Global Information Assurance Certification Paper

SANS GFCW PRACTICAL ASSIGNMENT

Firewalls, Perimeter Protection and VPNs
Version 1.7

GIAC Enterprises
A fortune cookie saying e-business

By Brian States

TABLE OF CONTENTS

Introduction

GIAC Enterprises is a small business in a unique niche market of providing online retailing of fortune cookie sayings. Through steady business growth, the company has had opportunity to implement a number of network security improvements. However the recent downturn in the economy has had the president of the company watching expenses closely. As a result, the IT staff must operate with the existing equipment and only a small budget for upgrades while maintaining the critical infrastructure needed to operate a successful e-business.

1. SECURITY ARCHITECTURE

1.1 Requirements

GIAC Enterprises has typical requirements for an e-business. In selling their fortune cookie sayings, they must be accessible to the public on the internet while also providing their employees, partners and suppliers the access they need to service the customers' requests and create new sayings that make the business profitable.

1.1.1 Customers

To maintain its profitability and integrity with its customers, GAIC Enterprises must maintain uninterrupted web access and secure the customers' information. Any down time of its web server results in a loss of sales and, potentially, customers. A compromise of customer data will result in a loss of confidence in the company by its customers and have a potential long-term consequence on the company.

Fortune cookie sayings are available in several languages by GIAC Enterprises and a customer is allowed to browse the selections of cookie sayings and make their purchase on line with the use of a credit card. Details of the transaction such as name, address, email address and credit card number are entered at the time of purchase and are secured across the internet by using an SSL enabled browser. This ensures that the connection between the customer's browser and server is encrypted. The customer is also able to verify the authenticity of the GIAC Enterprises website through a VeriSign digital certificate.

Once the payment is confirmed, a login and password are generated and sent to the customers email address. This allows the customer to access their selected sayings for download to their system or track their order. Email is also available to the customers to submit their questions and general correspondence to the GIAC staff.

1.1.2 Suppliers

GIAC Enterprises has contracted with several Chinese fortune cookie writers from Taiwan to supply their fortune cookie sayings. These suppliers access a private web server accessible only via a VPN. The writer uses VPN client software to establish an encrypted connection between their PC and the GIAC Enterprises firewall. Once connected, the writers can upload their current work, edit previous submissions and retrieve email.

1.1.3 Partners

GIAC Enterprises works with two types of partners: They have a number of partners that translate the fortune cookie sayings into other languages such as Spanish, French, German, Italian and Russian. They also work with several large printing companies to have orders printed and shipped to the customers that have chosen this option over down loading the sayings.

The translation partners access the information they need from a private web server accessible only via a VPN. They log into the same server as the suppliers to obtain the recent submissions and begin translating and updating the sayings. These partners are individual translators that connect using client VPN software to encrypt their connection from their PC to the GIAC firewall. Once connected, the translators can upload their current work, edit previous submissions and retrieve email

The printing partners are several large printing firms chosen as partners based on their quality and speed in providing a printed product to the customer. These partners use a firewall-to-firewall VPN between them and the GIAC firewall so the GIAC employees can upload the customer order information directly to the printing partners' servers.

1.1.4 GIAC Enterprises local employees

A small group of GIAC employees maintains the various servers and infrastructure needed to facilitate the day-to-day operations of the company. The employee's function within the company determines their access to the various servers in the company and the services they are allowed to use on the internet.

All employees have access to the mail server, can resolve DNS on the DNS server and access the web through a web proxy server. Customer service and sales employees have additional access to the customer database server and access to the partners through the VPN to either upload data using FTP or HTTP(S) based on the type of server of the partner site. Server administrators require SSH access to the servers both internally and on the DMZ for maintenance of the systems. The IT staff also requires SSH, and telnet to the network infrastructure along with managing a syslog server and time server for the network.

GIAC Enterprises has a strict internet use policy and the employees have signed this policy as a condition of their employment and also understand that they are subject to monitoring. The President of the company has taken it upon himself to make sure everyone is trained on the basic security practices with email, passwords, etc. and has the IT staff brief various aspects of network security at the quarterly corporate meetings.

1.1.5 GIAC Enterprises mobile employees

There is occasional travel by the local sales staff and President of the company along with several sales employees overseas. These employees require the same system access as they have at the corporate office. This is accomplished with company-supplied laptops with firewall software and anti-virus software loaded and maintained by the company IT staff. These employees connect to the systems using client VPN software to encrypt their connection from their PC to the GIAC firewall. Once the employees are connected, they can upload sales information, retrieve customer and customer sales information, retrieve email, and perform other required duties.

1.1.6 Table 1: Summary of user access requirements

Group	Requirement	Service	Port
Customers	Access into public web server	HTTP HTTPS	TCP 80 TCP 443
Suppliers	VPN access into web applications, email and file transfer	HTTP HTTPS FTP SSH	TCP 80 TCP 443 TCP 20/21 TCP 22
Partners	VPN access into web applications, email and file transfer	HTTP HTTPS FTP SSH	TCP 80 TCP 443 TCP 20/21 TCP 22
All Employees	Out to the internet via web proxy	HTTP HTTPS	TCP 80 TCP 443
Customer service & sales	Upload and download files with partners and suppliers	FTP SSH	TCP 20/21 TCP 22
Server Administrators	Secure access into external servers	SSH	TCP 22
IT Administrators	Access out to network equipment	SSH Telnet	TCP 22 TCP 23
Mobile Employees	VPN access into applications, and servers for email, file transfer, database access, and Microsoft services	HTTP HTTPS FTP SSH DNS SQL	TCP 80 TCP 443 TCP 20/21 TCP 22 UDP 53 TCP 1521

1.1.7 Table 2: Summary of system access requirements

System	Requirement	Service	Port
Mail servers	Send and receive mail from the internet	SMTP	TCP 25
Web servers	Provides Web pages to the internet	HTTP HTTPS	TCP 80 TCP 443
DNS servers	Receives and responds to DNS queries and updates	DNS	TCP 53 UDP 53
Web servers	Query data from database	SQL	TCP 1521
GIAC systems	Access to log server	Syslog	UDP 514
Time servers	Access to internet time server	NTP	UDP 123

1.2 Architecture

1.2.1 Overview

GIAC Enterprises security architecture, Figure 1, consists of zones to segregate the various levels of security risk based on its exposure to the internet and the type of traffic that is expected in that zone. Various types of access control and intrusion detection devices are placed in each zone to provide defense in depth against internal and external threats. These devices include a perimeter router and a firewall, with VPN capability, configured to create the zones of defense.

