Global Information Assurance Certification Paper

GCFW Practical
Version 1.7

Mike Bell

Table of Contents

List of Figures

List of Tables

Abstract

This paper is being submitted for review by Sans Institute as part of the qualifications for the GCFW certification. There are four main parts to this submission:

1. Assignment 1 - Security Architecture (15 points). Defines the security architecture for GIAC Enterprises.
2. Assignment 2 – Security Policy and Tutorial (35 points). Details of the proposed security architecture defined in 1 above.
3. Assignment 3 – Verify the Firewall Policy (25 points). Audit the policy developed in 1 and 2 above.
4. Assignment 4 – Design Under Fire (25 points). Propose attacks which could be carried out on previously completed practicals.

I. GIAC Enterprises Company Overview

GIAC Enterprises is a small but quickly growing business specializing in the retail operations of fortune cookie quotes. Established in 1995 as a small one person organization, GIAC has quickly grown to over sixty employees and looks to add up to ten more employees to the sales force before the end of 2002. The vast majority of these employees live within driving distance of GIAC Enterprises, located in Boca Raton, Florida, but four of these employees do work from out of their homes located in various parts of the continental United States. In addition, twenty-six of the employees in sales spend an average of twenty weeks each year traveling.

The Company has a market capital of just over $18,000,000, with revenue of $3,400,000. Due to analysis done by the companies accounting and marketing departments, GIAC Enterprises expects this number to double within the next four years. Besides a few outstanding short term loans, most of the revenue is available to be allocated back to the business for future growth.

GIAC currently has approximately 11,000 customers that purchase fortune cookie quotes from them. The GIAC customer base climbed dramatically in the few short years that the company has been extant, and continues to grow by roughly 15% yearly. These customers currently make purchases using mail-in forms and fax order forms on an as needed basis, and provide GIAC almost 65% of the total yearly revenue.

In addition to their customers, GIAC has sixty-seven partners which purchase quotes from GIAC in order to translate and resell them. Of these partners, only eleven are based in the continental United States, the others being based in Tokyo, Singapore, Norway, Belgium, Spain, and Hong Kong. Presently, the quotes are offloaded to tape and shipped to each partner company on a monthly basis. GIAC's partners provide just over 35% of the total yearly revenue.

The quotes are supplied to GIAC by four publishing companies who hire writers to author them. The quotes are sent to GIAC from the publishers on a weekly basis via 4mm tape. The tape is then loaded by GIAC employees to the quote database. Publishers are paid on the basis of the number of quotes supplied to GIAC.

GIAC wishes to streamline the entire operations of purchasing, distribution, and sales by utilizing the Internet. Although a web site is available for most of these

operations, bandwidth issues and stability of the communication link has hindered progress. The DSL provider has been contacted on these issues, but as of yet has been unable to provide satisfactory service.

The company is also concerned with Internet security issues, and proposes that a full five percent of the yearly revenue ($170,000) be allocated to developing a secure Internet infrastructure in which to continue operations. The requirements for this infrastructure are enumerated below.

GIAC Internet Infrastructure Requirements

The IS Director of GIAC Enterprises, Mr. Smith, after meeting with the board of directors and surveying the department heads, has proposed the following set of minimum requirements as a business solution.

- Customers must have the ability to browse and purchase quotes from the companies web site.
- Suppliers must have the ability to supply new quotes to GIAC Enterprises remotely via the Internet.
- Partners must have the ability to access and download the GIAC Enterprise quotes database.
- GIAC employees must have Internet access for a limited number of services. In addition, they will need access to the Oracle database server.
- GIAC traveling salesmen and GIAC remote employees must have access into the companies intranet based servers.
- All transactions involving e-commerce or movement of proprietary information must use secure transfer methods.

To meet these requirements, Low Country Security proposes the following infrastructure / architecture be implemented.

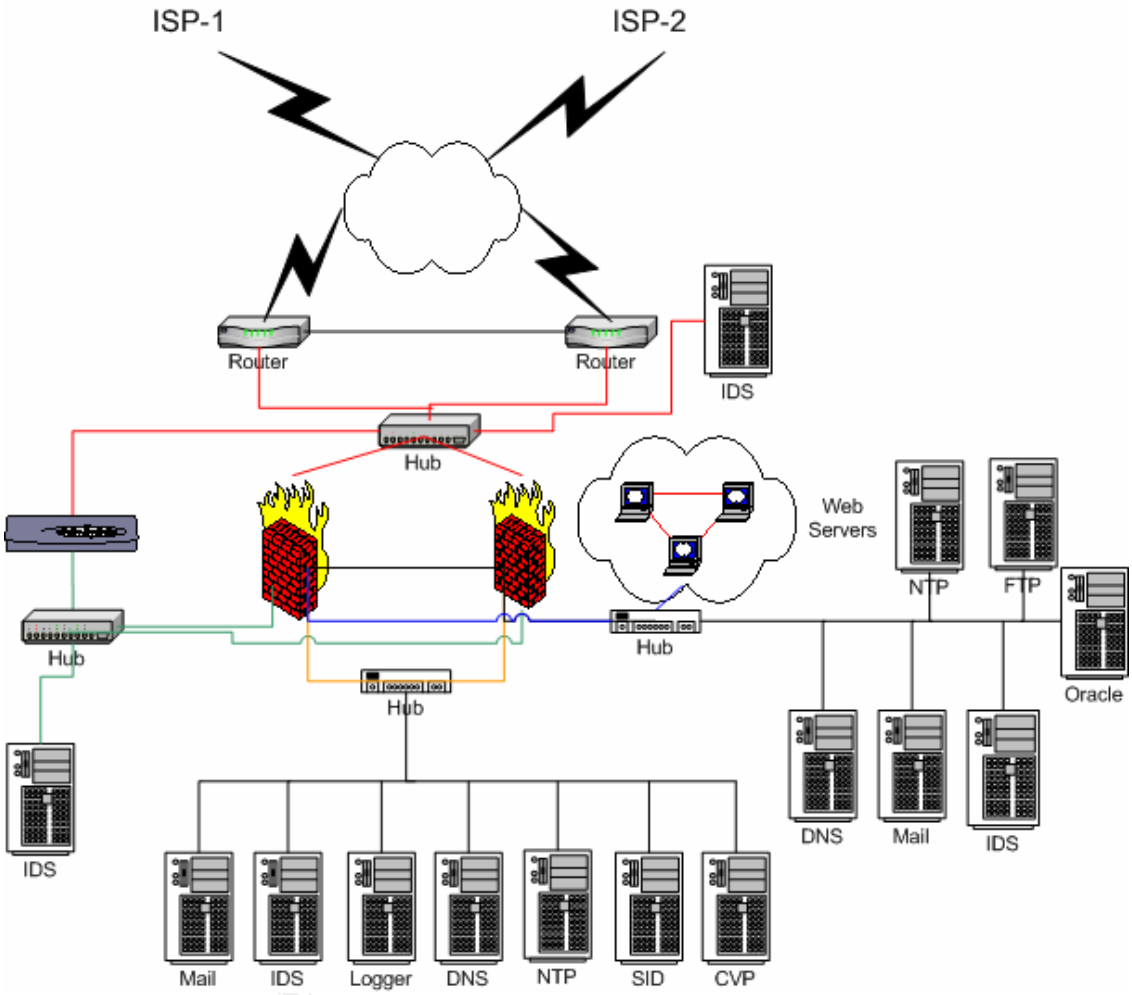


Figure 1-1

The above graphic depicts the GIAC Enterprises network configuration. The Checkpoint firewalls are running in High Availability mode. IDS and logging systems, NTP servers, mail servers and DNS servers are running iptables with only needed services available.

System	Interface	Address	Netmask	NAT Address	NAT Netmask
GIAC_Border_Router		85.10.12.65	255.255.255.224		
GIAC Checkpoint FW Complex	hme0	85.10.12.66	255.255.255.224		
GIAC Checkpoint FW Complex	hme1	172.17.0.1	255.255.0.0		
GIAC Checkpoint FW Complex	hme2	172.18.0.1	255.255.0.0		
GIAC Checkpoint FW Complex	hme3	172.19.0.2	255.255.0.0		
GIAC Checkpoint FW Module-1	hme4	172.20.0.2	255.255.0.0		
GIAC Checkpoint FW Module-2	hme4	172.20.0.3	255.255.0.0		
GIAC Checkpoint FW Mgmt.	hme0	172.20.0.1	255.255.0.0		
GIAC Cisco 3015 Concentrator	Ethernet 1	172.19.0.1	255.255.0.0		
GIAC Cisco 3015 Concentrator	Ethernet 2	85.10.12.67	255.255.255.224		
GIAC SecureID Auth. Server	hme0	172.17.0.2	255.255.0.0		
GIAC Intranet Email Server	eth0	172.17.0.3	255.255.0.0		
GIAC Intranet NTP server	eth0	172.17.0.4	255.255.0.0		
GIAC Intranet Syslog	eth0	172.17.0.5	255.255.0.0	85.10.12.70	
GIAC Intranet DNS server	eth0	172.17.0.6	255.255.0.0		
GIAC DMZ Web server	Ethernet 1	172.18.0.2	255.255.0.0	85.10.12.68	255.255.255.224
GIAC DMZ DNS Server	eth0	172.18.0.3	255.255.0.0		
GIAC DMZ NTP Server	eth0	172.18.0.4	255.255.0.0		
GIAC DMZ Oracle Server	Ethernet 1	172.18.0.5	255.255.0.0		
GIAC DMZ FTP Server	eth0	172.18.0.6	255.255.0.0		
GIAC External IDS	eth0	0.0.0.0	255.255.255.255		
GIAC External IDS	eth1	172.17.0.8	255.255.0.0		
GIAC DMZ IDS	eth0	0.0.0.0	255.255.255.255		
GIAC DMZ IDS	eth1	172.17.0.9	255.255.0.0		
GIAC Internal IDS	eth0	172.17.0.10	255.255.255.255		
GIAC VPN IDS	eth0	0.0.0.0	255.255.255.255		
GIAC VPN IDS	eth1	172.17.0.11	255.255.0.0		
GIAC DMZ Email Server	eth0	172.18.0.7	255.255.0.0	85.10.12.69	255.255.255.224
GIAC Internal Network		172.17.0.0	255.255.0.0	85.10.12.66	255.255.255.224

Table 1.1

Border Router

Purpose: To route permitted traffic from the Internet destined to GIAC's internal network and DMZ, and traffic from the DMZ and internal network out the Internet. It will also act as the first layer of defense by its ability to filter traffic based on source address, destination address, destination port, ICMP type, the transport used, and TCP flag settings.

The exterior routers connecting GIAC Enterprises to the Internet will be a pair of Cisco 3660 routers. Cisco, with almost 85% of the world router market was chosen because of its reliability, flexibility, and commitment to security. http://www.siliconvalley.com/mld/siliconvalley/business/companies/cisco/2672314.htm

Because we will utilize two ISPs for redundancy, these routers will employ BGP protocols. As BGP is memory intensive due to the routing table sizes, Cisco recommends at least 128 MB of memory be installed on routers using this protocol. The Cisco 3660 router supports up to 256 MB of memory, thus allowing ample room for growth. (See section Border Router Hardening for details on the router hardening process).

Key benefits / features of the Cisco 3660 routers include:

- Numerous authentication protocols including RADIUS and TACACS+
- Supports DES / 3DES encryption algorithms
- numerous Network Interfaces provides increased flexibility
- Redundant power supplies allow higher reliability

Firewall

Purpose: The firewall will be the primary point of defense of networks / subnets within the GIAC complex. The placement will be just inside of the border routers. Although the border routers will provide some degree of filtering, the firewall rule sets will be somewhat more detailed. In addition, the firewalls being implemented will maintain state ensuring that conversations will only be initiated from the hosts / networks intended to start such connections (the Cisco routers can maintain some degree of state, but at a performance hit). Although UDP is stateless, replies to UDP requests must be made within the pre-determined timeout period.

The firewall chosen for this implementation is a pair of Checkpoint Firewall-1 / VPN-1 modules utilizing Checkpoint's High Availability solution. This solution will require the installation of three Sun Sparc Ultra 10s. Two of the Ultra 10s will run the Firewall-1/VPN-1 modules acting as the gateway for Internet traffic. The third box will run the Checkpoint Management module. Because the GIAC administrator has experience with Checkpoint Firewall-1/VPN-1 version 4.1, this will be the version implemented with the highest service pack available at installation time (presently SP6 with the SP6-OpenSSL Hotfix). (See Firewall Configuration for details).

Key benefits / features of Checkpoint Firewall-1 / VPN-1

- Stateful Inspection firewall
- Simple Enterprise wide policy management

- Works with OPSEC partner solutions for content security
- Numerous authentication methods available
- High Availability options available

VPN Concentrator
Purpose: To provide a secure tunnel, between a client and this gateway, or from LAN-TO-LAN, through the Internet. Multiple encryption schemes can be used to provide the degree of security necessary for a given transmission. A VPN concentrator was included in the network to reduce the load on the firewall, and to provide an alternate means of connectivity if needed.

Placement of the concentrator will be inside of the border router. An interface will be installed on the Checkpoint firewalls to allow traffic forwarded through the VPN to pass through the firewall. This interface on the firewall will only deal with traffic destined to and from the VPN concentrator.

The 3015 VPN Concentrator will allow secure access to servers in the intranet and DMZ. The concentrator will be used for employee remote access as well as GIAC's partner's and supplier's access. Because the number of simultaneous connections will not approach 100 in the foreseeable future, the 3015 should provide more than enough capacity. However, if the access requirements change, requiring more than 100 connections, the customer may upgrade the 3015 to the 3030, 3060, and 3080 which handle 1500, 5000, and 10000 users respectively.

Intrusion Detection
Purpose: IDS systems provide an alert mechanism for suspicious traffic on the network. Additionally these systems will log all packets into and out of the network using tcpdump. These packets can be used for such things as benchmarking traffic patterns, trouble-shooting, and analyzing alerts provided by the IDS software. These systems can also be used to reset connections if malicious activity is detected, however because this is not foolproof, and because it may be used to deny services, this is not recommended.

Intrusion Detection Sensors will be placed on critical traffic paths into and out of the GIAC Enterprises network. The IDS will run on a fully patched Redhat Linux 7.3 system. The proposed IDS for this network is Snort, (www.snort.org), an open source based IDS. These IDS systems will be hardened, firewalled, and will utilize Tripwire for file integrity. Because the integrity of these systems is critical, they will implement SSH for secure communications whenever these systems are accessed using a method other than via direct console attachment (including from within the internal network). (See the section on Intrusion

Detection Setup Details for details).

Logging

Purpose: To provide a platform to improve the integrity and security, and to enable easier correlation, of log entries from critical infrastructure systems. In addition this system will provide email and pager alerts for log entries deemed to be of a critical nature.

The syslog server will be placed on the internal interface of the Firewall. The server will run on a fully patched Redhat Linux 7.3 system. The server will have all unneeded services removed and, additionally, run iptables. Iptables will be setup to accept only the minimum of services needed on all chains (INPUT, OUTPUT, and FORWARD). As above, the system will be hardened, firewalled, and utilize Tripwire and SSH. As an added measure of integrity, the logs will be written to a writable CD/ROM. (See section on Syslog Hardening Details for details).

Protocol / Service recommendations

Requirement 1 - Customers ability to browse and purchase quotes. With the prevalence of web applications today, customers are comfortable with the usage of browsers for the access of information. Therefore, standard HTTP protocols will be used for all publicly accessible documents. Access which requires the exchange of confidential information, such as credit card numbers, or other proprietary information, will use HTTPS protocols.

Requirement 2 - Suppliers ability to supply new quotes. Access will be allowed to the companies Oracle database via the Cisco 3015 VPN concentrator. Because the security of the publishers network can not be assessed, we will not use LAN-TO-LAN implementation, but will instead use remote access via the Cisco VPN client software to establish connectivity to our Oracle server. The concentrator will be configured to allow access only to the Oracle server via TCP port 1521 for these users.

Requirement 3 - Partners ability to download database. Because many of the partners have limited or non-compatible database infrastructures, the needed records will be exported to a CSV file. This CSV file will then be retrieved by the partners on a weekly basis. The protocol used for this will be FTP.

Requirement 4 - GIAC Employee Internet access. Upon further investigation of this requirement, it was determined that only a very limited number of services

are required. These services include HTTP, HTTPS, and FTP. Services for email will be handled by the Intranet email server. DNS will be served internally via the Intranet DNS server. This access will be implemented through the Checkpoint firewalls.
Access to the companies Oracle database server will be implemented through Checkpoint firewall via TCP port 1521.

Requirement 5 - Traveling / Remote employees access to internal (intranet) servers. These employees require access to several applications / servers within the GIAC internal network. In addition, because some of the information accessed may be confidential in nature, secure communications must be established. LCS proposes using the Cisco 3015 VPN concentrator to fulfill this requirement. The client machines will be configured with the Cisco VPN client. Application protocol access requirements include telnet, ftp, smtp, and pop-3 and Oracle services.

DNS, SMTP and NTP servers
These systems will also be running fully patched Redhat 7.3 systems utilizing iptables with only needed services accessible. In addition, Tripwire and SSH will be utilized for integrity and secure access. In order to keep the length of this proposal practical, the setup of these systems will not be shown.

II. Internet Infrastructure / Architecture Proposal from Low Country Security (LCS)

Border Router Hardening

The Cisco 3660 will run the latest version of IOS, currently Release 12.2 with all relevant security patches installed. Configuration changes will be implemented on the router which will mitigate exposure while maintaining the needed functionality. Access Control Lists will be employed to reduce opportunities to exploit vulnerabilities by persons attempting to penetrate defensive perimeters.

To reduce probability of DOS (Denial of Service) exploits services such as echo and chargen will be disabled. These DOS attacks can be used against GIAC, or GIAC's router may be used in a DOS attack (initiated via third party using spoofing techniques) of another company. This will be done for both the TCP and UDP ports (well known ports for these services are 7 for echo, 9 for discard, and 19 for chargen). The disabling of these services requires the following commands be entered via global configuration mode:

```
no service tcp-small-servers
no service udp-small-servers
```

SNMP is a service which can be used for both monitoring and configuration of networked devices. It has, however, been proven to have a number of security weaknesses and vulnerabilities. cve.mitre.org lists 52 entries which reference snmp (as of June 18, 2002). Because of problems associated with snmp, including buffer overflows, DOS attacks, and other format vulnerabilities, and because snmp will not be utilized for management of the routers, snmp will be disabled on the border routers. The command to do this, entered via global configuration mode is:

```
no snmp
```

The finger protocol can be used to enumerate information regarding logged on sessions, giving an attacker information which could be used in follow-up attempts. The finger protocol can be disabled on the Cisco 3660 with the following command from global configuration mode:

```
no ip finger
```

Directed broadcasts allow sites to be used as DoS amplification systems. These

should be disabled on each interface on the system.

```
no ip directed-broadcasts
```

Cisco CDP protocols are layer 2 protocols which advertise information about Cisco products. Since it is layer 2 based, it will not traverse routers, however it will be disabled due to the possibility of local attacks and sniffers. To disable the cdp protocol, enter the following command from global configuration mode:

```
no cdp running
```

For increased integrity of logged information and to enable easier correlation of logged entries from multiple network nodes, logging on the Cisco routers will be configured to use the secure syslog server. As extraneous log entries can easily be stripped using scripting languages such as perl, or with the use of grep, logging will be done at the informational level, thereby giving greater levels of detail if needed for analysis. The commands to enable logging are as follows:

```
logging trap informational
logging 85.10.12.70
```

To mitigate the attackers ability to define routes which could be used to access hosts on the internal and DMZ network, source routing will be disabled on all routing devices. This is recommended by the CERT Coordination Center, (http://www.cert.org/security-improvement/practices/p075.html). The commands to disable source routing on the Cisco 3660 is as follows:

```
no ip source-route
```

Enable passwords give administrator access to the Cisco 3660s. There are two methods to enter the enable password into the Cisco 3660 - enable password, *and* enable secret, *which uses a stronger encryption method (MD5 password hashing) to secure the password. We will use the enable secret to enter the password as such:*

```
enable secret <password>
```

Border Router ACLs

Access Control Lists will be added for both ingress and egress filtering on the

Cisco 3660s.

