regular customer is basically free to ftp any type of file that is desired to the public ftp server. As stated in the practical, virus scanning is an optional feature that is not necessarily implemented. This trust given to the regular customer group makes the public ftp server extremely vulnerable. There are a number of viruses in the wild that can attach themselves to files. A regular customer's machine could easily become infected with a virus given that their network is not nearly as secure as GIAC's. The regular customer could in turn ftp the infected file to GIAC's ftp server. GIAC employees are constantly transferring files to and from the public ftp server. Without virus scanning employed, that virus could easily infect GIAC's entire network.

- **Countermeasures**

Rather than using ssh, GIAC could use a VPN connection. GIAC already has a host-to-gateway channel defined for use by remote employees. It would be extremely easy to set up a Passport One profile for both regular customers and suppliers. The use of the Passport One mechanism would provide the following benefits:

- Allow remote employees, supplier, and regular customers to use the same VPN connection.
- Allow different packet filtering rules to be applied for each group.
- Enable the use of the FTP application proxy.
- Restrict FTP operations available to each group.

By taking this approach, GIAC would still maintain all of the benefits they desired of ssh, and they would gain all of the benefits listed above. The only downside to this approach would be that each group would be required to have Cyberguard's VPN client software.

5. Resources

1. Cyberguard Firewall Manual - Configuring the Cyberguard Firewall. http://www.bluesky.com.au/Products/CyberGuard/Documentation/v5.0/cg50cfg.pdf

2. Cyberguard Firewall Manual - Administering the Cyberguard Firewall. http://www.bluesky.com.au/Products/CyberGuard/Documentation/v5.0/cg50adm.pdf

3. Cyberguard Firewall Manual - Configuring SmartProxies for the Cyberguard Firewall. http://www.bluesky.com.au/Products/CyberGuard/Documentation/v5.0/cg50prox.pdf

4. YASSP – Yet Another Solaris Security Package. Jean Chouanard. http://www.yassp.org/

5. TFN2K – An Analysis. Jason Barlow and Woody Thrower. Axent Security Team http://packetstormsecurity.nl/distributed/TFN2k_Analysis.htm

6. Denial of Service Attacks. CERT Coordination Center. Carnegie Mellon http://www.cert.org/tech_tips/denial_of_service.html#1

7. CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks CERT Coordination Center. Carnegie Mellon http://www.cert.org/advisories/CA-1996-21.html

8. NSA Router Security Configuration Guide. http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

9. Introduction to IPSEC. Brad Marshall. http://staff.pisoftware.com/bmarshal/publications/ipsec/introipsec.html

10. Cisco 3600 Series — Modular, High-Density Access Routers. Cisco Systems Inc. http://www.cisco.com/univercd/cc/td/doc/pcat/3600.htm

11. Cyberguard FS Data Sheet. Cyberguard Corporation. http://www.cyberguard.com/PDF/datasheet_fs.pdf

12. What is Common Criteria EAL4 Certification and What Can It Mean For You? Cyberguard Corporation. http://www.cyberguard.com/SOLUTIONS/product_eal4.cfm

13. Vulnerability Development mailing list web archive.
http://lists.insecure.org/vuln-dev/2001/Mar/0103.html

14. Cyberguard FW Weak Permissions
http://archives.neohapsis.com/archives/bugtraq/2000-11/0051.html

15. Nessus
http://www.nessus.org/

16. GCFW Practical Assignment. Robert Wildt.
Posted at: http://www.giac.org/GCFW.php

17. GCFW Practical Assignment. Emily Gladstone.
Posted at: http://www.giac.org/GCFW.php

18. GCFW Practical Assignment. Steve Keifling.
Posted at: http://www.giac.org/GCFW.php

6. Appendix A – Certificate Generation Script

```
#!/bin/ksh

#
# pp1-makecert
#
# creates a self-signed cert for https authentication in Passport-1
#
# usage: pp1-makecert [-n nodename] [-d domainname]
# nodename.domainname is the hostname of the management interface
#

DEBUG=0

if [ $DEBUG -eq 1 ]
then
  typeset -ft usage
  PS4='$LINENO: '
  set -o xtrace
  exec 1>>/var/tmp/pp1-makecert.log 2>&1
  date
  echo $*
fi

usage() {

   print 'usage: pp1-makecert -n nodename -d domainname'
   print 'nodename.domainname is the hostname of the firewall'
}


typeset NEWNODE
typeset NEWDOM

arg=$*
while getopts ':d:n:?' arg
do
    case $arg in
      n) NEWNODE=$OPTARG;;
      d) NEWDOM=$OPTARG;;
      \?) usage
          exit 1;;
    esac
done

FQDN=$NEWNODE.$NEWDOM

if [ $FQDN = . ]
then
      usage
      print "No old FQDN: must use -n and -d"
      exit 1

    NEWDOM=${FQDN#*.}
    NEWNODE=${FQDN%%.*}
```

```
    if [ $NEWNODE = $NEWDOM ]
    then
      # there was no ".", let it pass
      NEWDOM=
    fi
elif [ $FQDN = "$NEWNODE". ] || [ $FQDN = ."$NEWDOM" ]
then
    usage
    print "Must use both -n and -d, or neither"
    exit 1
fi


if [ $DEBUG -ne 1 ]
then
    exec 1>/var/tmp/pp1-makecert.log 2>&1
fi

    typeset MINICADIR=/opt/cyberguard/minica
    typeset KEYFILE=newkey.pem
    typeset CERTFILE=newcert.pem
    typeset KEYDIR=/etc/security/firewall/keys
    typeset CERTDIR=/etc/security/firewall
    typeset KEYDEST=privkey.pem
    typeset CERTDEST=cgfw-cert.pem

      # make the bogus cert
      cd $MINICADIR
      rm CA/index.txt
      touch CA/index.txt
      cat > CA/serial <<!
01
!
      rm CA/newcerts/* >/dev/null 2>&1
      ./csr $FQDN
      [ $? -eq 0 ] || ( print "Can't request certificate for $FQDN" ;
exit 2)
      ./sign
      [ $? -eq 0 ] || ( print "Can't sign certificate for $FQDN" ; exit
3)
      # install it in the certs/keys dirs
      OLDUMASK=$(umask)
      umask 0377
      mv $CERTFILE $CERTDIR/$CERTDEST
      mv $KEYFILE $KEYDIR/$KEYDEST
      umask $OLDUMASK
```