1.2.2 Router

The border router is a Cisco 2600 series router running IOS 12.2. It is configured to provide the first line of defense to the network through the use of its access control list capability. The access control list has been defined to filter source and destination IP addresses to reduce the risk of address spoofing attacks of the local network IP address and to filter the private, reserved multicast and other prohibited IP addresses. Because of the routers fast and efficient processing of packets, these attacks can be quickly mitigated. Properly configured, this router will also help defend the firewall against a denial-of-service attack.

1.2.3 Firewall and VPN

The firewall is a Check Point Firewall-1, Next Generation version, with Feature Pack 2 loaded. It is running on a hardened Sun Ultra 60 with Solaris 8 installed. It is configured with a quad ethernet network interface card to allow the creation of the access zones in the firewall for separation of traffic. Management understood that there were some security issues with Check Point. However, they decided that these were minor in comparison to the business need for ease of use by the IT staff.

The VPN option was included with the Check Point software purchase. It was determined that it is best to have a VPN that integrates with the firewall, preventing the introduction of "holes" in the firewall to facilitate VPN support and for the ease of use. Combining VPN with the firewall also provides access control at the perimeter firewall. It is able to prevent unauthorized users from even entering into the network before being filtered off by the firewall. It thus allows partners and suppliers to authenticate and connect to the application server to either download or upload required data.

Leveraging the ability of the Sun Ultra 60 to have multiple network interface connections, it was configured to create the various security zones off of these interfaces. Traffic arriving on the outside interface of the system is routed to the correct interface after being inspected by the firewall software. The other interfaces create the public screened subnet, the partner/supplier screened subnet and the internal subnet.

The public screened subnet contains the public web server, mail relay server and DNS server. Even with the firewall limiting the type of traffic to those servers, their exposure to the universe increases their risk of being attacked and compromised. This creates the need for its isolation on a separate subnet. The partners/suppliers screened subnet has limited access to specific services and users who have gained a certain trust level due to their cooperative relations with GIAC. Despite the cooperative relationship and legal contracts outlining the network connections and requirements, GIAC cannot fully trust these outside, 3rd party, users. As a result GIAC Enterprises has separated them into their own subnet, with a web and web mail server providing them with the additional information and access they need to interface with GIAC Enterprises. Should the partners or suppliers network be compromised for any reason, the impact to the GIAC network would be contained to that screened subnet.

Access to the internal network is strictly limited. Only connections and services required to facilitate the operation, management and maintenance of the servers in the screened subnets are allowed and should originate from the internal network, if possible. Access to the universe from the internal network is restricted by type and user and must also originate from the internal network. Access by the mobile employees is regulated by a VPN and services limited to the specific protocols and systems that are needed to conduct business while away from the local network.

The internal servers and employees currently reside on the same internal network. The internal risk of compromise and attack has been greatly minimized with the firewall policy. However, these systems are at an increased risk from the internal threat. This has not been a factor yet for GIAC Enterprises due to their small company size and staff. However, the company has had steady growth that will result in additional employees in the near future. As a result, the IT staff has requested funds to purchase an internal firewall to further protect the servers from attack and provide greater defense in depth. However, management has placed that request on hold. Until the funds are made available, the

President of the company has insisted that the IT staff and system administrators follow industry standard best practices in maintaining the servers. This includes daily log audits, password verification and patch maintenance.

1.2.4 IDS

To monitor any suspicious network activity on the public screened subnet, the partner/supplier screened subnet and the internal network, network intrusion detection systems are employed. These systems are Microsoft Windows 2000 running ISS Real Secure 7.0. Host based intrusion detection is also deployed on the public web server in the public screened subnet. The IT staff has plans to expand the use of host based IDS on all the critical servers in the screened subnets and internal network in the near future.

1.2.5 Addressing

GIAC Enterprises' has been assigned a class C IP address range. For use in this document the private class C IP address of 192.168.1.0 will be used. GIAC Enterprises network access provider has assigned an address for the external interface of the GIAC Enterprises' boarder router represented with the non-routable address of 192.168.250.250. By using a subnet mask of 255.255.255.192 on the IP address range of 192.168.1.0 – 192.168.1.255 the GIAC address space has been subdivided into 4 subnets and used in the various security zones:

GIAC external network	192.168.1.0 – 192.168.1.63
GIAC public subnet	192.168.1.64 – 192.168.1.127
GIAC partner/supplier subnet	192.168.1.128 – 192.168.1.191
GIAC Internal network	192.168.1.192 – 192.168.1.255