Deny any ip traffic which does not include a source address.

```
access-list 101 deny ip host 0.0.0.0 any log
```

Deny incoming ip traffic which uses the loop back address as a source address. This address is used for internal communications and should never be encountered as a valid source address from the Internet.

```
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
```

Deny incoming ip traffic using private addresses, defined by rfc 1918, as the source address. The next three lines block private addresses for Class A, Class B, and Class C networks.

```
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
```

Deny incoming multicast traffic (224-239 in first octet)

```
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
```

Deny traffic inbound with a source address of this network.

```
access-list 101 deny ip 85.10.12.64 0.0.0.31 any log
```

Deny inbound icmp echo requests, which may be used to map the network.

```
access-list 101 deny icmp any any echo
```

These are services which may be used to establish connections to devices with-in the border router's perimeter defenses, used to enumerate systems, or be used for other malicious activity. Note that although these services should be blocked by the Firewall, these rules will provide an extra layer of protection in the event that a service becomes available on or through the firewall.

```
access-list 101 deny tcp any any eq 7
access-list 101 deny udp any any eq 7
access-list 101 deny tcp any any eq 9
access-list 101 deny tcp any any eq 11
```

```
access-list 101 deny udp any any eq 11
access-list 101 deny tcp any any eq 13
access-list 101 deny tcp any any eq 19
access-list 101 deny udp any any eq 19
access-list 101 deny tcp any any eq 21
access-list 101 deny tcp any any eq 22
access-list 101 deny tcp any any eq 23
access-list 101 deny tcp any any eq 69
access-list 101 deny tcp any any eq 79
access-list 101 deny tcp any any eq 111
access-list 101 deny tcp any any eq 137
access-list 101 deny tcp any any eq 138
access-list 101 deny tcp any any eq 139
access-list 101 deny tcp any any eq 161
access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 514
access-list 101 deny tcp any any eq 1723
```

Permit all other traffic inbound.

```
access-list 101 permit ip any any
```

Deny icmp time-exceeded messages from leaving the network. Although these may be valid, they are many times used by traceroute to map networks.

```
access-list 102 deny icmp any any time-exceeded
```

Permit all other outbound traffic.

```
access-list 102 permit ip any any
```

To install the access lists enter configuration mode for the specified interface and enter the following commands:

```
ip access-group 101 in
ip access-group 102 in
```

Operating System Hardening

Much of the information contained herein on the hardening of the OS was obtained from The SANS Institute Solaris Security Step by Step.

Configuration of /etc/init.d/inetinit

The following entries should appended to the /etc/init.d/inetinit file.

This tells the system to ignore incoming redirects. Redirects have the potential to cause the firewall to route packets to compromised machines, and can also be used to deny services if the router in which packets are redirected to is configured to drop them. (NOTE: redirects are normally only used if the redirect is originating from the same subnet).

ndd –set /dev/ip ip_ignore_redirect 1

Disable the sending of redirects from the firewall.

ndd –set /dev/ip ip_send_redirects 0

Broadcasts can be used for network mapping, or may also be used to amplify pings for such things as Smurf attacks. The firewall should not accept directed broadcasts.

ndd –set /dev/ip ip_forward_directed_broadcasts 0

Source routing enables a sender to define some or all of a path to a particular destination host. This can be used as "backdoor" pathways into networks, or also to attack private (rfc 1918) networks by specifying the path to the private network. Source routing should be disabled at the router.

ndd –set /dev/ip ip_forward_src_routed 0

If the Solaris detects more than one NIC on the system, it will automatically turn on routing for the system. IP forwarding should be turned off to avoid conditions where the system would act like an unfiltered router when the Checkpoint Firewall policy is not loaded and

running on the Firewall modules. The Checkpoint Firewall software will control IP forwarding, enabling traffic to traverse the system, when the policy is installed.

ndd –set /dev/ip ip_forwarding 0

Remove unneeded services from /etc/services and/or /etc/inetd.conf. *Make sure to remove both the TCP and UDP transport for each of these services, if required. The table below defines the services to be removed from the system.*

Port	Service		Port	Service		Port	Service
7	echo		9	discard		11	systat
13	daytime		15	netstat		19	chargen
20	ftp-data		21	ftp		23	telnet
25	smtp		37	time		42	name
43	whois		53	domain		67	bootps
68	bootpc		69	tftp		77	rje
79	finger		87	link		95	sysdup
101	hostnames		102	iso-tsap		103	x400
104	x400-snd		105	csnet-ns		109	pop-2
111	sunrpc		117	uucp-path		119	nntp
123	ntp		144	NeWS		512	exec
512	biff		513	login		513	who
514	shell		515	printer		530	courier
517	talk		520	route		560	rmonitor
540	uucp		550	new-rwho		750	kerberos
561	monitor		600	pcserver		2049	nfsd
1008	ufsd		1524	ingresslock		110	pop3
4045	lockd		6112	dtspc			

Table 2-1

Remove unneeded services from /etc/rc2.d and /etc/rc3.d

As stated above, services which are not needed should be disabled from the system. Following are the startup scripts which should be disabled, along with the reasons for disabling the services. As a precautionary measure, backups of the directories affected should be done prior to the deletions.

Line Printer services will not be used on the firewall. Because vulnerabilities, such as buffer overflows, have been associated with this daemon (see http://www.kb.cert.org/vuls/id/484011 *), this service*

should be disabled at startup. To disable this daemon, remove S80lp from /etc/rc2.d.

rm /etc/rc2.d/S80lp

Time synchronization is extremely useful for log and event correlation, and should be done on all critical servers and networking and security infrastructure hosts. However, because ntpd (network time protocol daemon) has been associated with vulnerabilities (http://online.securityfocus.com/bid/2540 *) , and because ntpdate can be executed from cron, thereby avoiding the vulnerabilities associated the ntpd server, this server should be disabled. To disable this service, remove /etc/rc2.d/S74xntpd, and add it to crontab.*

rm /etc/rc2.d/S74xntpd

To cron add

0 * * * * /usr/sbin/ntppdate *<ntp server ip address>*

NFS has historically been implicated in a multitude of vulnerabilities. *See (*
http://www.kb.cert.org/vuls/id/18287
http://www.kb.cert.org/vuls/id/635811
http://www.kb.cert.org/vuls/id/161931
) for just a few of the recent vulnerabilities associated with nfs daemons. Because nfs will not be used on this system, the client and server side will be disabled. To disable these services, remove /etc/rc3.d/S15nfs.server *and* /etc/rc2.d/S73nfs.client.

rm /etc/rc3.d/S15nfs.server
rm /etc/rc2.d/S73nfs.client

Automounter is a service which performs nfs mounts dynamically as a file system is accessed, then will unmount the file system after a specified time of inactivity. Because we will not require nfs services, we will also disable automounter. To disable automounter, remove /etc/rc2.d/S74autofs.

rm /etc/rc2.d/S74autofs

A search of the CERT Advisory database (www.cert.org *) for the*

words "sendmail" and "solaris" combined, returned 14 hits within the last year. Because the firewall will not be employed as a sendmail server, and because sendmail can be executed from cron, the sendmail should be disabled. To disable sendmail, remove /etc/rc2.d/S88sendmail and add it to the crontab.

```
rm /etc/rc2.d/S88sendmail
```

To cron add

```
0,15,30,45 * * * * /usr/lib/sendmail –q > /var/adm/sendmail.log 2>&1
```

SNMP is another service which historically has had its share of security related issues. Because the firewall will not be managed via SNMP protocols, and because SNMP will not be used for monitoring the firewall, SNMP should be disabled. To disable SNMP, remove /etc/rc3.d/S76snmpdx.

```
rm /etc/rc3.d/S76snmpdx
```

PPP and uucp services will not be required on the firewall. To disable these, remove /etc/rc2.d/S70uucp and /etc/rc2.d/S47asppp.

```
rm /etc/rc2.d/S70uucp
rm /etc/rc2.d/S47asppp
```

Other various services which should be disabled as they will not be needed are 1) Buttons and Dials support, print client, and Naming Services Caching Daemon services.

```
rm /etc/rc2.d/S89bdconfig
rm /etc/rc2.d/S80spc
rm /etc/rc2.d/S76nscd
```

Security Policy Setup

(1) Properties Setup

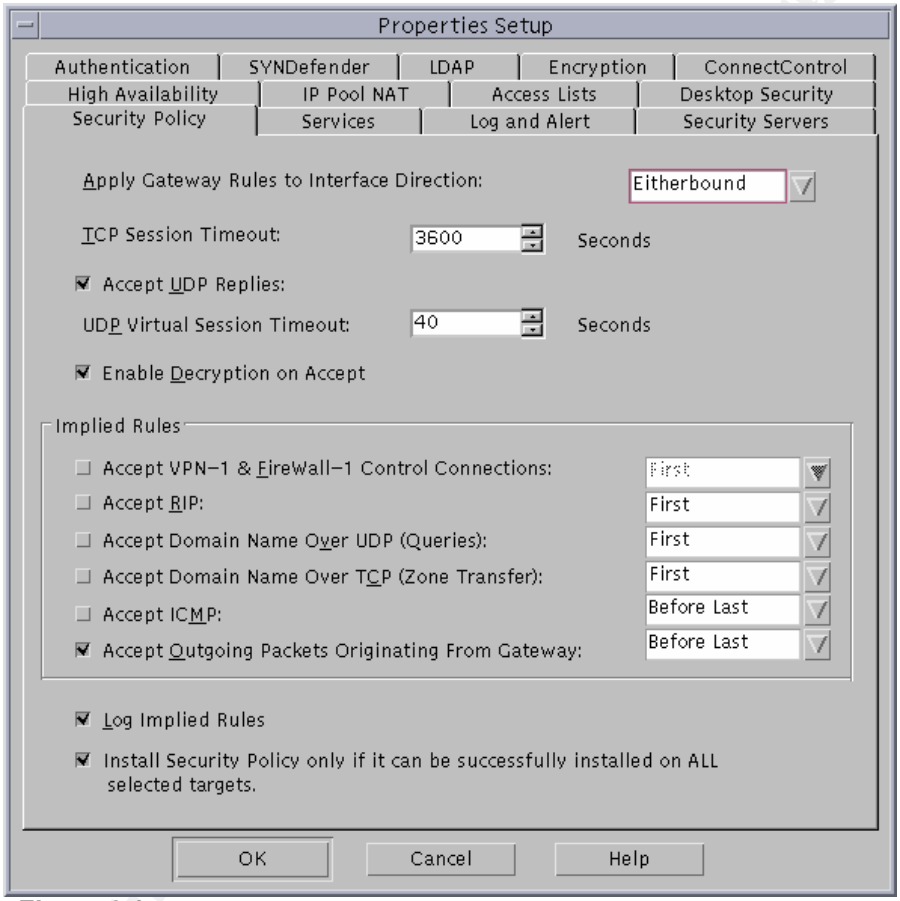


Figure 2.1

Apply Gateway Rules to Interface Direction: - This will be left at the Checkpoint default setting, Eitherbound. This allows the packets to be checked twice, once on the inbound interface and once on the outbound interface.

TCP Session Timeout: - This will be left at the default of 3600 seconds. After this time, inactive TCP sessions will be cleared from the state table.

Accept UDP Replies: - This will be left enabled. UDP packets originating from the internal network and traversing the firewall, such as in the instance of DNS queries, depend upon this to function correctly. As such, the replies will not be blocked, but will be allowed back to the client machine.

UDP Virtual Session Timeout: - This will be left at the default. Any UDP replies which take longer than 40 seconds will be dropped.

Enable Decryption on Accept: - This will be left enabled. This basically states that if a rule is defined that accepts a packet in an unencrypted form, and the packet instead is presented to the firewall in an encrypted form, it will be accepted. In theory, this allows for additional security due to the encryption of the packet while traversing the Internet.

Accept VPN-1 & Firewall-1 Control Connections: - This property will be disabled. Any needed control connections will instead be inserted into the explicitly defined rulebase. This allows for greater control of these connections. By not exposing these rules to the external interface it will also be more difficult to fingerprint the firewall as Checkpoint Firewall-1.

Accept RIP: - As in the Access List panel, we will disable this implied rule and instead use static routing.

Accept Domain Name Over UDP (Queries): - This option was disabled. Explicit rules were added to the rulebase to handle DNS via UDP transport. This allows us to manage the rules from one place without having to jump back to the Properties Setup.

Accept Domain Name Over TCP (Zone Transfer): - This option was disabled. Explicit rules were added to allow DNS over TCP transport outbound only. This allows the use of TCP as the transport protocol when DNS replies exceed the maximum allowable size for UDP (512 bytes). Zone Transfers are not needed in our configuration.

Accept ICMP: - Because other ICMP types can be used for network mapping, covert channels, and other enumerative techniques, they will be dropped.

Accept Outgoing Packets Originating from Gateway: - This option must be checked if the “etherbound” direction for packet inspection is checked, or a rule must be added to allow packets to leave the gateway.

Log Implied rules: - This option was selected to log the implied rules, those rules which are implemented via the properties setup, to the log file. These rules will show as Rule 0 in the logs.

Install Security Policy only if it can be successfully installed on ALL selected targets: - This option will be checked to insure that all firewall modules are

running the same rulebase.

(2) Services Setup

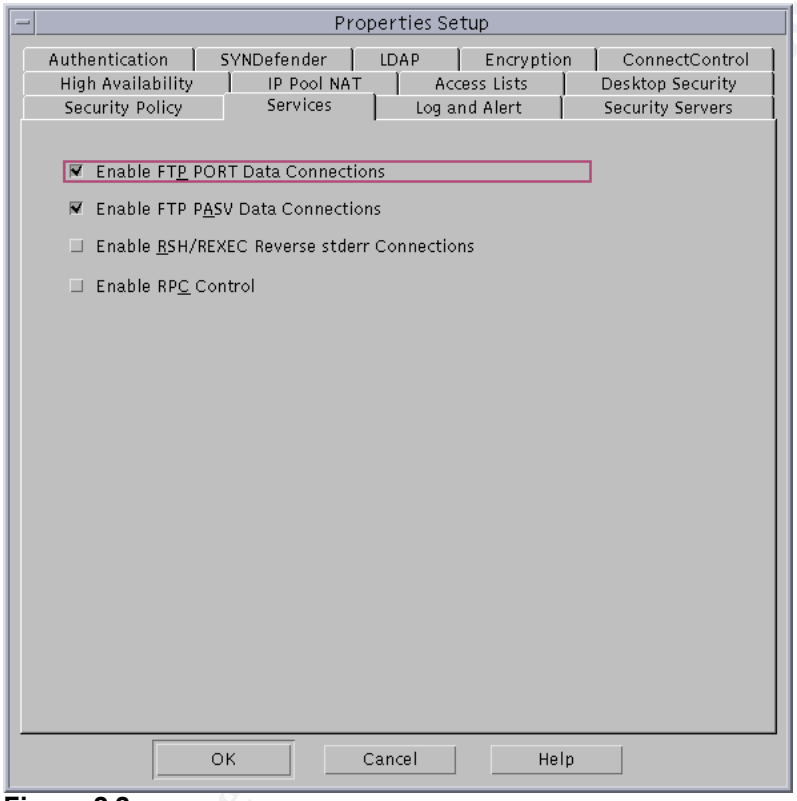


Figure 2.2

Enable FTP Port Data Connections: - This will allow the FTP server to establish a connection with the FTP client via the port that was specified in the PORT command of the FTP control session. This option is required for ACTV mode FTP to function properly.

Enable FTP Passive Data Connections: - This allows the client to establish the connection to the server via the port number specified in the reply from the server in response to the clients PASV command.

Enable RSH/REXEC Reverse stderr Connections: - Because multiple security related issues exist with rsh (i.e., problems with trust relationships), rsh related packets will not be allowed into the company via the Internet, therefor this option will be disabled. Furthermore, LCS recommends that this protocol be removed from all machines where it is not absolutely necessary, and where it cannot be replaced by other protocols (such as ssh).

Enable RPC Control: - RPC related protocols have had a long and distinguished history of security related issues. Because if this, RPC will not be allowed in through the firewall, therefore this option will be disabled.

(3) High Availability Setup

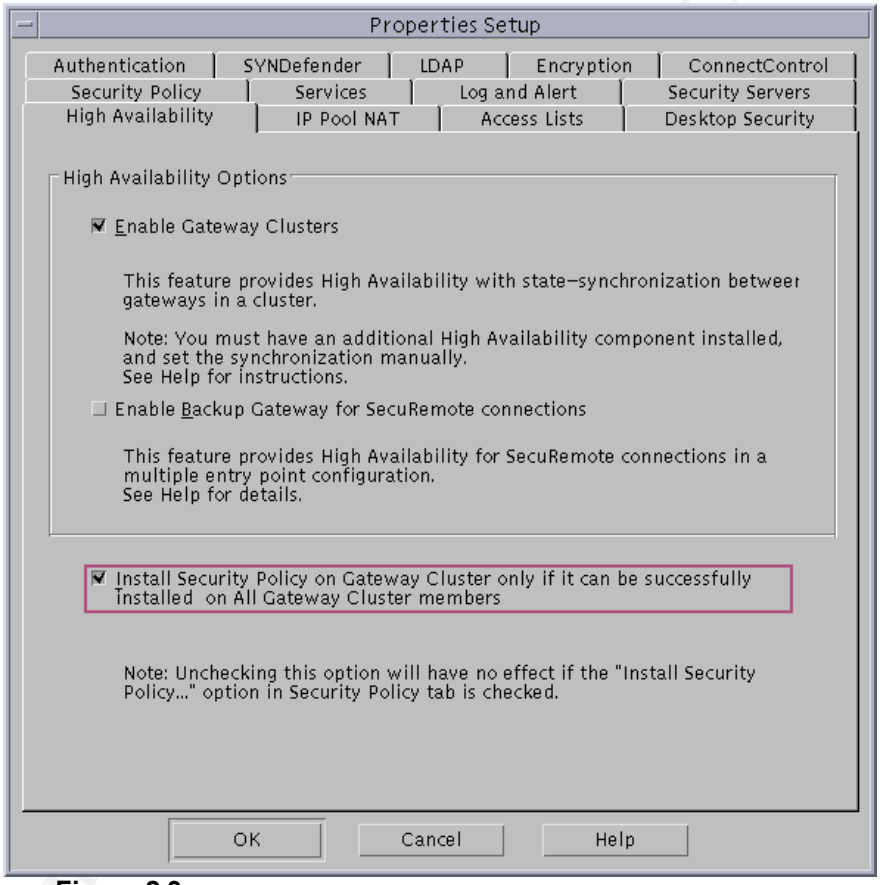


Figure 2.3

Enable Gateway Clusters: - Enabling of this parameter activates the Gateway Cluster as a menu item in the Network Objects window. This parameter must be checked in order to configure High Availability.

Enable Backup Gateway for SecureRemote connections: - We will leave this option unchecked since we will not be accessing the internal networks or DMZ via SecureRemote, but will instead use the Cisco VPN Concentrator for this.

Install Security Policy on Gateway Cluster only if it can be successfully installed on All Gateway Cluster members: - Check this option to ensure that as policy is

pushed, that all gateways are running the same policy. The policy should only load if it can be loaded on all gateways in the cluster. If this option were not checked and the primary gateway should fail, the secondary gateway may be running an older copy of the policy and newer rules would not be implemented.

(4) SYNDefender Setup

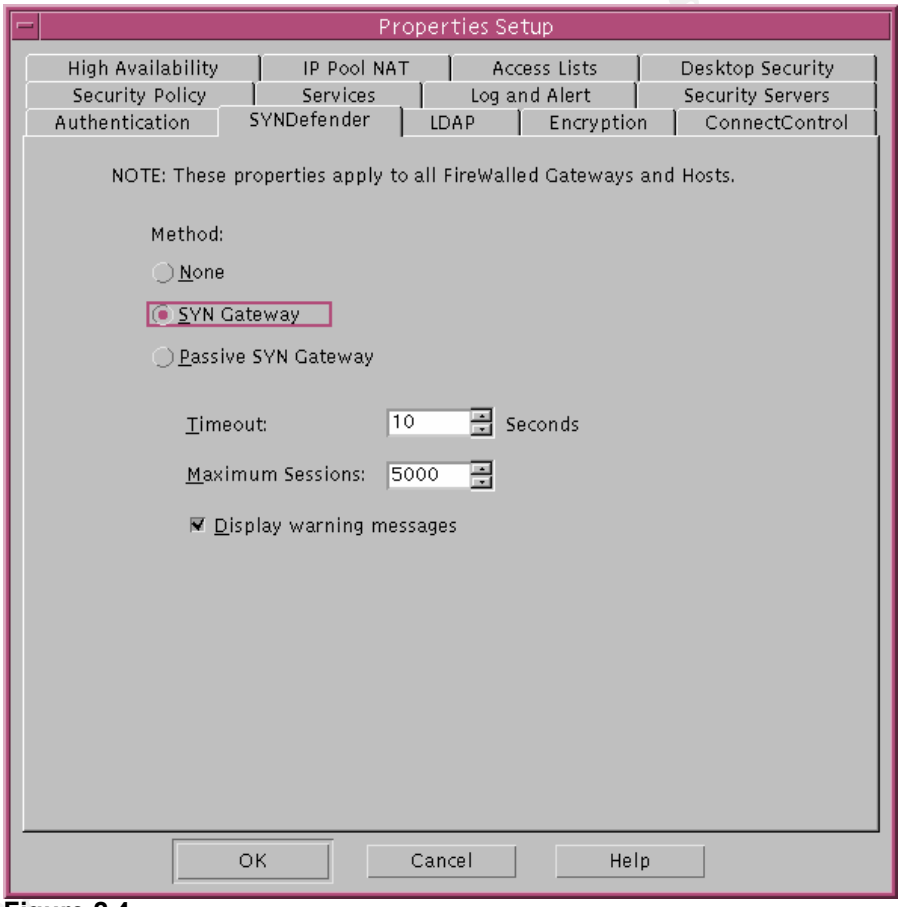


Figure 2.4

Method: - The method for defending against SYN attacks will be SYN Gateway. Using this method, the firewall actually opens the session with the server before receiving the final ACK packet from the client. If this ACK does not come in a specified amount of time, the firewall sends a RST packet to the server to terminate the session.
Timeout: - The amount of time allowed to elapse from the time a SYN is received from a client destined to a server, and the RST is sent to the server to terminate

the connection, if no corresponding ACK is received to the server's (firewall's) SYN/ACK. This is the default setting.