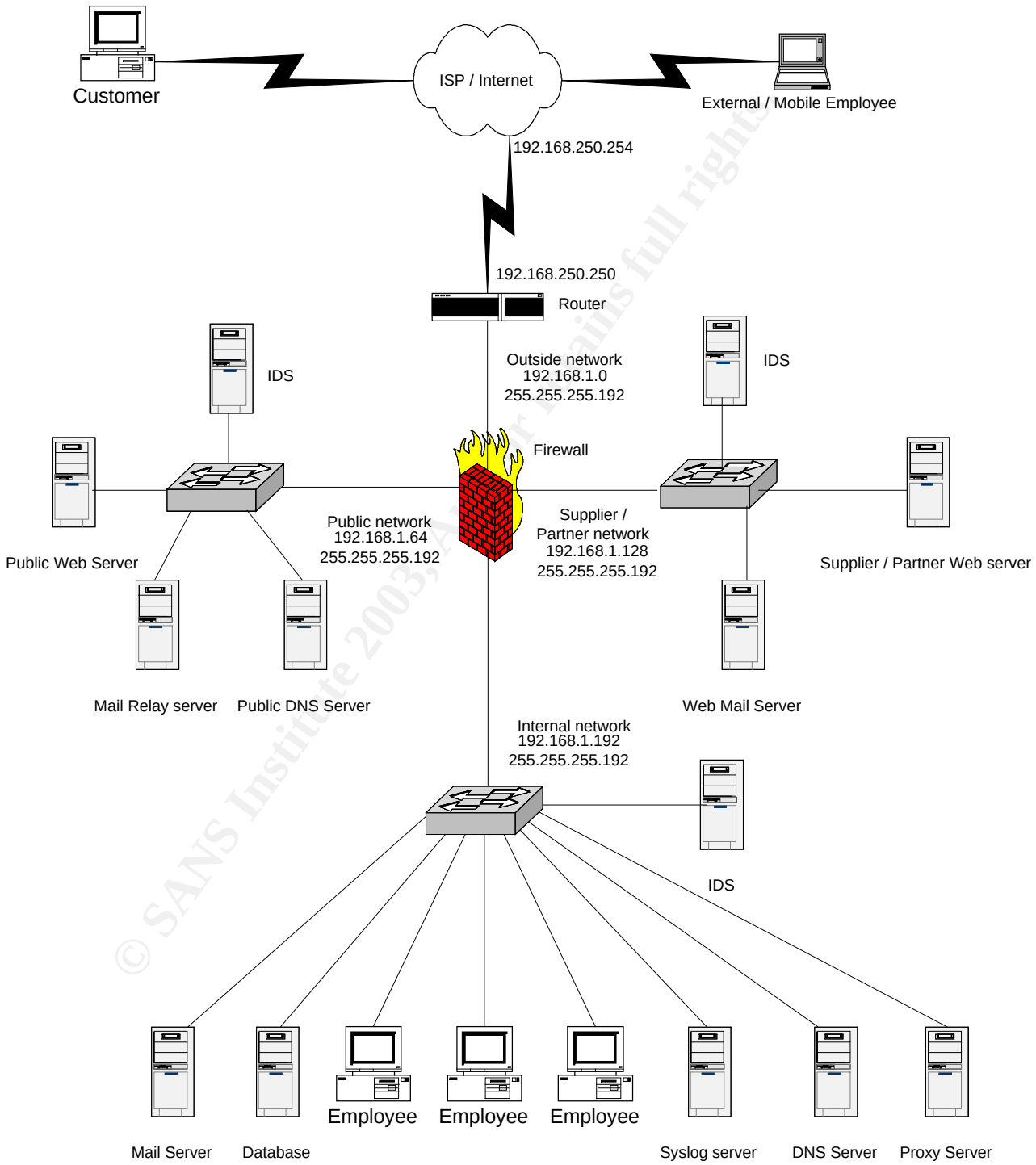
Key systems are assigned the following addresses from these ranges:

Router external interface	192.168.250.250
Router internal interface	192.168.1.1
Firewall external interface	192.168.1.2
Firewall public subnet interface	192.168.1.65
Firewall partner/supplier interface	192.168.1.129
Firewall internal interface	192.168.1.193
Public subnet IDS	192.168.1.66
Public DNS server	192.168.1.67
Public mail relay server	192.168.1.68
Public web server	192.168.1.69
Supplier/partner subnet IDS	192.168.1.130
Supplier/partner web server	192.168.1.131
Supplier/partner subnet IDS	192.168.1.132
Internal subnet IDS	192.168.1.194

Internal DNS server	192.168.1.195
Internal mail server	192.168.1.196
Internal syslog server	192.168.1.197
Internal proxy server	192.168.1.199
Internal database server	192.168.1.200
Workstations IT staff	192.168.1.208 – 215
Workstations System admin	192.168.1.216 – 223
Workstations customer service/sales	192.168.1.224 - 239
Workstations other employees	192.168.1.240 - 254

Figure 1

GIAC Enterprises Network Diagram



The actual IP addresses for the GIAC Enterprises network have been represented with the non-routable address from the private 192.168.x.x address range.

2. SECURITY POLICY

GIAC Enterprises considers all information as proprietary and has set a basic security policy accordingly. This policy is to deny access to the information unless access has been specifically authorized for a business need. It is the authorized access that determines the requirements for configuration and permissions that are put in place on the systems and infrastructure. Failure to fully implement this policy throughout the network results in a weakness of the network and a potential failure to defend the information against attack.

2.1 Border router configuration

The border router is the first line of defense in the GIAC perimeter to handle the traffic from the internet. It is important to leverage its ability to filter traffic with access-lists to eliminate unwanted traffic from entering the network. The Cisco IOS provides this filtering capability and includes a number of commands and settings that allow the administrator to configure the system so that it efficiently handles the traffic and also protects the router to ensure that it is not easily compromised.

2.1.1 Router security policy

The access control list (ACL) on the router must be defined to provide basic security to the network as defined in the GIAC policy. It must ensure that the critical network services do not enter or leave the network. Thus providing an additional layer of defense to the firewall. It is also critical that the router verify that packets conform to proper configuration for traffic flow regardless of protocols used. Proper ingress and egress filtering regulate this. Such as:

- No source-routed packets are permitted.
- No traffic using loopback, private or reserved addresses.
- No DHCP auto-configuration and multicast addresses.
- All traffic originating internally must have an internal address as the source only, and no traffic originating externally may have an internal address as the source address.

To verify the filtering provided by the ACL's and to monitor for malicious activity, it is essential that the ACL's be logged. Due to limitations in the routers logging capabilities, it must be configured to log to a syslog server on the GIAC intranet.

2.1.2 Router ACL

The following lines setup the basic global configuration of the router, including passwords and services:
service password-encryption

```
service linenumber
no service udp-small-servers
no service tcp-small-servers
!
hostname GIAC
!
logging trap debug
enable secret 5 $1$H71W$tM/1smWK6YoggHMOVwWb90
enable password 7 062A2E324D401A4957
!
!
no ip subnet-zero
no ip source-route
no ip domain-lookup
no cdp run
no ip finger
no ip source route
no ip bootp server
no ip http server
no ip domain
no ntp master
no logging console
no snmp
!
```

Define where to send the logs:

```
logging 192.168.1.197
!
```

Set up the router interfaces including IP address, services and access list to be used:

```
interface FastEthernet 0/0
description LAN connection
ip address 192.168.1.1
ip access-group 101 in
no ip directed-broadcast
no ip redirects
no ip proxy-arp
no ip mroute-cache
ntp disable
no cdp enable
duplex auto
speed auto
!
interface serial0/0
no ip address
no ip direct-broadcast
```

```
no ip mroute-cache
shutdown
!
interface FastEthernet 0/1
description connection to ISP
ip address 192.168.250.250
ip access-group 101 in
ip access-group 102 out
no ip directed-broadcast
no ip redirects
no ip unreachables
no ip proxy-arp
no ip mroute-cache
ntp disable
no cdp enable
duplex auto
speed auto
```

Define the routes:

```
ip route 0.0.0.0 0.0.0.0 192.168.250.254
ip route 192.168.1.64 255.255.255.192 192.168.1.2
ip route 192.168.1.128 255.255.255.192 192.168.1.2
ip route 192.168.1.192 255.255.255.192 192.168.1.2
```

Define the systems allowed to the router:

```
access-list 10 permit 192.168.1.210
access-list 10 permit 192.168.1.211
!
access-list 20 deny 0.0.0.0 255.255.255.255
!
```

Define the list of IP addresses and services to permit or deny on the router interface:

```
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 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny ip 255.0.0.0 0.255.255.255.any log
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 240.0.0.0 0.255.255.255 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 5.0.0.0 0.255.255.255 any log
access-list 101 deny ip 7.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 23.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 27.0.0.0 0.255.255.255 any log
access-list 101 deny ip 31.0.0.0 0.255.255.255 any log
access-list 101 deny ip 36.0.0.0 1.255.255.255 any log
access-list 101 deny ip 39.0.0.0 0.255.255.255 any log
access-list 101 deny ip 41.0.0.0 0.255.255.255 any log
access-list 101 deny ip 42.0.0.0 0.255.255.255 any log
access-list 101 deny ip 58.0.0.0 1.255.255.255 any log
access-list 101 deny ip 60.0.0.0 0.255.255.255 any log
access-list 101 deny ip 70.0.0.0 1.255.255.255 any log
access-list 101 deny ip 72.0.0.0 7.255.255.255 any log
access-list 101 deny ip 83.0.0.0 0.255.255.255 any log
access-list 101 deny ip 84.0.0.0 3.255.255.255 any log
access-list 101 deny ip 88.0.0.0 7.255.255.255 any log
access-list 101 deny ip 96.0.0.0 31.255.255.255 any log
access-list 101 deny ip 197.0.0.0 0.255.255.255 any log
access-list 101 deny ip 222.0.0.0 1.255.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log 0
access-list 101 deny ip 192.168.1.0 0.0.0.255 any log
access-list 101 deny ip host 192.168.1.1 any log
access-list 101 deny ip host 192.168.1.2 any log
access-list 101 deny icmp any any
access-list 101 deny tcp any any eq 113
access-list 101 deny ip any any range 135 139 log
access-list 101 deny ip any any eq 445 log
access-list 101 deny ip any any eq 1521 log
access-list 101 deny ip any any eq 2000 log
access-list 101 deny ip any any eq 2001 log
access-list 101 deny udp any any eq snmp log
access-list 101 deny udp any any eq snmptrap log
access-list 101 permit ip any 192.168.1.0 0.0.0.255
access-list 101 deny ip any any log
!
```

Define the list of IP addresses and services to permit or deny on the router interface:

```
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.16.0.0 0.15.255.255 any log
access-list 102 deny ip any 10.0.0.0 0.255.255255 log
access-list 120 deny ip any 172.16.0.0 0.15.255.255 log
access-list 102 deny ip 127.0.0.0 0.255.255.255 any log
access-list 102 deny ip 169.254.0.0 0.0.255.255 any log
access-list 102 deny ip 224.0.0.0 31.255.255.255 any log
access-list 102 deny ip 255.0.0.0 0.255.255.255 any log
access-list 102 deny ip 0.0.0.0 0.255.255.255 any log
access-list 102 deny ip 240.0.0.0 0.255.255.255 any log
access-list 102 deny ip host 0.0.0.0 any log 0
```

```
access-list 102 deny ip any any range 135 139 log
access-list 102 deny ip any any eq 445 log
access-list 102 deny ip any any eq 1521 log
access-list 102 deny icmp any any log
access-list 102 permit ip 192.168.1 0.0.0.255 any
access-list 102 deny ip any any log
!
```

Define the router login warning banner:

```
banner motd ^C WARNING: authorized access only.  Use without permission or in excess of authorization is consent to monitoring for prosecution. ^C
!
```

Setup the access to the router:

```
line con 0
transport input none
line aux 0
access-class 20 in
line vty 0 4
access-class 10 in
password 7 062A2E324D401A4957
login
exec-timeout 2
!
end
```

2.2 Firewall

The firewall has the major role in properly regulating traffic according to the security policy and requirements. The Check Point NG Firewall-1 provides this effectively and also meets the business requirement of ease of use and configuration. Loaded on a hardened Solaris 8 server, it is important to leverage the capabilities of the firewall to effectively control the network traffic through the firewall rules and configuration.

2.2.1 Firewall security policy

The firewall rules must be configured so that only specific required services are permitted to or from a specific server or network and all other traffic is denied. The critical rules on the firewall must also be logged for malicious activity. These include any rule that allows access from the universe or any drop or reject rules.