Maximum Sessions: - Specifies the size of the SYNDefender's connection table. This will be set at the default of 5000. SYNDefender will not analyze additional connection attempts if this table is full. Equilibrium of the table would be reached at 500 packets / second (5000 packets / 10 seconds). If we assume Windows based systems with an average SYN packet length of 48 bytes, the table would maintain this equilibrium state at 187.5 Kb/second, assuming no other incoming traffic on the wire.

(500 pps x 48 bytes/packet x 8 bits/byte) / (1024 bits/Kb) = 187.5 Kb/Sec

This is enough to mitigate the attacks of 3 households running on a 56Kbp/sec dialup connection.

(5) Access Lists Setup

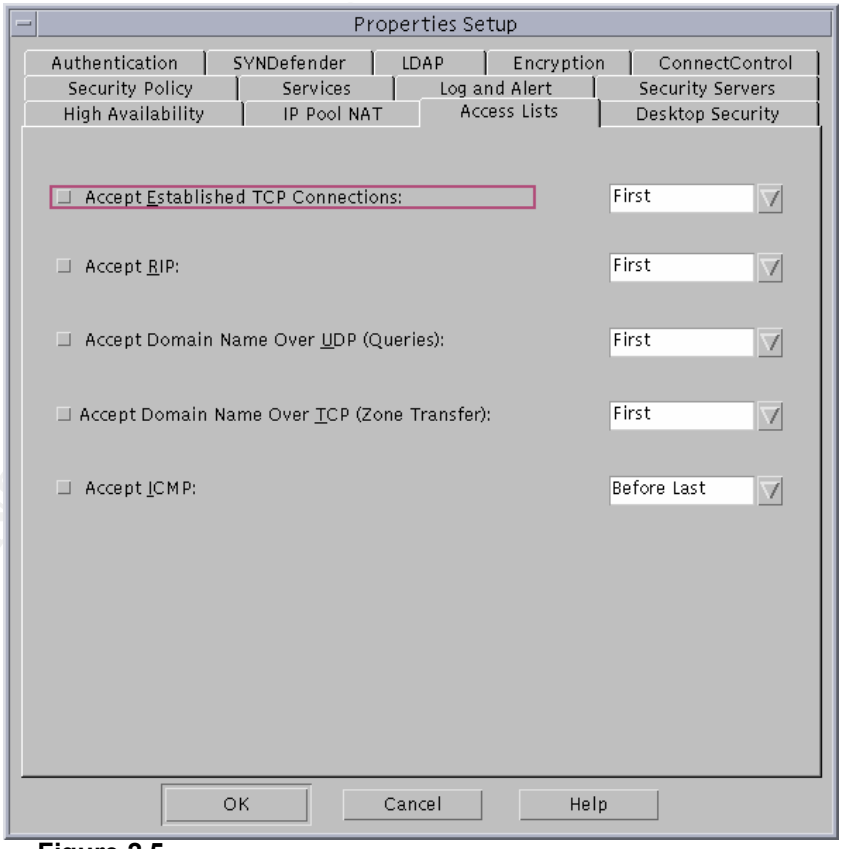


Figure 2.5

Since all router management will be done from the console in order to reduce the number of servers and management applications running on the router, access lists to control the Cisco Routers from the firewall will not be used. Even though we will not be using access lists, all options on the Access Lists window will be disabled as an added measure of caution.

Explicit rules

Ordering of Rules

The ordering of rules is an important aspect to consider when setting up a firewall. Checkpoint like many firewalls assesses its rules using a sequential method. It does not use a best-fit methodology. The rules are checked in the sequence they are entered in the rulebase, and the first rule to match dictates the action the firewall will perform. It is also important to note that this may include the implicit rules specified within Checkpoints Properties Setup.

The importance of this lies in the fact that a packet which may be denied on a later rule may be accepted in an earlier rule. For example, if I am using a server for URL filtering and I setup a rule for this resource as rule number 10, but I have a rule which allows all HTTP traffic as rule number 9, web sites which may have been blocked will be allowed because rule 9 will be encountered first.

A good rule of thumb to follow is to attempt to place more specific rules before more general rules. This type of placement helps to avoid the problems mentioned above where a packet matches on a more general rule, and would have been denied on a more specific rule. Had the specific rule been ordered before the general rule (i.e., the “URL filter” before the “allow all HTTP”) the packet would have been denied.

However, depending upon traffic volumes and types, performance can be improved by ordering the more frequently matched rules first. It is important to ascertain that the reordering of the rules does not produce any unexpected results, and an audit should undertaken to verify this.

There are also two important rules that every firewall should contain. The first rule is a rule that drops all traffic not absolutely necessary which has a destination address of the firewall. This rule should be placed fairly close to the top of the rulebase, after any rules that allow traffic that is needed to the firewalls. The second rule that should be in all firewalls is a rule which drops all traffic not allowed by an earlier rule. This rule should be the last rule in the rulebase and

basically sets the “deny all not explicitly allowed” policy.

Rule Parameters

The parameters (GUI fields) for the Checkpoint rules are as follows. For readability and due to horizontal space limitations, not all fields are shown in the rule illustrations. VPN-1/Firewall-1 Administration Guide was used as a reference for this section.

No. : The sequential rule number (not shown in illustrations).

Source : The source address of the sender represented as a network object. A network object can be a workstation, network, domain, router, switch, integrated firewall, group, logical server, address range, or gateway cluster. It is also possible to add users or groups of users for this field (limits actions available).

Destination : The destination addresses of the receiving party represented as a network object (see network object types above).

Service : The service pertaining to this rule. A service can be of type TCP, UDP, RPC, ICMP, Other, Group, or Port range. It can also be a service with a resource such as those defined for CVP servers.

Action : The action to be performed by the firewall in response to a match to the rule. Actions can be accept, reject, drop, user authentication, client authentication, session authentication, encrypt, and client encryption.

Track : Specifies how logging and alerting are to be handled in response to a match to this rule. Valid entries are no logging (leave field blank), short log, long log, accounting, alert, mail, SNMP trap and user defined.

Installed On : This determines which firewalls controlled by the management station will enforce this particular rule. Note that according to Checkpoint documentation, the entire policy is loaded to the firewall object, but only the rules

specific to that object will be enforced.

Time : Specifies the time ranges for which this rule will be enforced.

Comment : A field for rule related documentation.

Rule Setup

Rule 1.

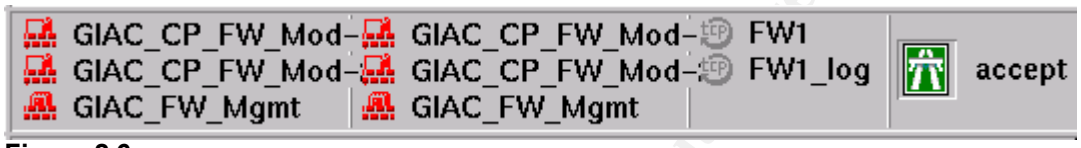


Figure 2.6

Because "Accept VPN-1 & Firewall-1 Control Connections" was disabled in the Security Policy tab of the Properties, this functionality must be explicitly implemented within the rulebase to allow the two gateways participating in the firewall cluster, and the management console, to communicate with one another. This rule allows the firewall modules to send logs to the management module, allows the management module to push the policy to the firewall modules, and allows the firewall modules to see each other for high availability functionality.

Rule 2.

Figure 2.7

This rule instructs the firewall to drop all connections from previous attackers. It is possible to shun entire countries using this rule. Information from previous attackers will be obtained from the firewall logs, and the IDS logs.

Rule 3.

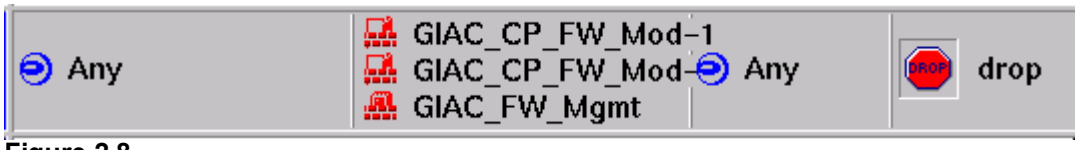


Figure 2.8

Rule 3 allows us to drop any connections destined to our firewall modules. This rule should be placed very close to the top of the firewall rulebase, after any rules allowing connections to the firewall. Rules allowing connections to the firewall should be few, being used only when necessary.
By placing this rule near the top of the rulebase, the chances of access being allowed due to a destination of "any" is greatly reduced.

Rule 4.

Figure 2.9

Rule 4 allows suppliers defined within the group "VPN_Supplier" to access the Oracle database server using TCP port 1521, the standard Oracle Listener port. Note that this port will not be open to the external interface of the firewall, but only via the VPN and internal network interfaces. SecurID authentication takes place on the 3015 concentrator.

Rule 5.

Figure 2.10

Rule 5 allows partners to access the ftp server for quote database downloads. This port will not be open to the external interface, only via the VPN interface, and for some internal users. SecurID authentication takes place on the 3015 concentrator.

Rule 6.

Figure 2.11

This rule allows the IP addresses listed in the group GIAC_Employee to access needed services on the internal network. Note that these users must be entering the firewall from the interface connected to the Cisco 3015 concentrator.

The list of allowed services defined by the GIAC_Services group include the following:

- telnet
- ftp
- smtp
- pop-3

Rule 7.

Figure 2.12

Rule 7 allows GIAC_Employees entering through the VPN to access the Oracle server within the DMZ via port 1521. This port will not be open to the external interface, only via the VPN and Internal interfaces. SecurID authentication takes place on the 3015 concentrator.

Rule 8.

Figure 2.13

Rule 8 allows the internal DNS server to query the DNS server in DMZ using port 53. DNS will attempt to query using UDP as the transport protocol, and should use TCP only for replies that exceed the maximum length allowed for DNS over UDP. The TCP connection initiation (SYN flag) must come from the internal DNS server. The connection can not be initiated from the DMZ DNS, thereby reducing chances of attacks utilizing zone transfers.

Rule 9.

Figure 2.14

Rule 9 allows the internal email server and the DMZ email server to send mail via port 25, the SMTP port. Incoming and Outgoing mail will be scanned for

malware on the DMZ email server.

Rule 10.

Figure 2.15

Rule 10 will allow the 3015 concentrator to act as an agent of the SecurID server to authenticate users connecting to the concentrator. All users must use SecurID to be able to use the GIAC Enterprise VPN.

Rule 11.

Figure 2.16

This rule allows designated NTP servers within the internal network to connect to Internet based NTP servers. Servers, workstations, etc., within the internal network will then connect to the internal NTP servers for time synchronization.

Rule 12.

Figure 2.17

This rule allows designated NTP servers within the DMZ to connect to Internet based NTP servers. Since holes should not be opened from the DMZ where public servers are located to the internal trusted network, the internal NTP servers will not be used to serve time to servers based within DMZ, but these servers will instead be served from Internet based NTP servers. These NTP servers will then serve time to all other devices located in the screened subnet.

Rule 13.

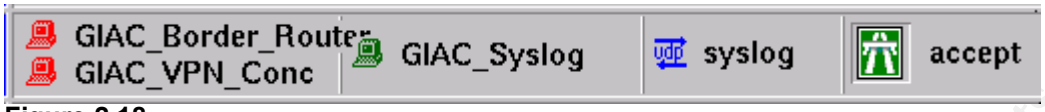


Figure 2.18

This rule allows the border router and VPN Concentrator to log to the syslog server via UDP port 514. Port 514 will be blocked inbound at the border router so this hole can not be easily exploited.

Rule 14

Figure 2.19

This rule allows SMTP access from any source except from GIAC Internal source addresses. This rule must be placed after the rule allowing the GIAC_Intranet_Email and GIAC_DMZ_Email server to communicate (rule 9). This rule will allow email delivery from Internet based email servers to GIAC's mail server in the DMZ.

Rule 15.

Figure 2.20

This allows email to be sent outbound via SMTP from the email server within the DMZ to email servers anywhere other than to email servers in the internal network. This rule must be placed after the rule allowing the GIAC_Intranet_Email and GIAC_DMZ_Email server to communicate (rule 9).

Rule 16

Figure 2.21

Rule 16 allows the internal network user to access the Oracle server located in the DMZ via port 1521.

Rule 17.

Figure 2.22

The Ident protocol, described in rfc 1413, "provides a means to determine the identity of a user of a particular TCP connection" (St. Johns). However, because this protocol can be used as a means of reconnaissance, it will be blocked on the firewall. Because email servers may use this protocol this can be a performance problem as the server must wait for a time-out since the requesting packet is dropped. We will therefore implement a rule, rule 17 in this case, to send a reject upon receiving an ident destined for the DMZ email server to avoid these delays.

Rule 18.

Figure 2.23

This rule allows access to the GIAC web server from any source IP address via port 80 (HTTP) and 443 (HTTPS).

Rule 19.

Figure 2.24

This rule allows users on the internal network to access Internet web servers using port 80 (HTTP) and 443 (HTTPS).

Rule 20.

Figure 2.25

This rule allows the GIAC_FTP_Users group to access FTP servers. To reduce trojans, pirated software, etc., from being retrieved from the net, it is recommended that FTP access be given only to users who show a real need.

These users will be placed in the GIAC_FTP_Users group.

Rule 21.

Figure 2.26

This rule allows the DNS server residing in the DMZ to issue DNS queries to other DNS servers providing that these servers do not reside on the internal network.

Rule 22.

Figure 2.27

Because of the volume of NBT traffic originating from the internal network, this traffic will be blocked and not logged.

Rule 23.

Figure 2.28

This rule will drop and log any remaining traffic. This rule should be employed in all firewalls to enforce the deny unless permitted rule. Although by default Checkpoint drops all packets not permitted via the explicit or implicit rules, it does not log these packets. This rule will allow the rules to be logged.

Installation of the Policy

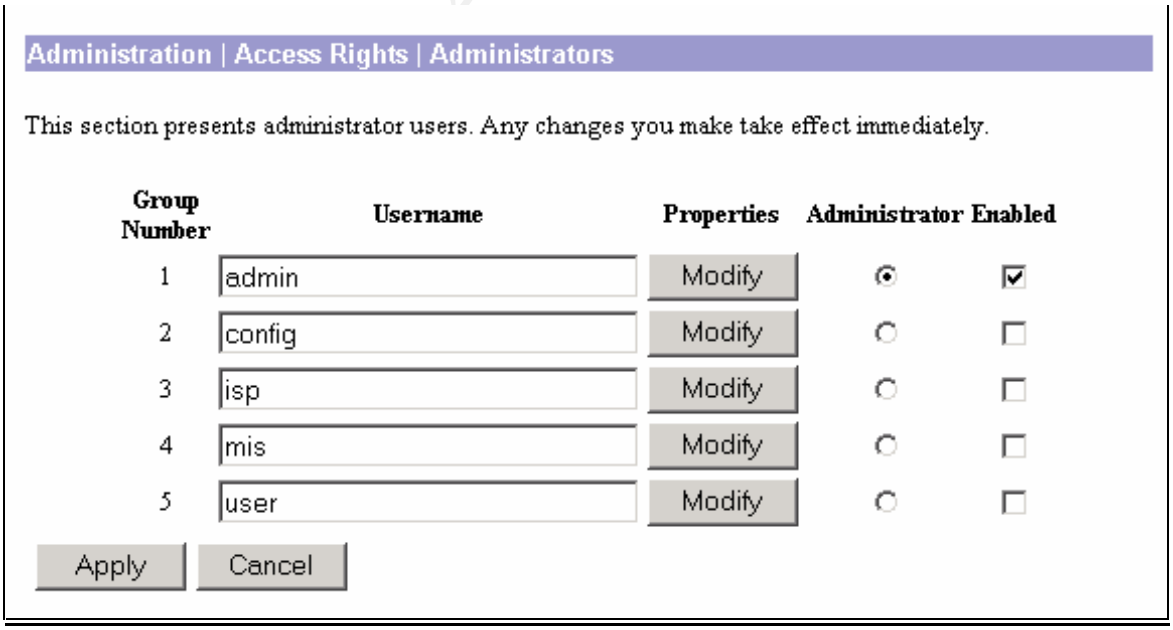
The Policy and Network Address Translation rules should be verified before beginning the installation. The verification can be performed by left clicking on the verify icon in the tool bar.

The policy is then compiled, pushed, and installed on the Firewall-1 modules by left clicking on the Install Icon.

Cisco 3015 Concentrator Setup

(**NOTE**: The device I had access to for the research for this part of the practical was not actually a Cisco 3015 VPN concentrator, but an Altiga concentrator. From talks with my vendor and a Cisco engineer, I understand the hardware and software to be practically identical. Since Altiga was purchased by Cisco in January 2000, I felt that it would be better to use the Cisco brand name for purposes of this practical. If there are any differences between the setup of the Altiga and the Cisco concentrators, I ask that this be taken into consideration.)

Figure 2.29
Administration



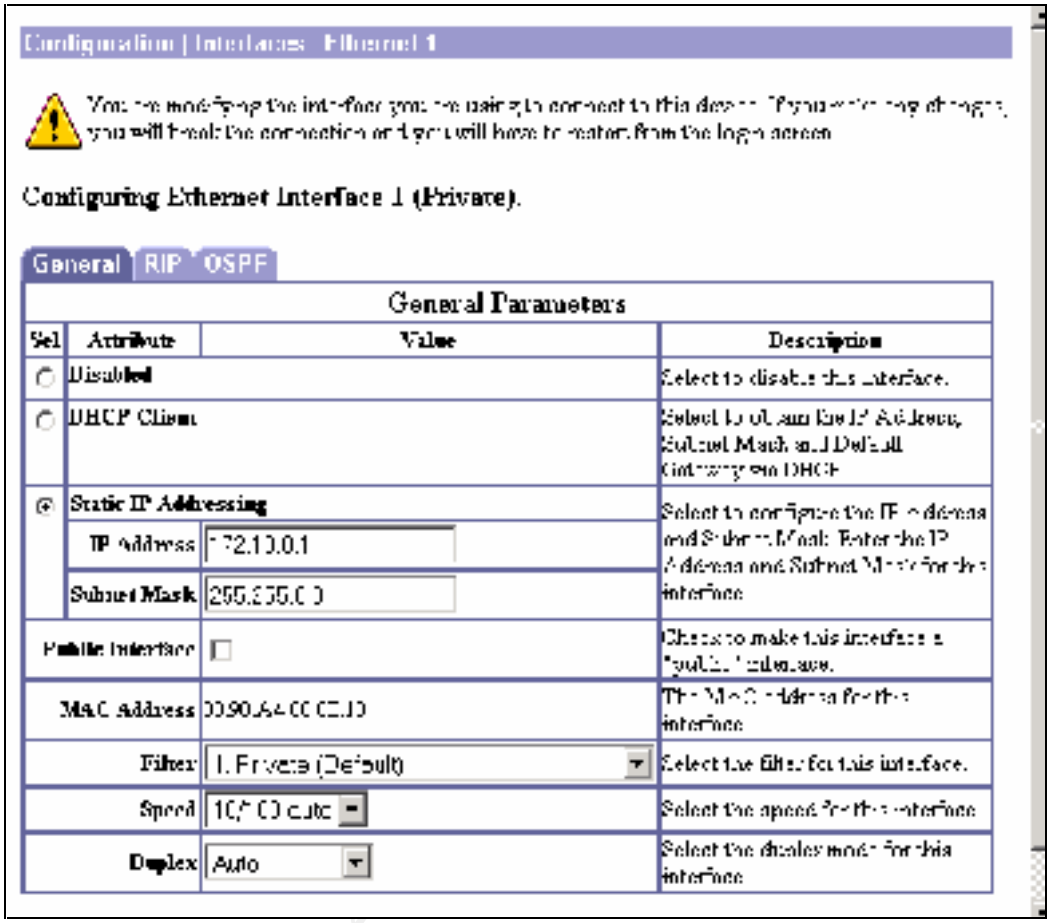
Several management protocols are available for the Cisco 3015, including HTTP/HTTPS, TFTP, Telnet, Telnet/SSL, SSH, and SNMP. Because of the critical nature of this component, and because the ubiquitous nature of browsers which support HTTPS, management will be done using HTTPS. HTTPS will provide a secure channel for all communications between the VPN concentrator and the management workstation. In addition, administration will only be allowed from a host on the internal network. Other hosts, either on the internal network, or via Internet access, can be added later as needed. This is configured via the **Administration->Access Rights->Access Control List** screen. An administrative workstation on the local network will be the only system allowed access. Please note that if no address is listed in the **Access Control List** screen, than any workstation can be used for administrative purposes as long as a valid administrator user name and password are entered. Sessions will be set to time out after 10 minutes of inactivity.