It is also important that the proper configuration and rules be established on the firewall to verify that packets conform to proper configuration for traffic flow regardless of protocols used. Anti-spoofing configuration on Check Point ensures that all traffic originating internally must have an internal address as the source only, and no traffic originating externally may have an internal address as the source address. Additional rules must be

configured to ensure that traffic using loop-back, private, reserved or multicast addresses is dropped.

The firewall's configuration/default settings must also be checked to ensure that selections external to the policy's rule base do not enable traffic to bypass the rules.

2.2.2 Firewall rules

In order to maximize performance, the firewall rules are ordered according to security requirements first, then the expected amount of traffic matching those rules.

No.	Source	Destination	Service	Action	Comment
1	Hot list	Any	Any	Drop & log	Deny access from sites that has had malicious activity. Also include private and reserved IP addresses.
2	Any	Hot list	Any	Drop & log	Deny access to sites that has had malicious activity. Also include private and reserved IP addresses.
3	Any	Public web server	TCP 80 TCP 443	Accept & log	Allow HTTP and HTTPS to public web server.
4	Any	Public DNS server	UDP 53	Accept & log	Allow external queries to public DNS server.
5	Any	Public mail server	TCP 25	Accept & log	Allow SMTP access to mail relay server.
6	Public mail server	Internal mail server	TCP 25	Accept & log	Allow SMTP to be relayed to internal mail server.
7	Internal DNS server	Public DNS server	UDP 53	Accept & log	Allow internal DNS server to make queries.
8	Internal proxy server	Any (not GIAC networks)	TCP 80 TCP 443	Accept & log	Allow HTTP and HTTPS from proxy server.
9	Internal mail server	Public mail server	TCP 25	Accept & log	Allow SMTP to be relayed from internal mail server.

10	Public DNS server	Any (not GIAC networks)	UDP 53	Accept & log	Allow public DNS server to make queries to universe.
11	Public mail server	Any (not GIAC networks)	TCP 25	Accept & log	Allow SMTP access from mail relay server.
12	GIAC systems	Internal syslog server	UDP 514	Accept & log	Allow external, public and partner/supplier networks to log to internal syslog server.
13	External DNS server	Time server X Time server Y	UDP 123	Accept & log	Allow public DNS server to act as the public screened subnet time server.
14	Time server	Time server X Time server Y	UDP 123	Accept & log	Allow internal DNS server to act as the time server for all non public systems.
15	External net & Partner/supplier net	Time server	UDP 123	Accept & log	Allow systems to access time server.
16	Public web server & partner/supplier web server	Internal database server	TCP 1521	Accept & log	Allow external web systems to access internal database server.
17	Partner/supplier mail server	Internal mail server	TCP 1037 TCP 1038	Accept & log	Allow partner/ supplier web mail server to access internal mail server.
18	Partners/suppliers VPN	Partners/suppliers web and email server	TCP 80 TCP 443 TCP 20 TCP 21 SSH 22	Accept, encrypt, decrypt & log	Allow suppliers and partners access to web and mail servers
19	Customer service/sales net	Partners/suppliers via VPN	TCP 20 TCP 21 SSH 22	Accept & log	Allow staff out to partners that require a VPN
20	Customer service/sales net	Partners/suppliers	TCP 20 TCP 21 SSH 22	Accept & log	Allow staff out to other partners.
21	Mobile employees VPN	Internal net	TCP 20 TCP 21	Accept, encrypt,	Allow mobile employees access to

			SSH 22 UDP 53 TCP 80 TCP 443 TCP 1521 Netbios Microsoft exchange	decrypt & log	all services available to internal users.
22	Server administrators	Public, and partner/supplier networks	SSH 22	Accept & log	Allow server administrators access external servers
23	IT staff net	External, public, and partner/supplier networks	SSH 22 Telnet 23	Accept & log	Allow network administrators access to external network equipment.
24	Firewall administrators	Firewall	SSH 22	Accept & log	Allow firewall administrators to the firewall OS
25	Any	Any	Any	Drop & log	Clean up rule

2.3 VPN

GIAC Enterprises determined it was best to use the integrated Check Point VPN-1 that is available with the Firewall-1 software. This integrated firewall functionality presents a complete security package. This was also determined by GIAC Enterprises to be best for preventing the introduction of "holes" in the firewall, to facilitate VPN support, and for the ease of use. Combining VPN together with the firewall for user access provides control at the perimeter firewall thus prohibiting users beyond the firewall prior to authentication.

By requiring all VPN's to decrypt at the firewall for both client and firewall-to-firewall VPN's, GIAC Enterprises also ensures that the firewall has an opportunity to limit the protocols passing through the firewall and that the network IDS has an opportunity to "screen" the traffic on the network.

2.3.1 VPN firewall encryption configuration

To enable the use of VPN's within GIAC Enterprises, Check Point requires that an encryption domain be defined. The encryption domain is the area within the network that is to be protected by the VPN. The GIAC firewall administrators included the internal server subnet and the suppliers/partners network in the group GIAC_VPN and used it with in the firewall VPN configuration as the encryption domain. GIAC Enterprises has chosen IKE as its standard method of encryption. The IKE configuration requires selection of

encryption algorithm(s) e.g. DES and 3DES, hash algorithm e.g. SHA1 and/or MD5, and authentication method e.g. shared secret or alternative PKI certificates. The firewall administrators prefer to use 3DES, MD5, with a pre-shared secret. However, specifics of VPN implementation firewall-to-firewall vary depending on the details of the firewall used by the partner/supplier organization. These properties are configured in the Check Point object representing the partner/supplier's firewall.

The VPN parameters for the firewalls are set in the firewall object properties VPN tab, including time intervals for renegotiating IKE and IPSEC security associations. Figure 2.