By default, five users are defined with some level of administrative privilege, however, only "admin" is enabled by default. Because there will be very few administrative duties once the concentrator is in production, the other administrators will not be enabled.

Interface Setup

There are three interfaces on the 3015 concentrator. These are the Private, Public, and External interfaces (Ethernet interfaces one, two, and three respectively). Interfaces are setup via the **Configuration->Interfaces->Ethernet X** screen. In the setup for GIAC Enterprises, only interfaces one and two will be utilized. Interface 1 will face the Checkpoint firewall, and interface two will face the border router. Interface 1 must traverse the Checkpoint firewall in order to reach the internal network. This provides improved traffic filtering and control, and improved logging. The following graphics shows the addressing and essential parameters for the Private and Public interfaces.

Figure 2.30



Configuration | Interfaces - Ethernet 1

You are modifying the interface you are using to connect to this device. If you change any settings, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General | RIP | OSPF

General Parameters

Sel	Attribute	Value	Description
○	Disabled		Select to disable this interface.
○	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
◉	Static IP Addressing		Select to configure the IP address and Subnet Mask. Enter the IP Address and Subnet Mask for the interface.
	IP Address	172.16.0.1	
	Subnet Mask	255.255.0.0	
	Public Interface	☐	Check to make this interface a "public" interface.
	MAC Address	0090.A400.0E10	The MAC address for this interface.
	Filter	1: Private (Default)	Select the filter for this interface.
	Speed	10/100 Auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.

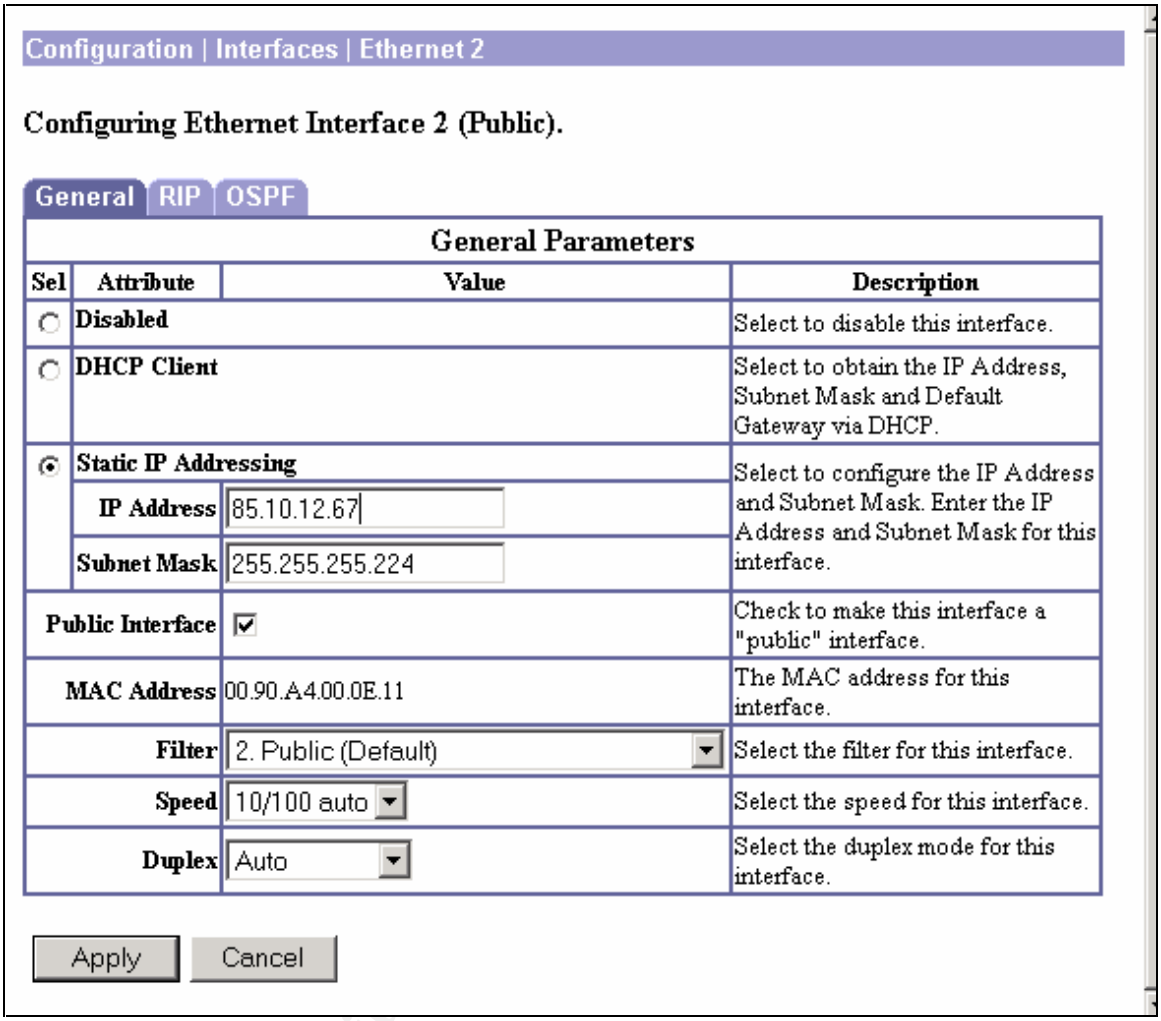


Figure 2.31

Also, since only static routing will be in use on the concentrator, RIP will be disabled both inbound and outbound, and OSPF will also be disabled. This reduces the probability of attacks utilizing bogus routes.

Server Setup

The only servers to be utilized in the setup of the GIAC Enterprises VPN concentrator will be an Authentication server, a DNS server, and an NTP server.

The Authentication server used will be an RSA/ACE server running on a hardened Solaris platform. The server will reside on the internal network with network address 172.17.0.2. The server will use the default timeout of 4 seconds and a default retry parameter of 2.

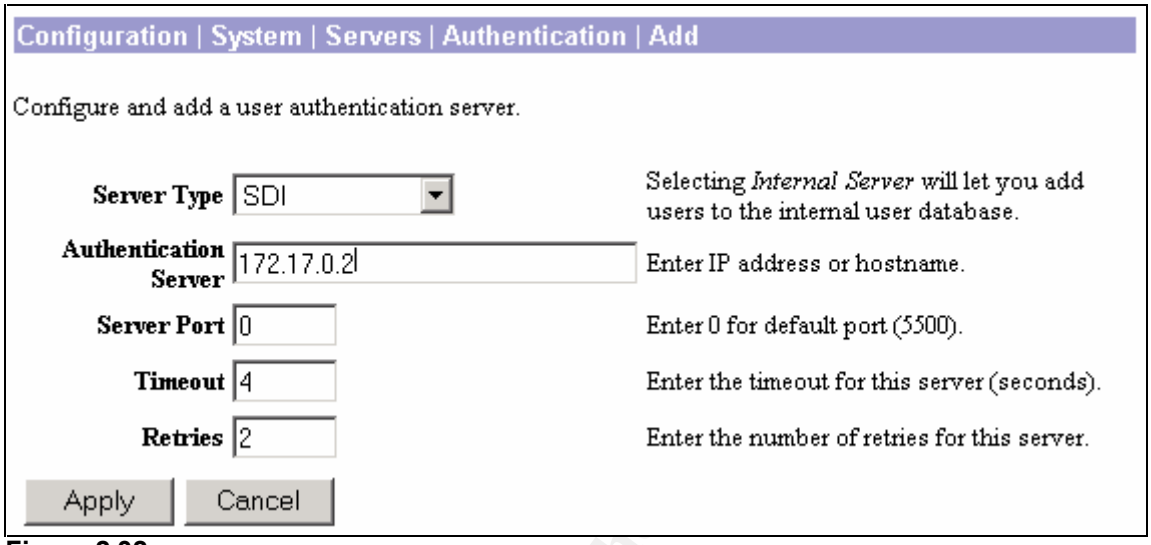


Figure 2.32

To avoid the number of openings through the firewall, the VPN concentrator will be configured to obtain time from Internet based time servers. NTP hosts are added to the concentrator via the **Configuration->System->Servers->NTP->Hosts->Add** screen.

Address Management

Addresses will be setup using a pool for each of the groups needing access to intranet / DMZ servers. Since we are using private addresses and have no problems with a shortage of addresses available, we will use a pool of 255 addresses for each group. Implementing the pools as such will also reduce the complexity of the firewall filtering rules. These address pools are setup via the **Configuration->System->Address Management-> Pools->Add** screen. The groups will be setup as shown in the following table.

Group	Begin Address	End Address
GIAC Enterprise Employees	172.19.2.1	172.19.2.255
GIAC Suppliers	172.19.3.1	172.19.3.255
GIAC Partners	172.19.4.1	172.19.4.255

Table 2.2

Tunneling Protocols

The Cisco 3015 VPN Concentrator supports PPTP, L2TP, and IPSec as tunneling protocols. It will also support L2TP over IPSec for Windows 2000 VPN Client support. The recommendation is for GIAC Enterprises to standardize on

the IPSec suite of protocols for all VPN communications. Therefore, we will disable (or not enable) the L2TP and PPTP tunneling protocols. This is done from the **Configuration|System|Tunneling Protocols| L2TP and Configuration|System|Tunneling Protocols| PPTP** screens.

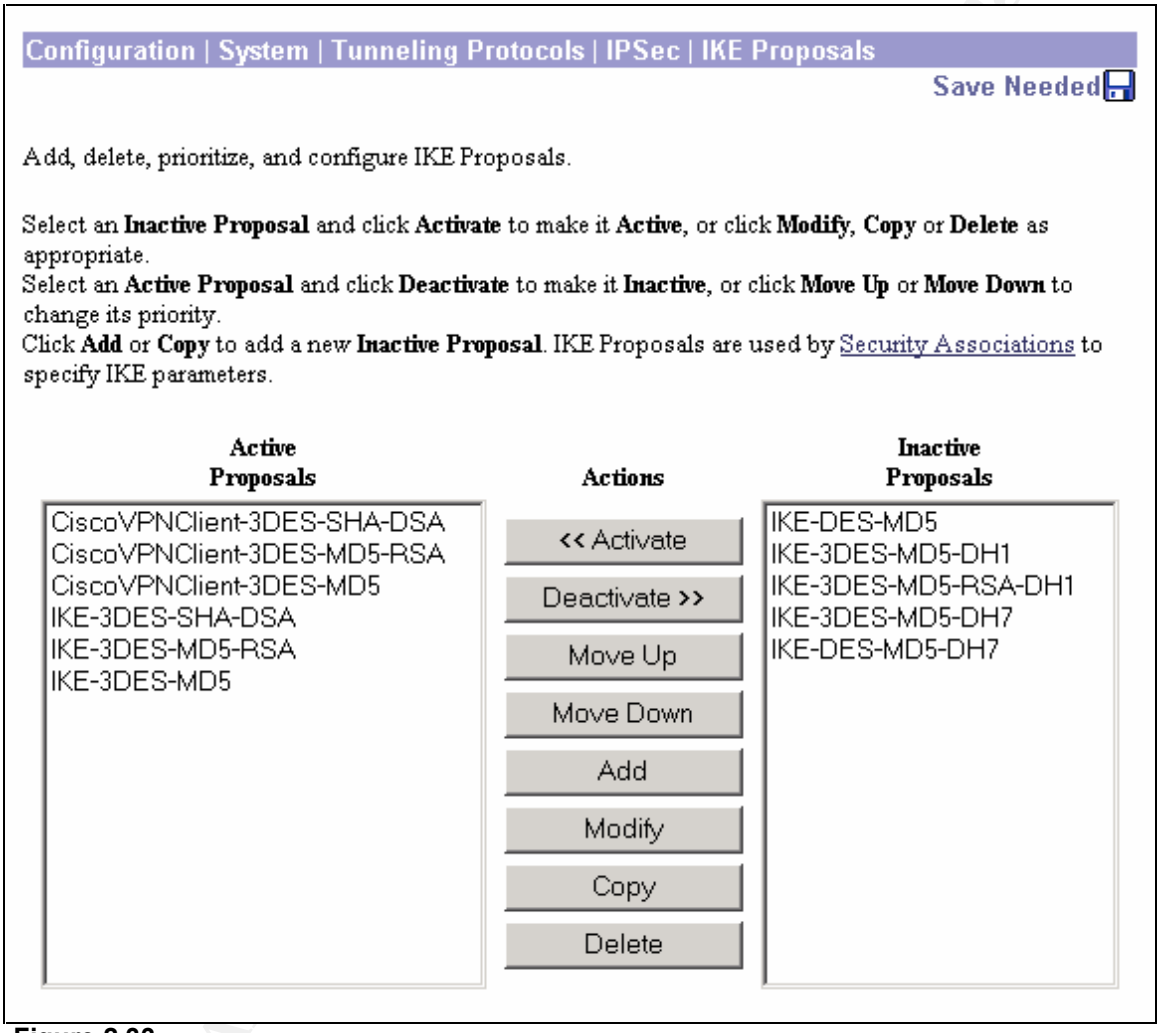


Figure 2.33

Routing

As mentioned previously, static routing will be used on the VPN. Any routes needed for the internal network and DMZ will be added, as well as a default gateway set as 85.10.12.65. In addition, OSPF, Redundancy, and Reverse Route Injection will be disabled.

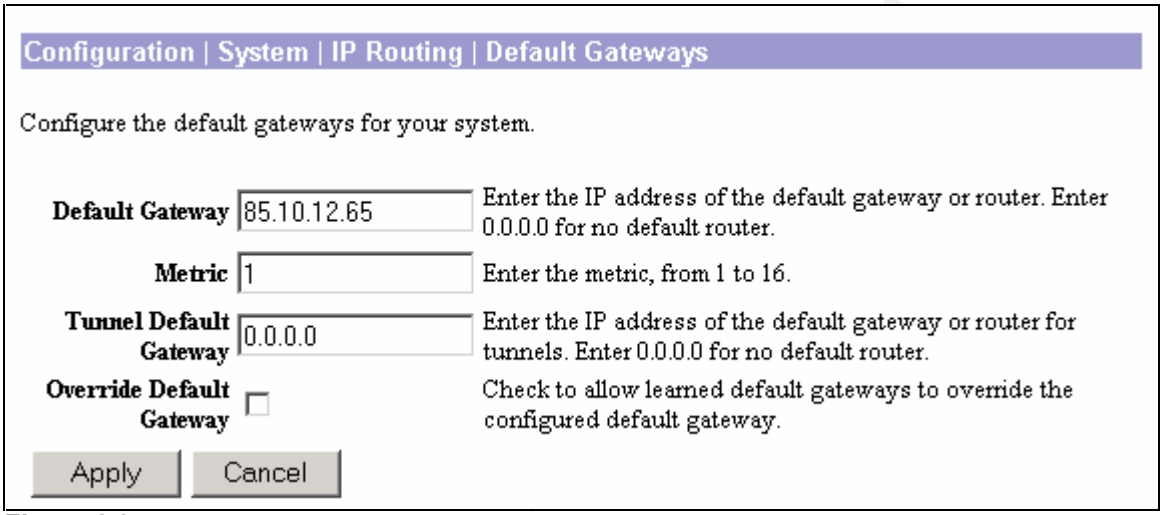


Figure 2.34

User Management – Base Group

The Base Group provides a means of setting parameters which may be common among other groups or users. The Base Group screen allows the setting of General, IPSec, Mode Config, Client FW, HW Client, and PPTP/L2TP parameters. With forethought about these settings, much time and effort can be saved with future additions of users and groups. Other groups will be configured to inherit parameter values from the base group, and the users will inherit values from the user's assigned group. We will discuss each parameter below.

General Tab

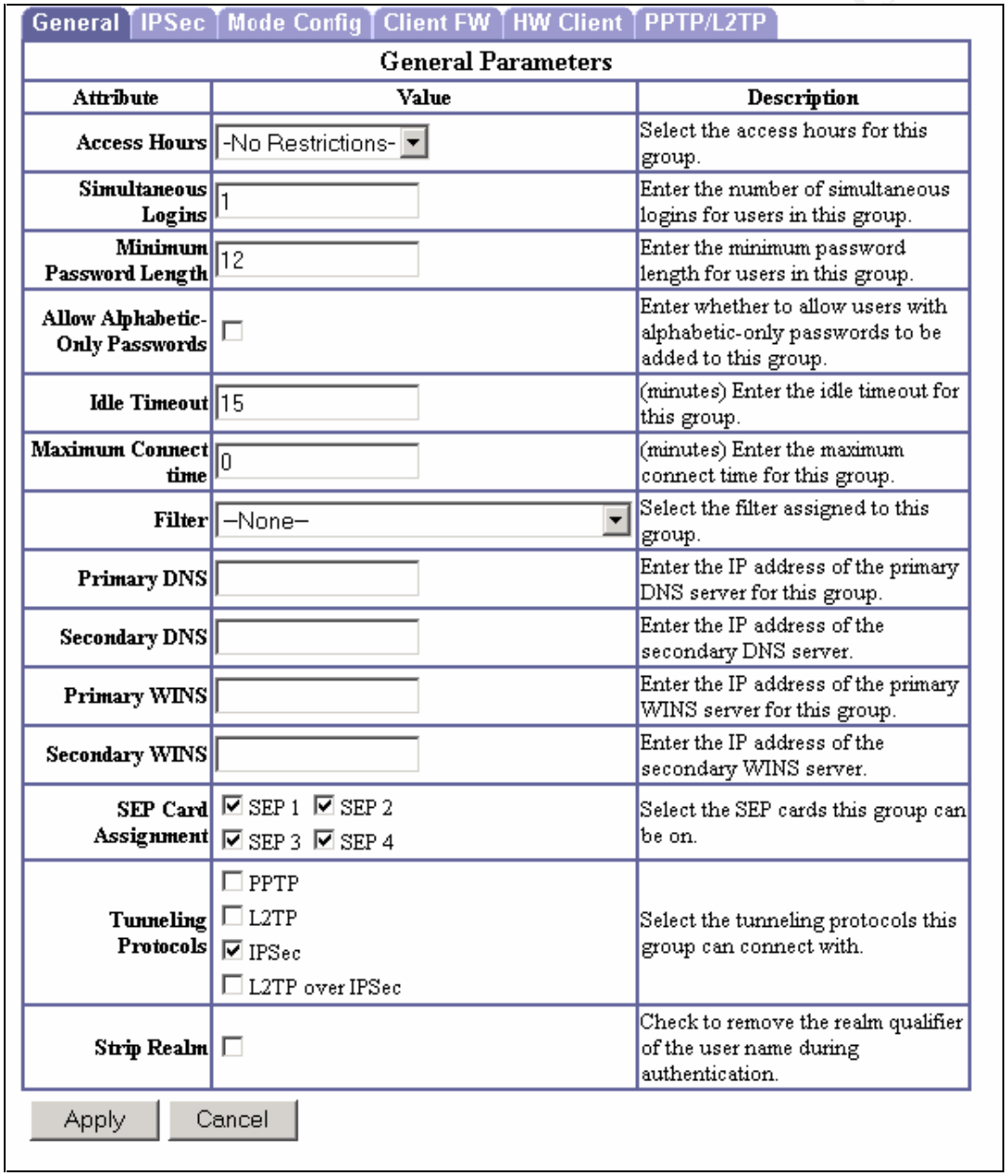


Figure 2.35

Access Hours – Since GIAC Enterprises is a global corporation, there will be no restrictions on access hours.
Simultaneous Logins – Each user will be assigned his own login and should not

be logged in more than once at anyone time.
Minimum Password Length – We will set this at 12, but will use the SecureID server for authenticating all logins.
Allow Alphabetic Only Passwords – If in the future passwords are used for authentication, users will be forced to use a mix of alpha and numeric / special characters to authenticate to the system.
Idle Timeout – After 15 minutes of inactivity, the user will be logged off the system. This will help to minimize problems with users leaving the terminals unattended. It will also keep the VPN resources free for people actively utilizing the VPN.
Maximum Connect Time – Users may stay connected for an unlimited amount of time as long as they are actively using the system.
Filter – Filters will be assigned on a per group / user basis. In addition, filtering will also be done at the Checkpoint firewall.
Primary DNS – Primary DNS server.
Secondary DNS – Secondary DNS server.
Primary WINS – Primary WINS server.
Secondary WINS – Secondary WINS server.
SEP Card Assignment – Because this concentrator has no SEP (Scalable Encryption Processing) cards installed, this parameter is ignored.
Tunneling Protocols – As mentioned previously, IPSec will be the standard tunneling protocol for GIAC Enterprises use.

IPSec Tab

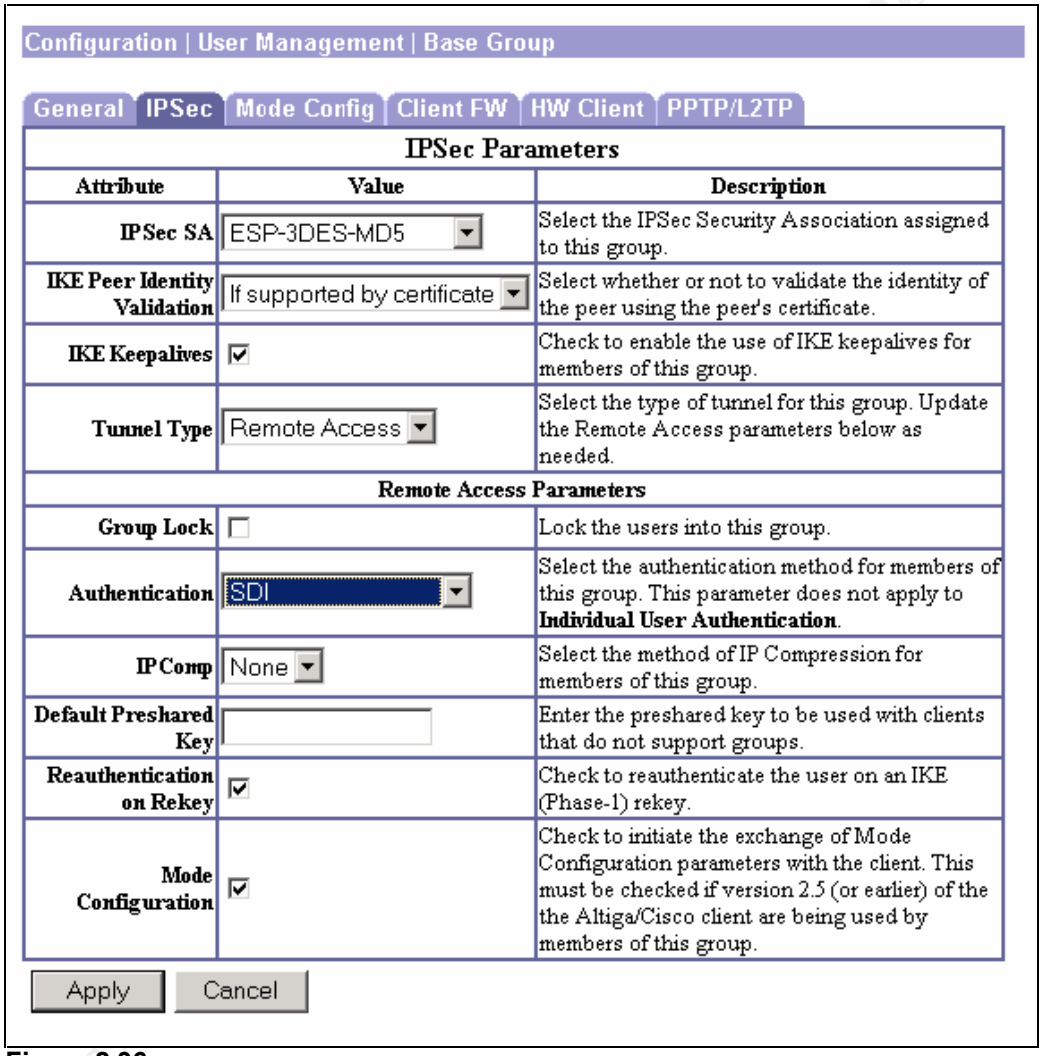
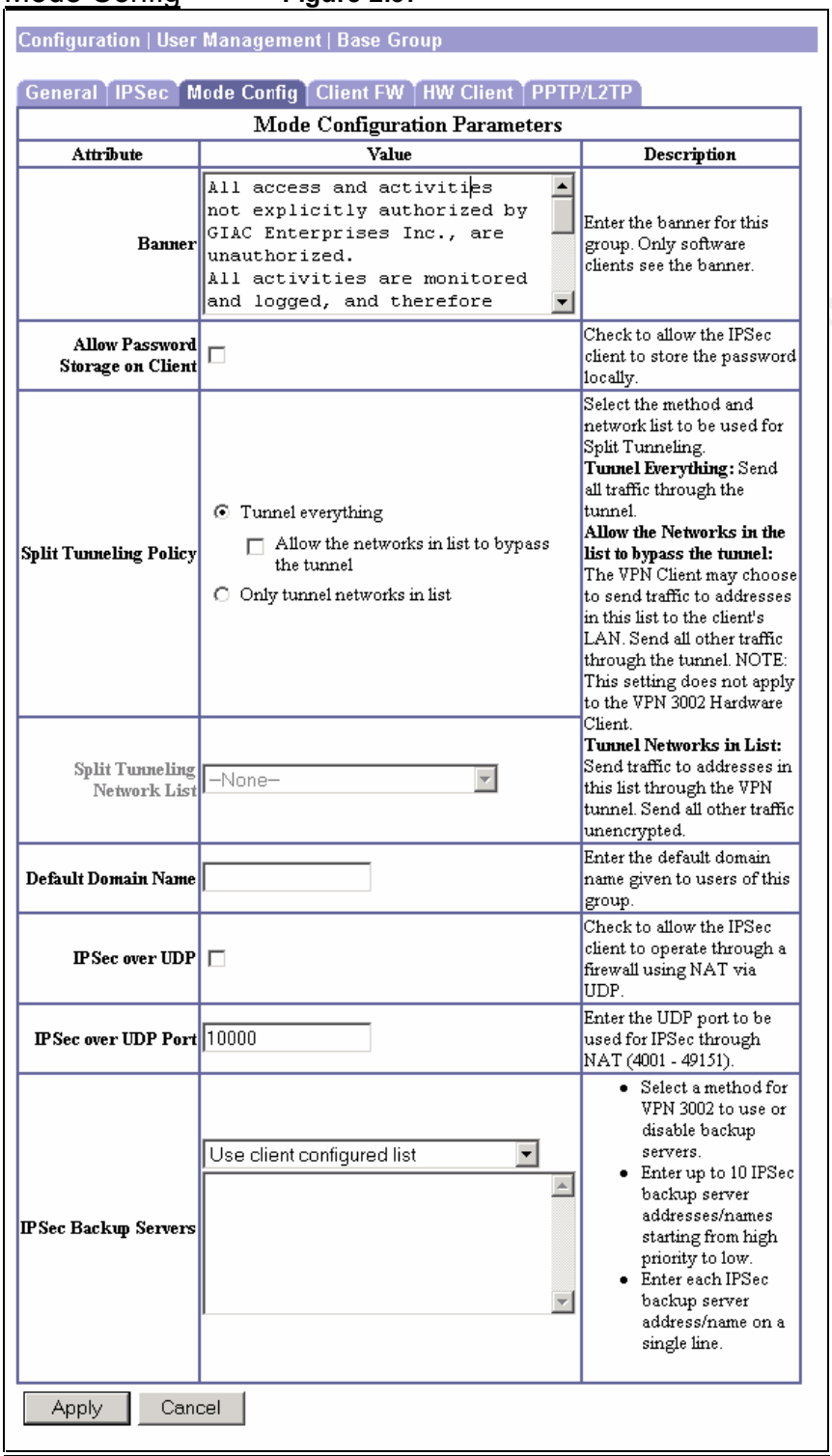


Figure 2.36

IPSec SA – This is the SA which will be associated with the Base group. This is the default method, and can be changed on a per group / user basis.
GIAC Enerprises will standardize on ESP as the IPSec protocol used since it provides confidentiality. MD5 or SHA will be used for hashing. The encryption protocol used will depend upon the level of confidentiality of the data being transferred, DES for less secure documents, and 3DES for more secure documents.

IKE Peer Identity Validation –If the peers certificate supports this, fields available in the peer's certificate will be compared to the peers identity to see if they match. This will not be used in our present configuration.
IKE Keepalives – This allows the concentrator to terminate connections which may have lost connectivity. Keepalives are sent between the peers to validate that the connection and session are in fact still present.
Tunnel Type – Since the present plan calls for not using LAN-TO_LAN connectivity but instead plans to use the Remote access capabilities of the Cisco VPN client software, the default type selected will be Remote Access.
Group Lock – The users will be assigned to specific groups at the User level using the **Configuration|User Management|Users** screen. By specifying a specific group for a user, either here or on the user screen the concentrator will validate authentication both at the group and user level.
Authentication – The authentication will be performed via a RSA SecureID server.
IP Comp – We will not use data compression because of increased memory and CPU requirements on the concentrator.
Default Preshared Key – This field is used for clients which do not support groups. Because all clients in our proposed setup will support groups, and thus will not need to validate with a preshared key, we will not utilize this field.
Reauthentication on Rekey – For additional security we will enable this parameter.
Mode Configuration – Mode configuration must be enabled to allow the exchange and enforcement of parameters of clients connecting to this concentrator.

Mode Config **Figure 2.37**



Banner- The Banner will be changed to construe not a message of welcome and good will, but instead issue a warning regarding the ownership and access rights of the enterprise network.
Allow Password Storage on Client – Because of problems with misplaced laptops and unattended workstations, password storage on the client will not be permitted. It is also suggested that GIAC policies prohibit the storage of the password in any other applications on the client, and also that the passwords not be physically written on the client.
Split Tunneling Policy – Because of additional risks associated with split tunneling, all traffic originating from the client will travel encrypted through the VPN tunnel for the duration of the VPN session.

Client FW Tab

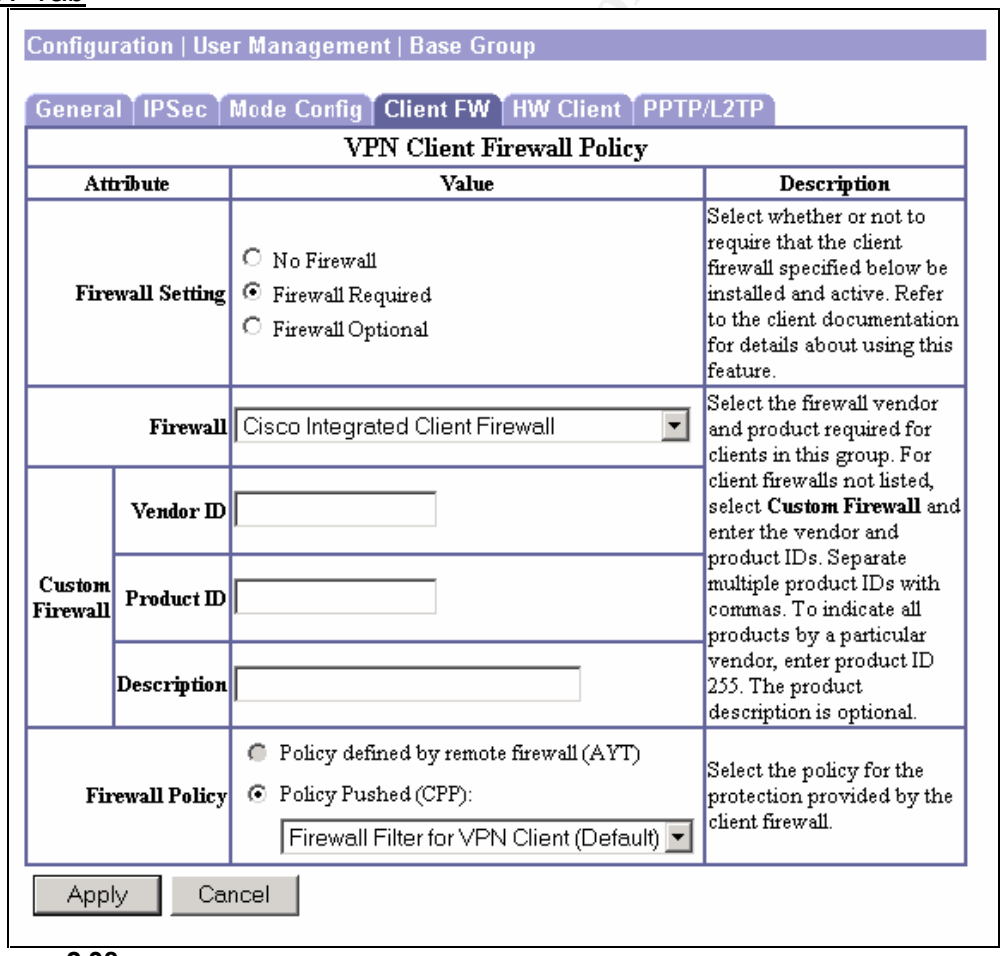


Figure 2.38

Firewall Setting – We will set this to "Firewall Required". This ensures that the client to which we have a session established has a firewall.
Firewall – This will be set to "Cisco Integrated Client Firewall", since this is the client / firewall combination we expect to have the highest access rates to the 3015 concentrator.
Firewall Policy – The policy will be pushed to the remote client. The filter used will be the "Firewall Filter for VPN Client (Default)" filter. This will effectively drop all traffic not originating from the client, and accept all traffic which does originate from the client. This filter is from the perspective of the client, not the concentrator.

Traffic Management Rules

We will add rules, both inbound and outbound, for telnet, ftp, smtp, pop-3, and Oracle Listening Service access. In addition, as specified earlier the firewall will be used to further control and limit traffic based on source IP (IP Pools defined in the concentrator).

A group will be created for Partner, Supplier, and Employee access. These groups will inherit the majority of parameter values from the Base group, with adjustments being made to the "Filters" parameter of the General Tab. Filters will be created using the rules which allow access to needed applications. Below is a table listing the Filter / Rule / Group combinations which will be implemented on the VPN concentrator.

Rule	Suppliers Filter	Partners Filter	Employees Filter
IKE/In (Forward/In)	X	X	X
IPSEC/ESP In (Forward/In)	X	X	X
TelnetIn (Forward/In)			X
SMTP/In (Forward/In)			X (note 1)
POP3In (Forward/In)			X
OracleIn (Forward/In)	X		X
FtpCtrlIn (Forward/In)		X	X
FtpDataIn (Forward/In)		X	X
IKE/Out (Forward/Out)	X	X	X
TelnetOut (Forward/Out)			X
SMTP/Out (Forward/Out)			X (note 2)
POP3Out (Forward/Out)			X
OracleOut (Forward/Out)			X

FtpCtrlOut (Forward/Out)		X	X
FtpDataOut (Forward/Out)		X	X

Table 2.3

Source ports for all rules will range from 1024 to 65535. Destination ports will use the IANA assigned ports.
Note 1: The allowed destination address will be that of the GIAC Intranet Email server only.
Note 2: The allowed source address will be that of the GIAC Intranet Email server only.

Intrusion Detection Setup Details

Snort Intrusion Detection Sensors will be placed on the external, DMZ, VPN, and internal interfaces of the Checkpoint Firewall cluster. These IDS systems will have the current set of signatures pushed to them nightly (the signatures will be updated from www.snort.org/dl/signatures/snortrules.tar.gz). A script initiated via cron will retrieve the new signatures from this site and push them out to each sensor using SCP. Each sensor will then run scripts initiated via cron to update these signatures and restart snort.

Each sensor will be equipped with two Ethernet interfaces. One interface will be used for remote access via OpenSSH and for maintenance functions such as receiving new rules from the rule server, updating the OS, etc. This interface will also be used for NTP and syslog communications. IP addresses on these interfaces will follow specifications as set forth in rfc 1918 utilizing the 172.16/12 prefix.

The second interface will be utilized on the external and DMZ sensors only (it will exist on the internal sensor only for backup purposes and to standardize sensors for ease of movement between zones should this become necessary). In the DMZ and external zones, this interface will initialize with no assigned IP address (0.0.0.0). Additionally, because these sensors could potentially form a gateway between the trusted and untrusted zones of the networks, a “receive-only” cable (see http://www.snort.org/docs/faq.html#3.1) will be used on these interfaces, thereby making it physically impossible to form a TCP connection via these interfaces.

Iptables will be implemented to provide an additional layer of security on the internal (172.16/12) interface. The policy scheme implemented will deny all traffic unless otherwise explicitly permitted. Implemented as such, this should

assist in minimizing both currently known and future exploits. Allowed traffic will permit usage of the following services: ntp(client), ssh(server), and syslog(client). Following is the script, with detailed comments, used in the iptables configuration.

Iptables script for IDS systems

--- Begin script (This tag for informational purposes only - not part of script)

```
#!/bin/bash
#
#   Initialize Variables
#
INTERFACE="eth1"
CLASSA="10.0.0.0/8"
CLASSB="172.16/12"
CLASSC="192.168.0.0/16"
CLASSD="224.0.0.0/4"                    # multicast
CLASSE="240.0.0.0/5"                    # experimental
LOOPBACK="127.0.0.0/8"
LOOPBACKIF="lo"
NTPSERVER="172.17.0.4"
DNSSERVER="172.17.0.6"
LOGSERVER="172.17.0.5"
NTP="123"
DOMAIN="53"
SYSLOG="514"
#
#   Set Network configuration
#
#   Do not accept redirects
#
echo 0 > /proc/sys/net/ipv4/conf/eth0/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/eth1/accept_redirects
#
#   Turn off forwarding
#
echo 0 > /proc/sys/net/ipv4/conf/eth0/forwarding
echo 0 > /proc/sys/net/ipv4/conf/eth1/forwarding
#
#   Do not accept icmp echoes
#
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
#
#
#   Flush all chains so we have a clean start.  If chains are not flushed, the rules in this
#   script will be appended to any pre-existing rules leading to unexpected results.
```

```
#
iptables -F
#
#   Zero out the counters.  Although this is not mandatory, this will allow us to keep
#   stats on this instance of iptables.
#
iptables -Z
#
#   Set the policies for INPUT, OUTPUT, and FORWARD to DROP.  This does two things
#      1)  Blocks all incoming traffic until remaining rules are in place, and
#      2)  Sets the policy to deny all unless explicitly allowed
#   By setting the policy to deny all unless explicitly allowed, this allows all traffic needed
#   for the sensor to function properly, but drops any potentially malicious traffic
#
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#
#   Now allow the loop back address to pass traffic
#
iptables -A INPUT -i $LOOPBACKIF -j ACCEPT
iptables -A OUTPUT –o $LOOPBACKIF -j ACCEPT
#
#   Allow ntp to flow over UDP port 123 get time from time server
#
iptables -A OUTPUT -p udp -d $NTPSERVER --dport $NTP -j ACCEPT
iptables -A INPUT -p udp -s $NTPSERVER --sport $NTP -j ACCEPT
#
#   Allow ssh via port 25022 (administration pc is 172.17.0.15)
#
iptables –A OUTPUT –p tcp -d  172.17.0.15  --sport 25022 –m state \
--state ESTABLISHED,RELATED –j ACCEPT
iptables –A INPUT –p tcp –s 172.17.0.15 --dport 25022 -m state \
--state NEW,ESTABLISHED,RELATED -j ACCEPT
#
#   Allow UDP connections to syslog server on syslog port.  Since UDP is a connectionless
#   protocol, and we do not require acknowledgements to be returned, this is a one-way
#   service (outbound).
#
iptables -A OUTPUT -p udp -d $LOGSERVER --dport $SYSLOG -j ACCEPT
#
#   Allow DNS queries to flow outbound to DNS server - Allow both UDP queries, and for
#   requests requiring over 512 byte responses (including headers), allow stateful TCP
#
iptables -A OUTPUT -p udp -d $DNSSERVER --dport $DOMAIN -j ACCEPT
iptables -A INPUT -p udp -s $DNSSERVER --sport $DOMAIN -j ACCEPT
iptables -A OUTPUT -p tcp -d $DNSSERVER --dport $DOMAIN -m state \
--state NEW,ESTABLISHED –j ACCEPT
iptables -A INPUT -p tcp -s $DNSSERVER --sport $DOMAIN -m state \
--state ESTABLISHED –j ACCEPT
```

--- End Script (This tag for informational purposes only - not part of script)

As a further means of securing the sensors, all services which are not explicitly needed for the functionality of the sensor will be removed. In addition, if a service can be run as a scheduled task as opposed to daemon mode, this will be implemented. SSH will be used for secure communications to these sensors, and Tripwire will be used to ensure integrity.

Syslog Hardening Details

As stated previously, the syslog server will reside on a fully patched version of RedHat Linux 7.3. The system will have all unneeded services removed. Services which will be left available are TCP port 25022 for ssh services (moved from port 22), and UDP port 514 for syslog communications. This system will employ swatch, a log watching program which will be used to notify concerned personnel of events deemed of interest by GIAC system administrators.
In addition, the syslog server will run iptables. Iptables on this system will be setup to deny all traffic unless specifically allowed. Implemented as such, this should assist in minimizing both currently known and future exploits. Allowed traffic will permit usage of the following services: ntp(client), ssh(server), syslog(server), smtp(client). Following is the script, with detailed comments, used in the Iptables configuration.