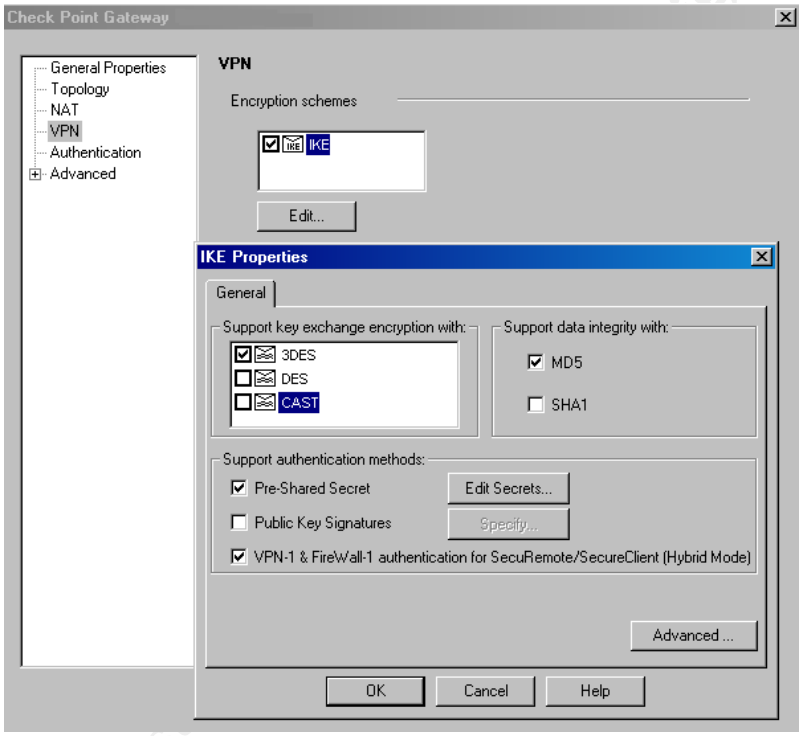


Figure 2: VPN settings

2.3.2 VPN client configuration

Check Point provides the SecuRemote software for use in implementing the client VPN solution. To prevent the user's desktop from being a weakness in the parameter defense, the firewall administrators have limited the traffic that is allowed into the networks from the VPN's and have also loaded personal firewalls on mobile employees' PC's. They have evaluated the Check Point SecureClient software that has the ability to impose a desktop security policy on the installed client firewall. However, due to the small user base and good accountability of those users, they have determined that the inexpensive personal firewalls currently used are adequate for their environment. For the partners and suppliers, GIAC Enterprises' holds them accountable for securing their client workstations through the contract agreements and has incorporated the right to terminate the contract and hold

them liable for breach of security if it is found that malicious activity has originated from them as a result of poor security practices.

The SecureClient software was installed and configured by the firewall administrators on the mobile employees PC's. This software was also provided to the partners and suppliers for their use with configuration documentation.

2.3.3 User authentication

There are several types of authentication methods available on the firewall. These include SecureID, Radius, TACACS, s/key and others. These options have been considered as better methods of VPN security and control by the IT staff of GIAC Enterprises. However, due to the expense of such systems and software, this is currently not an option. As a result, the VPN-1 and Firewall-1 password management capability of the Check Point firewall is currently used. It is a simple username and password system that has the potential for problems such as weak passwords, no password aging or other types of controls associated with other access methods. But with the small user base that GIAC Enterprises has for its VPNs, it currently best suits their business needs.

GIAC VPN users are created under manage -> users in the Firewall-1 software. Each user is provided a unique user ID and login, and the encryption properties, including the authentication and encryption scheme, which must be set. The user must also be assigned to a group based on their required access needs. It is this group that is then used in the firewall rule set. Figure 3.

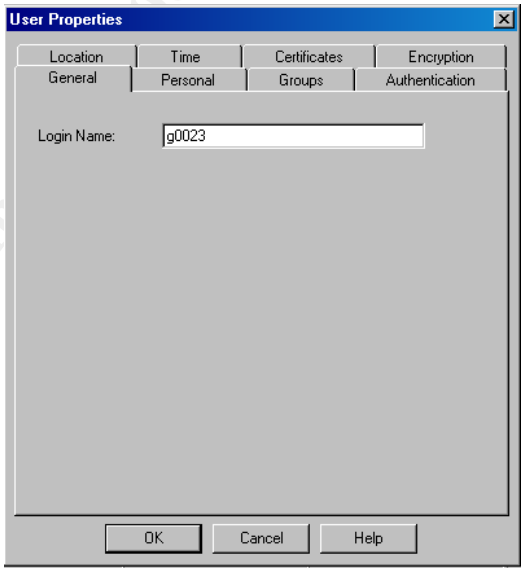


Figure 3: User settings

2.3.4 VPN firewall rule configuration

The basic Check Point VPN rule policy has the following format.

Source	Destination	Service	Action	Installed on
User_group@Any	Server network	Specific	Client encrypt	Gateway
Internal user	Partner/supplier	Specific	Encrypt	Gateway

The firewall administrators at GIAC have defined each rule necessary to allow the firewall-to-firewall VPN or authenticated VPN users to the required sources and protocols.

Authentication takes place at the firewall. When the VPN user initiates a connection with the server they want to connect to in the encrypted domain, the SecuRemote software contacts the firewall.

The firewall checks the incoming packet against the rule base for the destination address and service port. If the destination belongs to a server within the encrypted domain, an encrypted tunnel is established between the user's VPN client and the firewall after the user authenticates successfully.

Once the VPN is established, the packet is encapsulated and sent within the VPN tunnel between the workstation or remote firewall and the local firewall. With encapsulation, the packet is encrypted and "wrapped" within a packet and a new header. The firewall address then serves as the destination address of the packet. This protects not only the data within the packet but also the information within the original TCP header information. Only after reaching the firewall, is it unencapsulated, unencrypted and sent to the intended source.

2.4 Implementing firewall policy tutorial

2.4.1 OS installation

The Check Point NG FP-2 software is loaded on a Sun Ultra 60 running Solaris 8. Specific installation procedures must be followed in loading the Solaris 8 OS to harden the firewall server into a bastion host and minimize its vulnerabilities. There are several ways to harden the Sun OS including automated scripts written by Sun. See references for additional information. At no time during the installation and configuration of the firewall should it be placed on a live network. This ensures that the firewall will not be compromised during its vulnerable initial state. The following check list is just a representation of some of the steps to be taken during the OS install.