Iptables Setup for Syslog System

--- Begin script (This tag for informational purposes only - not part of script)

```
#!/bin/bash
#
#   Initialize Variables
#
INTERFACE="eth0"
CLASSA="10.0.0.0/8"
CLASSB="172.16/12"
CLASSC="192.168.0.0/16"
CLASSD="224.0.0.0/4"                    # multicast
CLASSE="240.0.0.0/5"                    # experimental
LOOPBACK="127.0.0.0/8"
LOOPBACKIF="lo"
NTPSERVER="172.17.0.4"
DNSSERVER="172.17.0.6"
LOGSERVER="172.17.0.5"
NTP="123"
DOMAIN="53"
```

```
SYSLOG="514"
SMTP="25"
#
#   Flush all chains so we have a clean start.  If chains are not flushed, the rules in this
#   script will be appended to any pre-existing rules leading to unexpected results.
#
iptables -F
#
#   Zero out the counters.  Although this is not mandatory, this will allow us to keep
#   stats on this instance of iptables.
#
iptables -Z
#
#   Set the policies for INPUT, OUTPUT, and FORWARD to drop.  This does two things
#      1)  Blocks all incoming traffic until remaining rules are in place, and
#      2)  Sets the policy to deny all unless explicitly allowed
#   By setting the policy to deny all unless explicitly allowed, this allows all traffic needed
#   for the sensor to function properly, but drops any potentially malicious traffic
#
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#
#   Now allow the loop back address to pass traffic
#
iptables -A INPUT -i $LOOPBACKIF -j ACCEPT
iptables -A OUTPUT -o $LOOPBACKIF -j ACCEPT
#
#   Allow ntp to flow over UDP port 123 get time from the time server
#
iptables -A OUTPUT -p udp -d $NTPSERVER --dport $NTP -j ACCEPT
iptables -A INPUT -p udp -s $NTPSERVER --sport $NTP -j ACCEPT
#
#   Allow ssh via port 25022 (administration pc is 172.17.0.15)
#
iptables –A OUTPUT –p tcp -d  172.17.0.15  --sport 25022 –m state \
--state ESTABLISHED,RELATED –j ACCEPT
iptables –A INPUT –p tcp –s 172.17.0.15 --dport 25022 -m state \
--state NEW,ESTABLISHED,RELATED -j ACCEPT
#
#   Allow DNS queries to flow outbound to DNS server - Allow both UDP queries, and for
#   requests requiring over 512 byte responses (including headers), allow stateful TCP
#
iptables -A OUTPUT -p udp -d $DNSSERVER --dport $DOMAIN -j ACCEPT
iptables -A INPUT -p udp -s $DNSSERVER --sport $DOMAIN -j ACCEPT
iptables -A OUTPUT -p tcp -d $DNSSERVER --dport $DOMAIN -m state \
--state NEW,ESTABLISHED –j ACCEPT
iptables -A INPUT -p tcp -s $DNSSERVER --sport $DOMAIN -m state \
--state ESTABLISHED –j ACCEPT
#
```

```
#   Allow SMTP to be used for notifications from the swatch program.  SMTP will
#   be allowed to connect outbound only.
#
iptables -A OUTPUT -p tcp --dport $SMTP -m state \
--state NEW,ESTABLISHED –j ACCEPT
iptables -A INPUT -p tcp --sport $SMTP -m state \
--state ESTABLISHED –j ACCEPT
```

--- End Script (This tag for informational purposes only - not part of script)

As a further means of securing the server, all services which are not explicitly needed for the functionality of the server will be removed. In addition, if a service can be run as a scheduled task as opposed to daemon mode, this will be implemented. SSH will be used for secure communications to this server, and Tripwire will be used to ensure integrity.

III. Security Audit

Security Assessment

Upon completing the installation of the described security architecture, LCS will conduct a security audit to ensure proper operation and configuration of the Checkpoint firewall complex. Because many security breeches are associated with configuration errors of network / host security implementations, it is important to conduct a complete audit to determine if the configuration is secure. A properly conducted audit will expose weaknesses that can be rectified before they can be exploited. Conducting these audits on a periodic basis, and when changes are made to security related hardware / software will enable GIAC Enterprises to constantly evaluate and improve their security posture.

To minimize impact on network resources, and because there is some small element of risk involved in the testing procedures, the audit will be conducted on the Saturday following the security implementation (Note: Internet access should not be available until after the audit is complete). By conducting the audit on a Saturday, the testing will have the least impact on the GIAC internal network (the DMZ and external interfaces will not be available for use until the audit is complete, so testing should not present problems on those interfaces).

In addition, because some of the auditing tools may be disruptive LCS will request a GIAC System Administrator be available during the active audit. Although LCS expects there to be no loss of data, and *should not* experience any system outages due to testing procedures, the on-site availability of the administrator will help to reduce downtime on the servers thereby ensuring availability to GIAC users / partners / customers, and reducing testing time and costs.

Although other components of the system should be tested, the primary focus will be aimed at finding weaknesses within the firewall complex. LCS feels that all security and server related components such as the border router, IDS systems, logging system, web server, etc., should be tested although this is not within the scope of this project. As an additional precaution, LCS recommends that GIAC System Administrators perform the following.

1) All host machines be scanned for viruses / trojan software using the latest GIAC Enterprises standard Anti-Virus software,
2) That password cracking software be used on server machines to find weak passwords,

3) Nessus be run against all servers / security components,
4) Baseline configurations be established on all servers / security components

All audits should be run on a periodic basis or when changes to the systems warrant a new audit.

GIAC Enterprises believes that many of the free security tools on the market perform as well or better than commercially available tools, and therefore wishes to use these free tools to perform the vulnerability audits. LCS has chosen five tools for these audits. Each of the tools being used to perform the analysis was listed the "Top 50 Security Tools" (http://www.insecure.org/tools.html) from a survey of 1200 nmap users (nmap was not included in the survey). The tools and a short description of each is listed in table 3.1.

Auditing Tool	Description
Nessus	A security vulnerability scanner. According to the Nessus web site, Nessus has two features which increase it's functionality as a scanning tool: 1) It does not assume that services are running on a given well-known port, and can find these services on non-standard ports, and 2) it does not guess about the vulnerability, but will actually try to exploit it. The web site also states that "Nessus was awarded the Information Security Magazine Excellence Award in the Security Freeware/Shareware category" (Deraison). It was also listed as the number one security tool on http://www.insecure.org/tools.html.
HPing2	HPing2 is a feature rich security tool supporting TCP, UDP, and ICMP. It will also support RAW-IP. Among some of it's uses are port scanning and firewall testing. This information and more can be found at http://www.hping.org/.
Nmap	Nmap is a network scanning utility which can be used to map hosts on a network, the services available on the hosts, and can also perform OS finger printing. ' Nmap has won numerous awards, including "Information Security Product of the Year" by both Info World and Codetalker Digest ' (Fyodor).
tcpdump	A tool used for sniffing network packets. It may be used as is or in conjunction with tcpshow for easier data conversion.

lsof	A tool to list open files and ports on a system and which processes have them open (ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/).

Table 3.1

Estimated Costs

Task Description	Hours	Cost	Task Total
Test Planning			
Review OS Implementation	2	$100.00	$200.00
Review Firewall Policies	2	$100.00	$200.00
Develop Test Procedures	2	$100.00	$200.00
Penetration / Rule Testing			
Nmap scans	8	$100.00	$800.00
Hping Testing	1	$100.00	$100.00
Nessus Testing	1	$100.00	$100.00
lsof and Ping Testing	0.25	$100.00	$25.00
Analysis and Recommendations	6	$100.00	$600.00
Total for Audit			**$2,225.00**

Technical Description of Audit

Security Infrastructure Validation

After review of the security policies with GIAC representatives, and to make sure that both parties were in agreement, the following conclusions were reached.

CheckPoint Firewall

External Interface

1. Any packets addressed directly to a firewall interface, either DMZ, internal network, VPN, or Internet, should be dropped and no response returned to the requesting party.
2. ICMP error messages should not originate from the firewall.
3. TCP port 80 will be open for inbound services to the GIAC_DMZ_Web.
4. TCP port 443 will be open for inbound services to the GIAC_DMZ_Web.
5. TCP port 25 will be open for SMTP services to GIAC_DMZ_Email.
6. UDP port 514 will be open for the border router to the Intranet syslog server.
7. RST/ACKs will be returned by the firewall due to Syn being sent to port 113 of the GIAC_DMZ_Email server.

VPN Interface

1. Any packets addressed directly to a firewall interface, either DMZ, internal network, VPN, or Internet, should be dropped and no response returned to the requesting party
2. GIAC Suppliers should have access to port 1521 on the Oracle DB server
3. GIAC Partners should have ftp access to the DMZ FTP server
4. GIAC Employees should have telnet, smtp, pop-3, and ftp access to servers within the internal network, and Oracle access to Oracle server.
5. The VPN Concentrator should have access to UDP 5500 for SecurID authentication.
6. The VPN concentrator should have access to UDP port 514 for syslog logging to the Intranet syslog server.

DMZ Interface

1. Any packets addressed directly to a firewall interface, either DMZ, internal network, VPN, or Internet, should be dropped and no response returned to the requesting party.
2. TCP port 25 (with resource) will be open to the GIAC_Intranet_Email from the GIAC_DMZ_Email server.

3. TCP / UDP ports 123 will be open for NTP to Internet NTP servers from the GIAC_DMZ_NTP server.
4. TCP port 25 will be open to any Internet destination for SMTP services from GIAC_DMZ_Email.
5. TCP and UDP port 53 will be open to the Internet DNS servers for the GIAC_DMZ_DNS server.

Internal Interface

1. Any packets addressed directly to a firewall interface, either DMZ, internal network, VPN, or Internet, should be dropped and no response returned to the requesting party.
2. TCP and UDP port 53 will be open to the GIAC_DMZ_DNS server from the GIAC_Intranet_DNS server.
3. TCP port 25 (with resource) will be open to GIAC_DMZ_Email from the GIAC_Intranet_Email server.
4. TCP and UDP port 123 will be open to Internet based NTP servers from the GIAC_Intranet_NTP server.
5. RST/ACKs will be returned by the firewall due to Syn being sent to port 113 of the GIAC_DMZ_Email server.
6. TCP port 80 will be open for HTTP services to Internet based web servers (including GIAC_DMZ_Web).
7. TCP port 443 will be open for HTTPS services to Internet based web servers (including GIAC_DMZ_Web).
8. FTP services will be available for select users to Internet based FTP servers.
9. TCP port 1521 will be open to the GAIC_DMZ_Oracle server from the GIAC Intranet network.

NMAP

The port scanning tool, nmap, will be used to scan for open ports on the firewall complex. Ports scanned will include both TCP and UDP transport protocol ports. By default, nmap normally scans approximately 1540 ports, but our scans of the firewall interfaces will include all 65535 TCP ports and 65535 UDP ports. This will help to ensure that a session can not be established with the firewall on any port.

Although TCP is described by rfc 0793, and later updated by rfc 3168, many vendors have somewhat different implementations. Because of these differing implementations, some TCP / IP stacks may respond differently to “unexpected” stimuli. Therefore, while testing for allowed connections to the TCP ports using

the SYN flag, we will also test using unexpected flag sequences. These connection types and expected responses are outlined below in Table 3.3.

TCP Flag Setting	Expected Response
ACK	An ACK is normally sent from the second TCP packet (the SYN/ACK packet, the second packet in the TCP 3 way handshake) through the last packet exchanged in the session (may be combined with other flags such as PSH/ACK, and FIN/ACK). Sent to a host as a first step (without the SYN from the destination host), a RST is expected for both open and closed ports.
FIN	FIN is used to terminate a TCP session, therefore its presence in the TCP header in the absence of an established session is not expected. In the Unix machines researched, the FIN, the FIN/PSH/URG, and the Null scans all returned the same responses. These responses were RST/ACK for a closed port, and no response for an open port.
SYN	This flag is normally sent to establish TCP sessions. It may be sent absent any other flags by the requesting, or client machine, or with SYN/ACK combination from the serving host. In the Unix machines researched, SYN elicited a SYN/ACK from an open port, and a RST/ACK from a closed port.

Table 3.3

(The above research was conducted using hping2 with AIX 4.3 and a Linux 2.4 kernel being the tested systems).

Although more combinations exist, these combinations should adequately test the ports for both expected and unexpected stimuli. The results will be compiled, and if possible adjustments made to produce the expected results.

(Note to grader: Because of limited testing facilities, addresses may have been changed in some of the scans to reflect those of GIAC Enterprise facilities).

Test Suite 3
Tests firewall rule 3 (External Interface)
Rule: any (firewall nodes) any drop
Scanner Position: External Interface
Scanner Source Address: 85.10.12.75
Notes: The external interface, being the one most exposed to Internet related threats, will have a full TCP scan (all 65,535 ports) for the following flag types: S,F, and A and will have all UDP ports scanned as well
This scan will help to ensure that various flag types do not cause any unexpected results on the firewall

3a)
```
nmap -sS -P0 -v -oN /gcfw/fwscan3a-syn.out -p 1-65535 -g80 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.66
```
3b)
```
nmap -sF -P0 -v -oN /gcfw/fwscan3b-fin.out -p 1-65535 -g80 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.66
```
3c)
```
nmap -sA -P0 -v -oN /gcfw/fwscan3c-ack.out -p 1-65535 -g80 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.66
```
3d)
```
nmap -sU -P0 -v -oN /gcfw/fwscan3d-udp.out -p 1-65535 –g53 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.66
```

Test Suite 3 continued
Tests firewall rule 3 (VPN Interface)
Rule: any (firewall nodes) any drop
Scanner Position: VPN Interface
Scanner Source Address: 172.19.0.5
Notes: The VPN interface, being a critical interface, will have a full TCP Syn scan and a full UDP port scan (all 65535 ports for both scan types).
3e)
```
nmap -sS -P0 -v -oN /gcfw/fwscan3e-syn.out -g80 -p 1-65535 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.19.0.2
```
3f)
```
nmap -sU -P0 -v -oN /gcfw/fwscan3f-udp.out -g53 -p 1-65535-n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.19.0.2
```

Test Suite 3 continued
Tests firewall rule 3 (DMZ Interface)
Rule: any (firewall nodes) any drop
Scanner Position: DMZ Interface
Scanner Source Address: 172.18.0.10
Notes: The DMZ interface, being a critical interface, will have a full TCP Syn scan and a full UDP port scan (all 65535 ports for both scan types).

3g)
```
nmap -sS -P0 -v -oN /gcfw/fwscan3g-syn.out  -g80 -p 1-65536 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.1
```
3h)
```
nmap -sU -P0 -v -oN /gcfw/fwscan3h-udp.out  -g53  -p 1-65535 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.1
```

Test Suite 3 continued
Tests firewall rule 3 (Internal Interface)
Rule: any (firewall nodes) any drop
Scanner Position: Internal Interface
Scanner Source Address: 172.17.0.10
Notes: The Internal interface, being a critical interface, will have a full TCP Syn scan and a full UDP port scan (all 65535 ports for both scan types).

3i)
```
nmap -sS -P0 -v -oN /gcfw/fwscan3i-syn.out  -g80  -p 1-65535 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.1
```
3j)
```
nmap -sU -P0 -v -oN /gcfw/fwscan3j-udp.out  -g53  -p 1-65535 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.1
```

Test Suite 4
Test firewall rule 4 (GIAC Supplier access to Oracle)
Rule: GIAC_Supplier GIAC_DMZ_Oracle Oracle Accept
Scanner Position: VPN Interface
Scanner Source: 172.19.3.10
Notes: Scan will be for default nmap ports only

```
nmap -sS -P0 -v -oN /gcfw/oracle4-syn.out  -g80 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.5
```

Test Suite 5
Tests firewall rule 5
Rule: GIAC_Partner GIAC_DMZ_FTP ftp Accept
Scanner Position: DMZ Interface
Scanner Source: 172.19.4.10
Notes: Scan will be for default nmap ports only

```
nmap –sS –P0 –v –oN /gcfw/ftp5-syn.out –g80 –n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.6
```

Test Suite 6
Tests firewall rule 6
Rule: GIAC_Employee GIAC_Internal GIAC_EMP_Services Accept
Scanner Position: VPN Interface
Scanner Source: 172.19.2.10
Notes: Scan will be for default nmap ports only

```
nmap -sS -P0 -v -oN /gcfw/emp6-syn.out -g80 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.0-10
```

Test Suite 7
Tests firewall rule 7
Rules: GIAC_Employee GIAC_DMZ_Oracle Oracle Accept
Scanner position: VPN interface
Scanner source: 172.19.2.10
Notes: Scan will be for default nmap ports only

```
nmap -sS -P0 -v -oN /gcfw/emp7-syn.out -g80 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.5
```

Test Suite 8
Tests firewall rule 8
Rules: GIAC_Intranet_DNS GIAC_DMZ_DNS dns Accept
Scanner position: Internal interface
Scanner source: spoofs the Internal DNS server (172.17.0.6)
Notes: Scan will be for default nmap ports only

8a)
nmap -sS -P0 -v -oN /gcfw/IntraDNS8a-syn.out –g53 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.3
8b)
nmap -sU -P0 -v -oN /gcfw/IntraDNS8b-udp.out –g53 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.3

Test Suite 9
Tests firewall rule 9
Rule: GIAC_DMZ_Email GIAC_Intranet_Email smtp Accept
Scanner position: DMZ Interface
Scanner Source: spoofs the DMZ email server (172.18.0.7)
Notes: Scan will be for default nmap ports only

9a)
nmap -sS -P0 -v -oN /gcfw/DMZEmail9a-syn.out –g25 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.3

Rule: GIAC_Intranet_Email GIAC_DMZ_Email smtp Accept
Scanner position: Internal Interface
Scanner Source: spoofs the Intranet email server (172.17.0.3)
Notes: Scan will be for default nmap ports only
9b)
nmap -sS -P0 -v -oN /gcfw/DMZEmail9b-syn.out –g25 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.7

Test Suite 10
Tests firewall rule 10
Rule: GIAC_VPN_Conc GIAC_Securid securid-udp Accept
Scanner position: VPN Interface
Scanner Source: spoofs the VPN Concentrator (172.19.0.1)
Notes: We will perform both a UDP and TCP scan because of the criticality of the authorization server.

```
nmap –sU -P0 -v -oN /gcfw/securid10-udp.out  -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.2

nmap –sS -P0 -v -oN /gcfw/securid10-syn.out –g80 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.2
```

Test Suite 12
Tests firewall rule 12
Rule: GIAC_DMZ_NTP (Internet NTP server) NTP Accept
Scanner position: DMZ Interface
Scanner Source: spoofs the DMZ NTP server (172.18.0.4)
Notes: 85.10.12.75 must be setup in NTP_Servers.

12a)

```
nmap -sU -P0 -v -oN /gcfw/DMZNTP12a-udp.out –g123 -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.75
```

12b

```
nmap -sS -P0 -v -oN /gcfw/DMZNTP12b-syn.out –g123-n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.75
```

Test Suite 13
Tests firewall rule 13
Rule: GIAC_Border_Router GIAC_Syslog syslog Accept
Scanner position: External Interface
Scanner Source: spoofs the border router (85.12.10.65)

13a)
```
nmap -sU -P0 -v -oN /gcfw/border-syslog13a-udp.out -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.70
```
13b)
```
nmap -sS -P0 -v -oN /gcfw/border-syslog13b-syn.out -n –g80 \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.70
```

Rule: GIAC_VPN_Conc GIAC_Syslog syslog Accept
Scanner position: VPN Interface
Scanner Source: spoofs the concentrator (172.19.0.1)

13c)
```
nmap -sU -P0 -v -oN /gcfw/border-syslog13c-udp.out -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.5
```
13d)
```
nmap -sS -P0 -v -oN /gcfw/border-syslog13d-syn.out -n –g80 \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.17.0.5
```

Test Suite 16
Tests firewall rule 16
Rule: GIAC_Internal GIAC_DMZ_Oracle Oracle Accept
Scanner position: Internal Interface
Scanner Source: 172.17.0.10
Notes: Scan will be for default nmap ports only

```
nmap -sS -P0 -v -oN /gcfw/Ident16-syn.out -n -g 80 \
--max_rtt_timeout 500 --initial_rtt_timeout 250 172.18.0.5
```

Test Suite 17
Tests firewall rule 17
Rule: Any GIAC_DMZ_Email ident Reject
Scanner position: External Interface
Scanner Source: 85.10.12.75
Notes: Scan will be for Ident port 113

```
nmap -sS -P0 -v -oN /gcfw/Ident17-syn.out -n –p 113 \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.65-95
```

Test Suite 18
Tests firewall rule 18
Rule: Any GIAC_DMZ_Web http/https Accept
Scanner position: External Interface
Scanner Source: 85.10.12.75
Scan will be for default nmap ports only

```
nmap -sS -P0 -v -oN /gcfw/DMZWeb18-syn.out -n -g 80 \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.68
```

Test Suite IntTrf
Tests Internal traffic escaping
Tests firewall rules 11, 19, 20, 22

Rule: GIAC_Intranet_NTP	NTP_Servers	ntp	Accept
Rule: GIAC_Internal	Any	http/https	Accept
Rule: ftp_users	Any	ftp	Client Auth
Rule: Any	Any	NBT	Drop

Scanner position: Internal Interface
Scanner Source: spoofs the Internal NTP server (172.17.0.4)
Notes: Tcpdump will be used to trace packets flowing from the external address to see which traffic is allowed out of the Internal network. 85.10.12.75 must be setup in NTP_Servers.

IntTrfa)

```
nmap -sS -P0 -v -oN /gcfw/IntTrfa-syn.out –n -p 1-65535 -g 80 \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.75
```

IntTrfb)

```
nmap -sU -P0 -v -oN /gcfw/IntTrfb-udp.out -n \
--max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.75
```

Nessus
The vulnerability scanning tool, Nessus, will be used to scan for weaknesses in both the Solaris operating system implementation, and the Checkpoint VPN-1/Firewall-1 software. Nessus utilizes plug-ins with tests for the various components on the system. The plug-ins are grouped into families. For instance, the plug-in family for the "Gain a shell remotely" contains 30 individual plug-ins as of this writing. For our purposes, the granularity of the tests will be focused at the plug-in family level, not at the individual plug-in. The reasoning for this is that running the extraneous tests will probably do no harm to the systems, and disabling these tests would probably take more time than just letting it execute.

Nessus also contains tests, classified as dangerous tests, which could cause problems such as loss of service, on the systems. However, a document published on a University of Missouri website by Greg Johnson, http://bengal.missouri.edu/~johnsong/audit/audit_files/frame.htm, states that in using Nessus and Nmap to scan over 13,000 connections, no data was ever lost. This document further states that only about 1 in 600 systems froze using the non-dangerous scans, and about 1 in 3 systems froze using the dangerous scans. Because of this, LCS requires an administrator be present during these vulnerability scans.

Information garnered with Nessus will be compiled and recommendations made to correct problems encountered.

Nessus tests done on host machines will be performed on the subnet where the tested host resides. A quote taken from http://www.nessus.org/doc/faq.html#Q.OTHER.FIREWALL states "If you want to be 100% sure you have hardened you host you should not rely on a firewall in front of it" (van der Kooij). Because LCS is in agreement with this statement, and because this goes along with a defense-in-depth strategy, if a firewall resides on the host being tested, such as iptables, the host will be tested with the firewall in both an active and an inactive state.

Plug-ins families which will be used to audit the firewall include: CGI abuses, Denial of Service, Finger abuses, FTP, Gain a shell remotely, Gain root remotely, General, Misc., NIS, Remote file access, RPC, SMTP problems, SNMP, and Firewall plug-ins.

HPING2
Hping2 will be used to attempt mapping of firewall rulesets. Using the ports shown to be in an open state from the nmap test results, hping2 will use TTL

values of 1 to attempt to elicit time-exceeded messages from the firewall. Logically, the tests work as follows. With the scanning device on the Internet side of the firewall located between the firewall and border router, hping2 will attempt to connect to various ports with a TTL value set to 1. If the port is a filtered port, the firewall should drop the packet and hping2 should see no response. If the port is not filtered, and if the firewall's IP stack sends out a time-exceeded message, one of two results should be observed:

1 – If the firewall software blocks this message originating from the firewall's own machine, the time-exceeded message will be blocked and the scanning device will receive no packets back.

2 – If the firewall software does not block messages originating form the firewalls own machine, the time-exceeded message will pass through and the scanning device will receive it and know that the port is unfiltered.

We will use this only on a handful of ports to verify the expected results (number 1 above), and not attempt all ports. Although it is possible to map all TCP ports open on a firewall (it will not work with UDP), a small number of ports should suffice for the audit.

```
Test Suite MapRules
Test for ICMP ttl expired messages being returned from the firewall
Scanner Position: External Interface
Scanner Source: Any valid address on that interface

hping2 –S –t 1 –p 80 85.10.12.68
```

In addition, Hping2 will be used to test rules 13 and 14 of the firewall rulebase.

```
Test Suite 14
Test firewall rule 14
NOT GIAC_Internal_Email          GIAC_DMZ_Email   smtp   Accept
Scanner Position: Internal Interface
Scanner Source: spoofs Internal Email server
Notes: Must disable rule 9 for this to be tested

hping2 –S –p 25 172.18.0.7
```

```
Test Suite 15
Test firewall rule 15
GIAC_DMZ_Email   NOT-GIAC_Intranet_Email          smtp   Accept
```

Scnner Position: DMZ Interface Scanner Source: spoofs DMZ Email server Notes: Must disable rule 9 for this to be tested hping2 –S –p 25 172.17.0.3

Hping2 will also be used for verification and clarity, if needed, of test results from nmap.

lsof
lsof is a tool available on most Unix variants for listing open files, the commands using those files, and the owners of those files. In addition, if used with the –i option, it will list open sockets. This can be useful for determining which services are listening on a given system. Thus, lsof will be run to verify which services are in fact listening on the firewalls, IDS systems, and logging system. These results will also be archived as a base for future runs of lsof to determine if and what network services on a given system have changed over time.

lsof -i

Ping
A ICMP Ping will be attempted on each interface (External, VPN, DMZ, and Internal) to verify that the firewall complex is not returning ICMP Replies.

ping 85.10.12.66 ping 172.17.0.1 ping 172.18.0.1 ping 172.19.0.2

Analysis and Recommendations

Test Results
(Note to grader: These test results were simulated by running the tests on a similar environment. Where results are shown, the addresses were changed to match those belonging to GIAC Enterprises).

---

* * * Results of Test 3a
This entry represents the nmap Syn scan of the external interface of the firewall.

```
# nmap (V. 2.54BETA22) scan initiated Mon Sep  9 09:19:07 2002 as: nmap -sS -P0 –v \
 -oN /gcfw/fwscan1a-syn.out -g80 -n -p 1-65535 --max_rtt_timeout 500 --initial_rtt_timeout 250
85.10.12.66
All 65535 scanned ports on  (85.10.12.66) are: filtered

# Nmap run completed at Mon Sep  9 10:09:04 2002 -- 1 IP address (1 host up) scanned in 2997
seconds
```

---

* * * Results of Test 3b

This entry represents the nmap FIN scan of the external interface of the firewall.

```
# nmap (V. 2.54BETA22) scan initiated Mon Sep  9 10:35:06 2002 as: nmap -sF -P0 –v \
 -oN /gcfw/fwscan1b-fin.out -g80 -n -p 1-65535 --max_rtt_timeout 500 --initial_rtt_timeout 250
85.10.12.66
All 65535 scanned ports on  (85.10.12.66) are: filtered

# Nmap run completed at Mon Sep  9 11:31:55 2002 -- 1 IP address (1 host up) scanned in 3408
seconds
```

---

* * *Results of Test 3c

This entry represents the nmap ACK scan of the external interface of the firewall.

```
# nmap (V. 2.54BETA22) scan initiated Mon Sep  9 12:09:20 2002 as: nmap -sA -P0 -v \
-oN /gcfw/fwscan1c-ack.out -g80 -n -p 1-65535 --max_rtt_timeout 500 --initial_rtt_timeout 250
85.10.12.66
All 65535 scanned ports on  (85.10.12.66) are: filtered

# Nmap run completed at Mon Sep  9 12:59:35 2002 -- 1 IP address (1 host up) scanned in 3015
seconds
```

---

* * *Results of Test 3d

This entry represents the nmap UDP scan of the external interface of the firewall.

```
# nmap (V. 2.54BETA22) scan initiated Mon Sep  9 13:02:05 2002 as: nmap -sU -P0 -v -oN
/gcfw/fwscan1d-udp.out -g80 -n -p 1-65535 --max_rtt_timeout 500 --initial_rtt_timeout 250
85.10.12.66
All 65535 scanned ports on  (85.10.12.66) are: filtered

# Nmap run completed at Mon Sep  9 13:58:54 2002 -- 1 IP address (1 host up) scanned in 3408
seconds
```

Results of Test 3e not shown, results same as 3a
Results of Test 3f not shown, results same as 3d
Results of Test 3g not shown, results same as 3a
Results of Test 3h not shown, results same as 3d
Results of Test 3i not shown, results same as 3a

Results of Test 3J not shown, results same as 3d

Results of Test 4 not shown, port 1521 reported as open, remainder filtered.
Results of Test 5 not shown, port 21 reported as open, remainder filtered.

Results of Test 6 not shown, non-existent machines reported all ports filtered, machines running telnet showed port 23 open, machines running ftp showed 21 open, Internal mail server reported 25 and 110 open, machines without these services showed ports as closed.
Results of Test 7 not shown, port 1521 reported as open, remainder filtered.
Results of Test 8 not shown, port 53 TCP and UDP reported as open, 80 and 443 reported as closed, remainder reported as filtered.
Results of Test 9a not shown, port 25 reported as open, port 113 reported as closed, remainder filtered.
Results of Test 9b not shown, port 25 reported as open, port 80, 113, and 443 reported as closed, remainder filtered.
Results of Test 12a not shown, all UDP ports show open, however, tcpdump traces on the external side of the firewall show only UDP port 123 allowed thorough.
Results of Test 12b not shown, all TCP ports reported as filtered.
Results of Test 13a and 13c not shown, all UDP ports show open, however tcpdump traces on the external side of the firewall show only UDP port 514 allowed through.
Results of Test 13b and 13d not shown, all TCP ports reported as filtered.
Results of Test 14 not shown, hping2 reported 100% packet loss.
Results of Test 15 not shown, hping2 reported 100% packet loss.
Results of Test 16 not shown, TCP port 1521 reported as open, TCP ports 80 and 443 reported as closed, all others reported as filtered.

---

* * *Results of Test 17

This entry represents a nmap Syn scan to port 113 all addresses within the 85.10.12.64/24 address space. The scanning position was external of the firewall. Not all entries are shown.

```
# nmap (V. 2.54BETA22) scan initiated Mon Sep  9 15:01:04 2002 as: nmap -sS -P0 -v \
-oN /gcfw/Ident17a-syn.out -n -p 113 --max_rtt_timeout 500 --initial_rtt_timeout 250 \
85.10.12.65-95
The 1 scanned port on  (85.10.12.65) is: closed
Interesting ports on  (85.10.12.66):
Port       State       Service
113/tcp    filtered    auth

Interesting ports on  (85.10.12.67):
Port       State       Service
113/tcp    filtered    auth

Interesting ports on  (85.10.12.68):
Port       State       Service
113/tcp    filtered    auth

The 1 scanned port on  (85.10.12.69) is: closed
```

---

* * *Results of Test 18

This entry represents an nmap Syn scan from the external interface of the firewall to the web server in the DMZ.

```
# nmap (V. 2.54BETA22) scan initiated Mon Sep  9 15:04:35 2002 as: nmap -sS -P0 -v \
-oN /gcfw/DMZWeb18-syn.out -n --max_rtt_timeout 500 --initial_rtt_timeout 250 85.10.12.68
Interesting ports on  (85.10.12.68):
(The 1540 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https


# Nmap run completed at Mon Sep  9 15:07:27 2002 -- 1 IP address (1 host up) scanned in 172
seconds
```

---

* * * Results of Test IntTrfa

These entries represent the packet traces taken with tcpdump of the traffic moving from the internal network to the external network. The tcpdump sniffer was positioned on the external side of the firewall. For brevity's sake, not all packets are shown.

```
-------------------------------------------------------------------------
Packet 1
TIME:   15:38:18.573885
  IP:     85.10.12.66 -> 85.10.12.75 hlen=20 TOS=00 dgramlen=44 id=D1A9
          MF/DF=0/1 frag=0 TTL=255 proto=TCP cksum=B06E
 TCP:   port 49994 -> http seq=2852898935 ack=0000000000
          hlen=24 (data=0) UAPRSF=000010 wnd=8760 cksum=461D urg=0
DATA:   <No data>
-------------------------------------------------------------------------
-------------------------------------------------------------------------
Packet 15
TIME:   15:52:43.153885 (11:0.780000)
  IP:     85.10.12.66 -> 85.10.12.75 hlen=20 TOS=00 dgramlen=40 id=2F59
          MF/DF=0/0 frag=0 TTL=40 proto=TCP cksum=69C4
 TCP:   port 24203 -> https seq=2987088034 ack=0000000000
          hlen=20 (data=0) UAPRSF=000010 wnd=2048 cksum=433B urg=0
DATA:   <No data>
-------------------------------------------------------------------------
-------------------------------------------------------------------------
Packet 19
TIME:   16:02:35.094888 (08:37.321003)
  IP:     85.10.12.66 -> 85.10.12.75 hlen=20 TOS=00 dgramlen=40 id=F5EE
          MF/DF=0/0 frag=0 TTL=40 proto=TCP cksum=A32E
 TCP:   port 24662 -> ntp seq=2987088034 ack=0000000000
          hlen=20 (data=0) UAPRSF=000010 wnd=2048 cksum=42B0 urg=0
DATA:   <No data>
-------------------------------------------------------------------------
-------------------------------------------------------------------------
Packet 25
TIME:   16:19:40.114888 (05:8.700000)
  IP:     85.10.12.66 -> 85.10.12.75 hlen=20 TOS=00 dgramlen=40 id=7740
          MF/DF=0/0 frag=0 TTL=40 proto=TCP cksum=21DD
 TCP:   port 25158 -> ftp seq=2987088034 ack=0000000000
          hlen=20 (data=0) UAPRSF=000010 wnd=2048 cksum=4126 urg=0
DATA:   <No data>
-------------------------------------------------------------------------
```

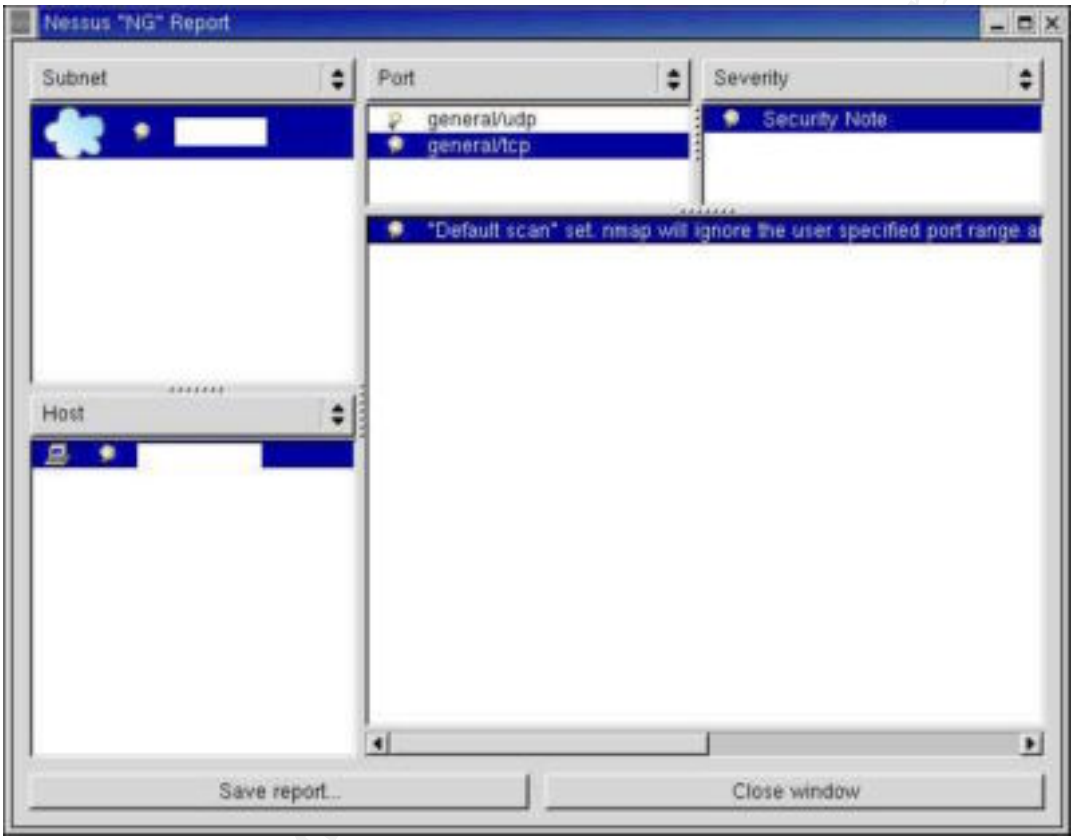
Results of Test IntTrfb

These entries represent the packet traces taken with tcpdump of the traffic moving from the internal network to the external network. The tcpdump sniffer was positioned on the external side of the firewall.

```
Packet 1
TIME:   17:36:15.282285 (35:33.790000)
  IP:     85.10.12.66 -> 85.10.12.75 hlen=20 TOS=00 dgramlen=28 id=B80D
          MF/DF=0/0 frag=0 TTL=44 proto=UDP cksum=DD10
```

UDP: port 28079 -> ntp hdr=8 data=0
DATA: <No data>

Results of Nessus Scan



The results of the Nessus scan showed no vulnerabilities. The only output was a security note for UDP and TCP showing the traceroute information, which was unable to discover the route to the firewall. There are **no further recommendations** for this test. (Addresses sanitized).

Analysis of Test Results with Recommendations

Analysis of Tests 3a through 3j

The results of this test were consistent with expectations for rule 3. There are **no further recommendations** regarding this test.

Analysis of Tests 4

The results of this test were consistent with expectations for rule 4. There are **no further recommendations** regarding this test.

Analysis of Tests 5
The results of this test were consistent with expectations for rule 5. There are **no further recommendations** regarding this test.
Analysis of Tests 6
The results of this test were consistent with expectations for rule 6. There are **no further recommendations** regarding this test.
Analysis of Tests 7
The results of this test were consistent with expectations for rule 7. There are **no further recommendations** regarding this test.
Analysis of Tests 8
The results of this test were consistent with expectations for rule 8, however this test also showed two additional closed ports not related to rule 8. These ports were TCP port 80 and TCP port 443. These ports are consistent with results which would be expected from rule 18. There are **no further recommendations** regarding this test.
Analysis of Tests 9a
The results of this test were consistent with expectations for rule 9, however, one additional port, TCP 113, reported as closed. This is consistent with results which would be expected from rule 17. There are **no further recommendations** regarding this test.
Analysis of Tests 9b
The results of this test were consistent with expectations for rule 9, however, three additional TCP ports, 80, 443, and 113, reported as closed. Ports 80 and 443 reporting as closed are consistent with expectations of rule 18. Port 113 reporting as closed is consistent with rule 17. There are **no further recommendations** regarding this test.
Analysis of Tests 12
After analysis of the tcpdump data, the results of the test were consistent with expectations for rule 12, parts a and b. There are **no further recommendations** regarding this test.
Analysis of Tests 13
After analysis of the tcpdump data, the results of this test were consistent with expectations for rule 13, all parts. There are **no further recommendations** regarding this test.
Analysis of Tests 14
The results of this test were consistent with expectations for rule14. There are **no further recommendations** regarding this test.
Analysis of Tests 15
The results of this test were consistent with expectations for rule 15. There are **no further recommendations** regarding this test.
Analysis of Tests 16
The results of this test were consistent with expectations for rule 16, however,

two additional TCP ports, 80 and 443, were reported as closed. This is consistent with results expected from rule 18. There are **no further recommendations** regarding this test.

Analysis of Tests 17

The results of this test were consistent with expectations for rule 17. All firewall protected entities reported filtered for TCP port 113, except for the DMZ email server, which reported as closed. There are **no further recommendations** regarding this test.

Analysis of Tests 18

The results of this test were consistent with expectations for rule 18. There are **no further recommendations** regarding this test.

Analysis of Tests IntTraf

The results of this test were consistent with expectations for rules 11, 19, 20, and 22. There are **no further recommendations** regarding this test.

Analysis of Test MapRules

The Checkpoint firewall did return a "TTL 0 during transit from ip=85.10.12.66 name=UNKNOWN" in response to receiving a packet with a ttl=1 value when used in conjunction with an allowed rule. This could be used to map or partially map the firewalls rule set. After the results of this test were compiled, a rule was added to the firewall as follows:

(firewall nodes) any time-exceeded drop

This had no effect on the results.

Recommendations: Block time exceeded messages from leaving the network at the border router.

Analysis of PING Test

The scanner reported 100% packet loss on all pings. There are **no further recommendations** regarding this test.

IV. Test under Fire

Attack 1 - Firewall Attack

Research conducted at http://cve.mitre.org during the week of August 4, 2002, on several popular commercial and free firewalls elicited the following in terms of vulnerabilities (includes candidates).

Firewall Product	No. Vulnerabilities
Checkpoint Firewall-1 / VPN-1	26
Cisco Pix	8
Symantec Axent Raptor	6
NAI Gauntlet	3
Iptables	2

Table 4.1

A good way to make your defenses stronger is to know your enemy. Although Checkpoint was chosen to protect GIAC Enterprises in this practical, this was also the firewall architecture chosen for this assignment. In the table above, Checkpoint has the highest number of vulnerabilities of the firewalls listed. Even so, on a fully patched and properly configured system, exploiting this firewall could prove to be challenging.

Of the 26 vulnerabilities listed for checkpoint (counting all versions / service packs listed) roughly 27% were denial of service attacks. Also, of the 26 vulnerabilities listed, at least 4, or about 15%, were exploitable on Checkpoint 4.1 SP5, all other vulnerabilities listed being directed against earlier service pack levels. The vulnerabilities are described below (the details were compiled from information on the online.securityfocus.com web site).