-
-
-

"Select Software" – select **Core System Support**

Note: ***End user Support*** *can be used, however, it includes a large number of packages that are not necessary for firewall functionality. It is recommended that as many of these packages should be removed to ensure the security and integrity of the system. See appendix for additional information.*
Note: ***Core System support*** *installs 83 packages of which approximately 53 can be removed. Use your discretion in doing this based on your type of system and hardware installed. Note also that volume management will not be installed, thus access to the CDROM will require mounting the drive.*

- Select **64 bit Support**
- Select **customize**

"Customize Software" under Software Clusters and Packages
Verify the following files required for Check Point are installed and add if needed

- **SUNWlibC**
- **SUNWlibCx**
- **SUNWter**
- **SUNWadmc**
- **SUNWadmfw**

Add On-line Manual Pages
SUNWdoc
SUNWman
Snoop sniffing utility
SUNfns
SUNfnsx
Additional packages to consider
Compression utilities
System Accounting Packages
NTP
Delete any non required packages.
Select **OK**

-
-
-

Make sure if the following files exist that they will not start by removing them or changing the name to a lower-case "s":

In **/etc/rc3.d**
rm S15nfs.server
mv S76snmpdx s76snmpdx
mv S77dmi s77dmi

In **/etc/rc2.d**
rm S73nfs.client
rm S80lp

rm S88sendmail
rm S74autofs
rm S71rpc
mv S92volmgt s92volmgt
mv S30sysid.net s30sysid.net
mv S71sysid.sys s71sysid.sys
mv S72autoinstall s72autoinstall
mv S99dtlogin s99dtlogin

vi /etc/inetd.conf and at minimum comment out ALL lines.
:g/^[^#]/s/^/#!/

Now add this line near the top of the file using tab between the fields.
ssh stream tcp nowait root /usr/local/sbin/sshd sshd -i

chmod 000 /usr/lib/sendmail
◆
◆
See references for further information on hardening the firewall.

2.4.2 Firewall rules configuration

Once the OS has been hardened, the Check Point software can be installed and configured on the system including the type of firewall features and administrators. Detailed installation and configuration instructions for the Check Point software is provided in their Getting Started Guide and User Guides. See references.

The firewall administrators can then access the Check Point firewall management software to configure the system and firewall's rules. The first object that must be created is the firewall object representing the firewall that is to be managed. In the GUI, choose the Check Point tab and right mouse click then click on new -> gateway option. Once the managed object screen appears, Figure 4, the firewall object name and IP address can be entered onto the screen. To establish communications with the firewall the communications button must be selected through the Secure Internal Communications area (SIC). Enter the password that was entered in the firewall during installation and initialize. See references for a link to further information by Check Point on SIC and troubleshooting SIC.

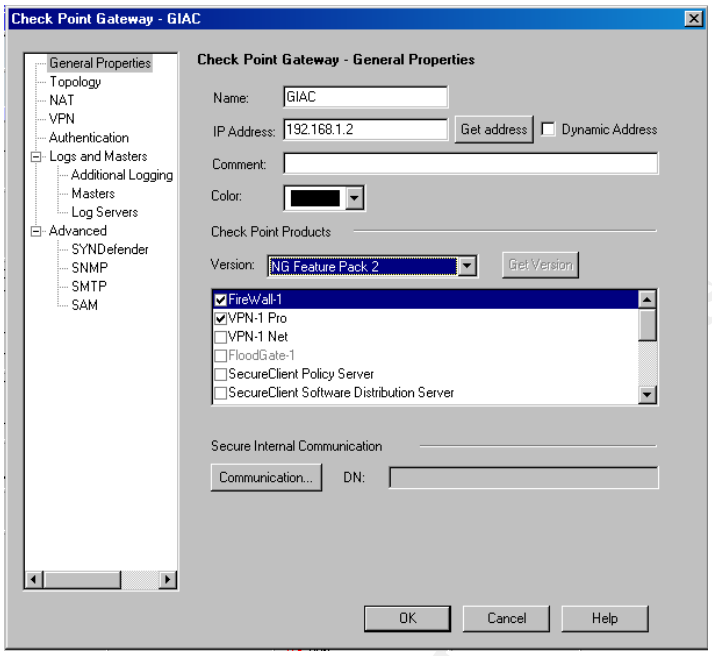


Figure 4: Firewall object

Once the general properties have been configured, it is important to define the topology of the firewall. This will determine what interfaces of the firewall that the various networks will sit behind. Click on the topology tab, once the topology screen is up, the firewall administrator can either have the management server get the topology information from the firewall or manually add it. See Figure 5.

With the firewall's interface IP addresses configured and the subnet mask set, it is possible then for the firewall to monitor that interface for spoofing based on the information provided by the firewall administrator. It is important to correctly identify the networks that the firewall interface will see; otherwise it will drop all traffic that it determines it does not expect to see at that interface. As seen in Figure 6, options include external, which is all traffic except that as defined by the internal interfaces, internal which is the network defined by the interface IP and subnet mask or internal and specific, which is all the networks that that interface can expect to see traffic from.