Vulnerability 1

CVE Info: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-089

BID Info: http://online.securityfocus.com/bid/725

Details: Involves Checkpoints support for LDAP
To exploit must have valid username / password on Firewall
Access may be granted to all protected network objects

Client Sign on must be setup in a specific manner

Vulnerability 2
CVE Info: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-1037
BID Info: http://online.securityfocus.com/bid/1662
Details: Involves Checkpoints Session Agent
Session Agent on firewall normally prompts client for authentication
Will prompt unlimited number of times allowing brute force attacks
Exploits are available

Vulnerability 3
CVE Info: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0940
BID Info: http://online.securityfocus.com/bid/3336
Details: Attacking hosts must already be permitted to view the log files with the GUI interface
May possibly allow execution of arbitrary code
Buffer overflow attack

Vulnerability 4
CVE Info: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0428
BID Info: http://online.securityfocus.com/bid/4253
Details: Clients may override timeout values on caching of credentials
Attacker must be able to read or write the users.C file

Three of the above attacks needed some type of previous authentication or access to the system in order to succeed. The brute force attack did not, but is a very noisy attack and if the authentication is tightly regulated using strong passwords could be very time consuming.

The practical I chose for this assignment was Todd Greenlaw's practical, http://www.giac.org/practical/Todd_Greenlaw_GCFW.zipHis network diagram is replicated below in Figure 4.1.

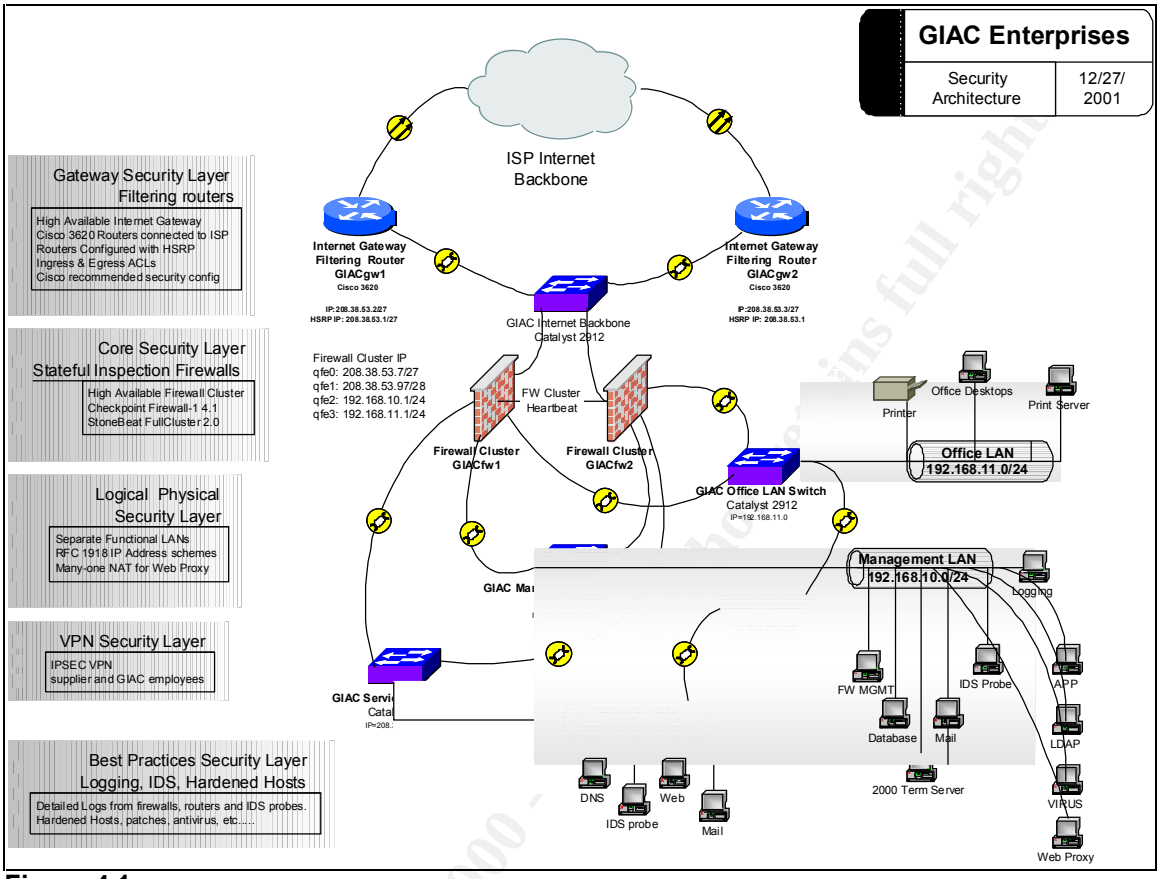


Figure 4.1

Upon examination of Todd's router configuration, it appears that ip unreachables are not turned off. Using this, it may be possible to use reverse network mapping to determine the firewall location. The conclusions here are hypothetical, since I did not have this exact configuration to test.

Todd drops all packets destined to his firewalls, but allows rejects to be sent out for the ident protocol for all systems protected by his firewall. Therefore, packets will be sent to port 113 in an attempt to map the live systems. The firewall should return a RST/ACK for all systems that it protects. Those addresses not having a corresponding system available should respond with "Destination Host Unreachable" from the router (this may depend upon if Todd has published ARP entries for all systems in the network range, or just the live systems). However, the firewall, configured to drop all packets destined to its own IP address, should not respond at all. Thus, using this technique, it may be possible to deduce (guess?) the firewalls location. The command is shown below.

nmap –sS –p 113 203.38.53.96-128

Because Todd drops all packets destined to his firewall, it would be much more difficult to determine the firewall product running on it. Social engineering is possibly the best bet at this point. An article posted on the SecurityFocus web site, http://online.securityfocus.com/infocus/1527, had this to say about social engineering: "Even for technical people, it's often much simpler to just pick up the phone and ask someone for his password. And most often, that's just what a hacker will do". In our case, however, we will pretend to be a research firm attempting to determine how many firewalls of "brand X" are used, and how satisfied the users are. With a small amount of persistence it should be possible to entice someone to expose the needed information.

There are two exploits available against Checkpoint's Session Agent which deals with session authentication for users. According to information on SecuriTeam's web site, http://www.securiteam.com/securitynews/5NP0F2A2AW.html, the session agent will respond with a "220 User x not found" if the user does not match an entry in the user database. Otherwise, a "331 *FireWall-1 password:" message will be returned, allowing an attacker to know when a correct user id was located. The session agent will continue to allow attempts for user ids and passwords indefinitely. There are two exploits available on the SecurityFocus site, http://online.securityfocus.com/bid/1662/exploit/, either of which could be attempted at this time.

Conclusion: This exploit would not be successful as Todd does implement a rule which forces session authentication. It would also be noisy and would probably be detected with little effort.

Attack 2 - DDoS Attack

Some of the DDoS tools in use today are TFN, TFN2K, Trinoo, and Stacheldraht, mstream, and shaft. An excellent analysis of TFN was written by David Dittrich (information presented here was gathered from his paper). TFN was authored by Mixter to execute on Unix systems. TFN employees the attackers which initiate the attack process by communicating with the clients. The clients then communicate with the daemons which carry out the attack. Attacks which are possible using TFN are ICMP floods, SYN floods, UDP floods and attacks utilizing Smurf techniques.

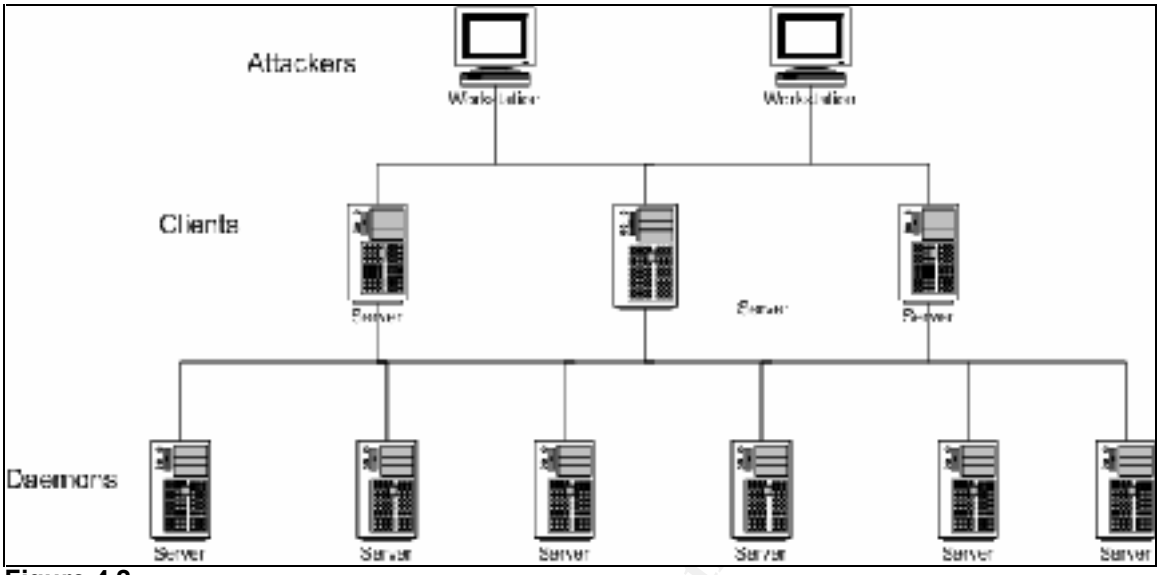


Figure 4.2

The DDoS attack chosen for this practical assignment is TFN, although any of the ones listed above would have had a severe impact on Internet traffic. It is assumed that I have gained control over 50 DSL connected PCs on the Internet, and installed the TFN daemon (td.c) on them, or at least have a list if 50 of these compromised systems. It is also assumed that I have installed the client on at least one or more Internet reachable systems. The attack type chosen would be a SYN flood to the web server, as this would constitute a double whammy. The sheer volume of traffic from the 50 systems would be enough to completely overwhelm the network connections, and the SYNs would soon fill the SYNDefender connection table on the Checkpoint firewall.

I could not find where Todd defined the speed of the lines from the ISPs. Assuming however, that the connection to the Internet was via T1 lines, 50 DSL modem connected systems would be more than enough to administer a serious denial of service attack against the network. The mathematics I used to deduce this is as follows (numbers are approximate).

Speed of a T1 in bits/sec = 1.54Mb/s x 1024 Kb/Mb x 1024 b/Kb = 1614808 b/sec

Referencing Chris Brenton's book Mastering Cisco Routers, pg. 76, the speed of an ADSL modem (upstream) ranges from 64-384Kbps. If we assume that most people run a bandwidth close to the mean of this (probably overly optimistic), we arrive at 224Kbps. Therefore, using this figure the speed of one ADSL modem connection will yield the following.

Speed of one ADSL modem = 224Kb/sec x 1024b/Kb = 229376 bits/sec

So fifty would yield 50 x 229376 bits/sec = 11468800 bits/sec.

If we divide this figure by the number of bits/sec in a T1, we see that it would take over 7 T1s to sustain this kind of traffic.

11468800 bits/sec / 1614808 bits/sec/T1 = 7.1 T1s

One obvious way to mitigate such an attack is to increase the bandwidth to T3s, BUT, an obvious way to counter is for the attackers to add more daemon systems. The point being this: if attackers want you bad enough, and they have enough patience and resources, it may not be worth the cost to mitigate the DoS attacks using this strategy.

A better strategy may be to work upstream of the attack on your ISPs network. Determine if it is possible to block the offending traffic on their network. Certainly using techniques to block IP spoofing from your network and broadcast packets coming into your network will help yours and other companies networks reduce the frequency and severity of these types of attacks, and this should be put into place by everyone.

Attack 3 - Internal System

Attacks against web servers are very common, and there are several ways to identify web servers to compromise. Tools such as whois, searching registration sites, or doing DNS lookups are some of the ways information may be gathered for targeting specific sites. For nonspecific targets, nmap may be used to scan for web servers by looking for services running on port 80.

It is possible to kick off a scan of network blocks using nmap. Using the following command, I could scan the entire Class B address range for web servers.

```
nmap -sS -P0 -p80 --randomize_hosts 203.38.*.*
```

This tells nmap to do a half-open scan to port 80 without pinging the hosts first to see if they respond. It also instructs nmap to randomize the hosts which are being scanned. This may make it slightly harder to detect, especially on smaller networks. The network range being scanned is 203.38.0.0 to 203.38.255.255. Nmap will compile a list of servers running services on port 80. It is quite possible, however, that this will be logged by IDS servers at the scanned site.

Running this at a slow pace over several days would be less noticeable.

Because of the information gathered thus far, it can be seen that a web server resides at 208.38.53.100. This can be verified by connecting to the HTTP port, possibly retrieving additional information from text returned in the headers. This can be used to determine the web server being utilized and possibly the version of the server. I could find no information on which web server was chosen to be implemented in Todd Greenlaw's site design, so let's for the sake of this practical assume that it would be Microsoft IIS version 5.0. I verify this information by running a sniffer, such as tcpdump, and looking at the contents of the returned packets. Within the packets I see "Server: Microsoft-IIS/5.0".

```
tcpdump -lexn -i eth0 port 80 | tcpshow -pp -cooked  \
-noHostNames > /tmp/junk
```

It is also possible to find out the version of IIS by telneting to port 80 of the server, typing in the following command, and pressing the enter key a couple of times.

```
telnet 208.38.53.100 80

HEAD / HTTP/1.0
```

At this point, the web can be searched for exploits against this version of IIS. For example, utilizing the http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl web with a keyword search for "IIS" on September 9, 2002 returned 50 vulnerabilities.

The attack chosen for this practical was "Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability". The information on this attack can be found at the http://online.securityfocus.com/bid/4525/info/ site.

CodeBrws.asp was written to allow viewing of the source of certain file types. This was intended to be used with the /IISSamples directory as the root directory, and it was not intended for ".." to be used within the URL. However, the script did not take into account the various Unicode representations of the ".." string. According to information obtained from this site, the CodeBrws.ASP does not filter Unicode thoroughly enough.

Attempting to run the command

```
http://www.giac.com/iissamples/sdk/asp/docs/CodeBrws.asp?Source=/IISSAMPLES/%c0%ae%c0%ae/default.asp
```

on Todd Greenlaw's site returns a **404 Not Found** message. Todd, as many good security administrators have done, recommended that GIAC's system administrators remove the sample scripts from the web servers.

References:

Books:

Brenton, Chris. Mastering Cisco Routers Cybex Inc., 2000.

Robert L. Ziegler. Linux Firewalls Second Edition New Riders Publishing, 2002.

Pomeranz, Hal, et al. The SANS Institure Solaris Security Step by Step Version 1.0, Deer Run Associates, 1999.

VPN-1/Firewall-1 Administration Guide, Check Point Software Technologies Ltd., 1999-2000.

Stevens, Richard. TCP/IP Illustrated, Volume 1. Addison Wesley Longman Inc, 1994.

VPN Concentrator User Guide. Altiga Networks, Inc., March 2000.

Welch, Daemon. Essential Checkpoint Firewall-1: an installation, configuration, and troubleshooting guide. Addison-Wesley, 2000.

Web sites:

Dana Graesser. 2001.
URL: rr.sans.org/firewall/router2.php

"Improving Security on Cisco Routers". 01 May 2002.
URL: www.cisco.com/warp/public/707/21.html

Foydor. "Quality Security Tools". 05 May 2002.
URL: http://www.insecure.org/tools.html

Deraison, Renaud. "The Nessus Project : Introduction".
URL: http://www.nessus.org/intro.html

Unknown. "Hping Home Page".

URL: http://www.hping.org/

Schiffman, Mike. “Firewalk”. 02 March 2001.
URL: http://www.packetfactory.net/Projects/Firewalk/

Foydor. “Nmap -- Free Stealth Port Scanner For Network Exploration & Security Audits. Runs on Linux/Windows/UNIX/Solaris/FreeBSD/OpenBSD”. 10 August 2002.
URL: http://www.insecure.org/nmap/index.html

Unknown. “NIDSbench”.
URL: http://packetstorm.widexs.nl/UNIX/IDS/nidsbench/nidsbench.html/

van der Kooij, Hugo. “Nessus F.A.Q.”. 29 April 2002.
URL: http://www.nessus.org/doc/faq.html#Q.OTHER.FIREWALL

Johnson, Greg. “Using Nessus and Nmap to Audit Large Networks” 19 December 2001.
URL: http://bengal.missouri.edu/~johnsong/audit/audit_files/frame.htm

Spitzner, Lance. “Auditing Your Firewall Setup”. 12 December 2000.
URL: http://www.enteract.com/~lspitz/audit.html

Farrow, Rik. “ICMP Stands for Trouble”. 09 May 2000.
URL: http://www.networkmagazine.com/article/NMG20000829S0003

St. Johns, Michael. “Identification Protocol”. February 1993.
URL: ftp://ftp.isi.edu/in-notes/rfc1413.txt

Unknown. “User Management”. 7 August 2002.
URL:http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/rel3_5_1/config/usermgt.htm#xtocid21

Dittrich, David. “The "Tribe Flood Network" distributed denial of service attack tool”. 21 October 1999.
URL: http://staff.washington.edu/dittrich/misc/tfn.analysis

Dittirch, David. “Distributed Denial of Service (DDoS) Attacks/tools”. 30 July 2002.
URL: http://staff.washington.edu/dittrich/misc/ddos/

Unknown. “SecurityFocus home vulns discussion: Microsoft IIS CodeBrws.ASP

Source Code Disclosure".
URL: http://online.securityfocus.com/bid/4525/discussion/

Duchemin, Gregory. "SecuriTeam.com &#153 (Firewall-1 Session Agent vulnerable to dictionary attack)". 16 August 2000.
URL: http://www.securiteam.com/securitynews/5NP0F2A2AW.html

Unknown. "SecurityFocus home vulns exploit: Check Point Firewall-1 Session Agent Dictionary".
URL: http://online.securityfocus.com/bid/1662/exploit/

Unknown. "Firewall-1 Home".
URL: http://www.checkpoint.com/products/protect/firewall-1.html

Ruiu, Dragos. "Snort FAQ". Version 1.4. 24 March 2002.
URL: http://www.snort.org/docs/faq.html#3.1

Reuters. "Mercury News | 02/14/2002 | Cisco gains 4th-qtr market share". 14 February 2002.
URL:http://www.siliconvalley.com/mld/siliconvalley/business/companies/cisco/2672314.htm

Unknown. "Isolate the Web server from public and internal networks" 12 June 2000.
URL: http://www.cert.org/security-improvement/practices/p075.html

Rekhter, Y., et al. "Address Allocation for Private Internets ". February 1996.
URL: ftp://ftp.isi.edu/in-notes/rfc1918.txt

Havrilla, Jeffrey. "CERT/CC Vulnerability Note VU#484011". 31 August 2002.
URL: http://www.kb.cert.org/vuls/id/484011

Unknown. "SecurityFocus HOME Vulns Info: Ntpd Remote Buffer Overflow Vulnerability".
URL: http://online.securityfocus.com/bid/2540

Hernan, Shawn. "CERT/CC Vulnerability Note VU#18287". 25 June 2001.
URL: http://www.kb.cert.org/vuls/id/18287

Rafail, Jason and Havrilla, Jeffrey. "CERT/CC Vulnerability Note VU#63581". 14 May 2002.
URL: http://www.kb.cert.org/vuls/id/635811

Rafail, Jason. “CERT/CC Vulnerability Note VU#161931”. 13 May 2002.
URL: http://www.kb.cert.org/vuls/id/161931

Postel, J. “Transmission Control Protocol”. 1 September 1981.
URL: ftp://ftp.isi.edu/in-notes/rfc793.txt

Ramakrishnan, K. “The Addition of Explicit Congestion Notification (ECN) to IP”. September 2001.
URL: ftp://ftp.isi.edu/in-notes/rfc3168.txt

Unknown. “CAN-1999-0089 (under review)”.
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-089
Unknown. “CVE-2001-0940”
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0940

Unknown. “CAN-2002-0428 (under review)”.
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0428

Unknown. “CAN-2000-1037 (under review)”.
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-1037

Greenlaw,Todd.
URL: http://www.giac.org/practical/Todd_Greenlaw_GCFW.zip

Unknown. “SecurityFocus HOME Vulns Info: Check Point Firewall-1 LDAP Authentication Vulnerability”
URL: http://online.securityfocus.com/bid/725

Unknown. “Check Point Firewall-1 Session Agent Dictionary Attack Vulnerability”.
URL: http://online.securityfocus.com/bid/1662

Unknown. “Check Point Firewall-1 GUI Log Viewer Vulnerability”.
URL: http://online.securityfocus.com/bid/3336

Unknown. “Check Point FW-1 SecuClient/SecuRemote Client Design Vulnerability”
URL: http://online.securityfocus.com/bid/4253