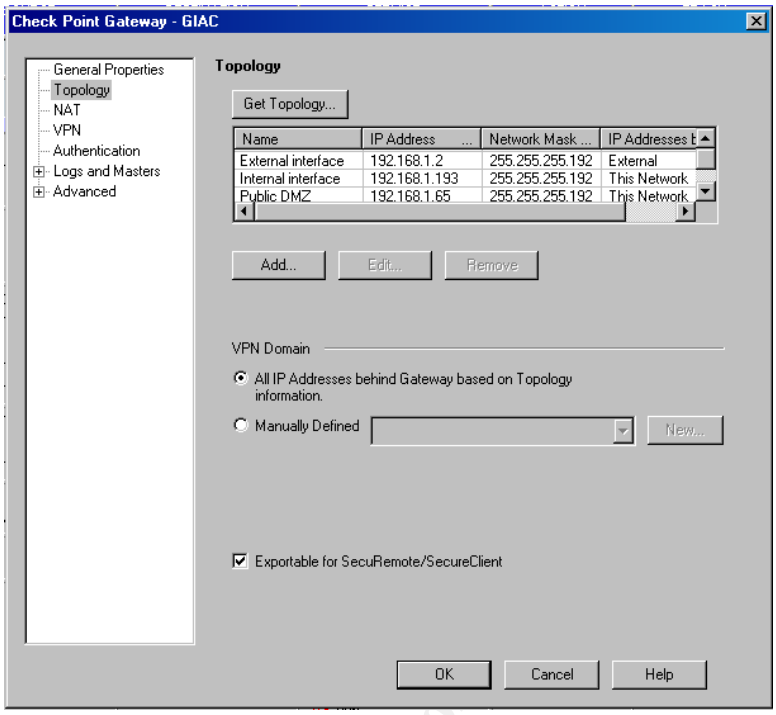


Figure 5: Firewall topology

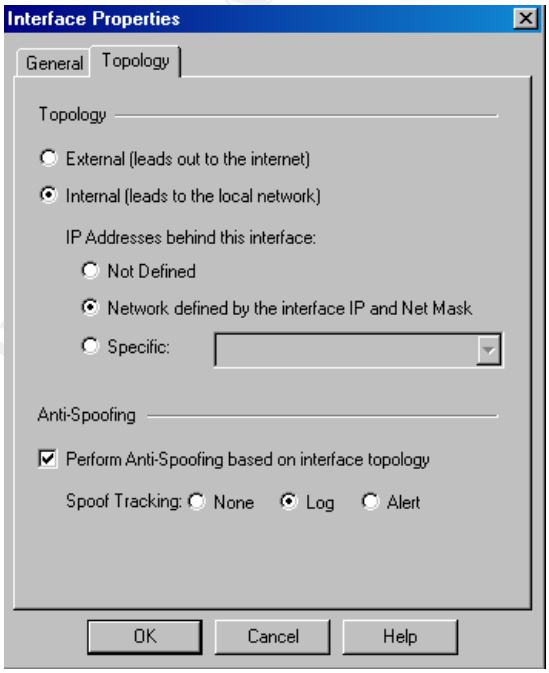


Figure 6: Interface properties & anti-spoofing

In order to create rules each system, network, network subnet, user and port that require access through the firewall, must be defined. This is done in Check Point by creating

objects that represent the respective network systems. In the GUI, right click on the corresponding tab for either node or network and add the object that needs to be created. See Figures 7 and 8.

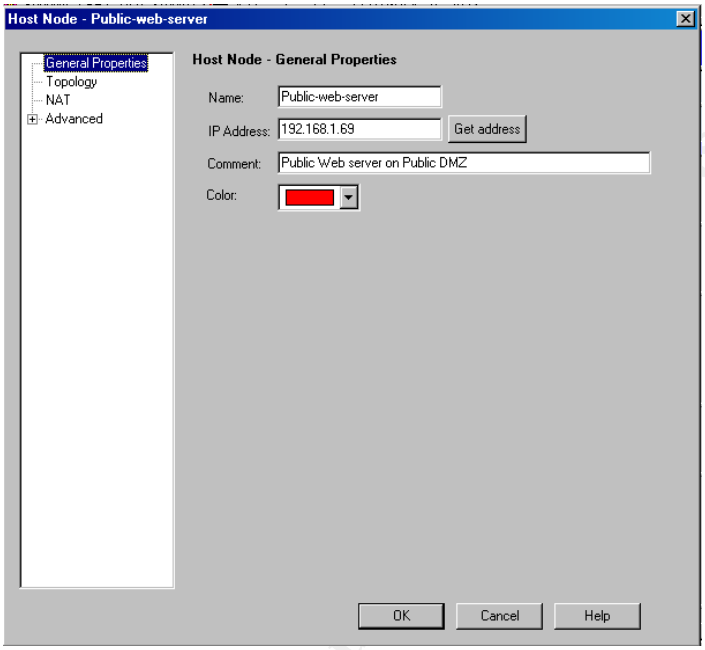


Figure 7: Creating a system or workstation object.

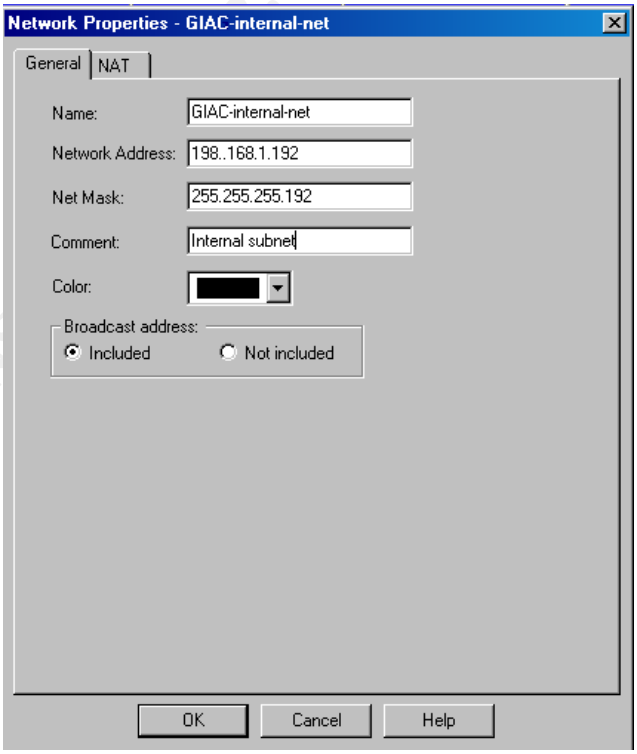


Figure 8: Creating a network object

For additional services that are not predefined by Check Point, click services in the GUI and right click tab for the corresponding service type such as TCP or UDP and add the new service. Figure 9.

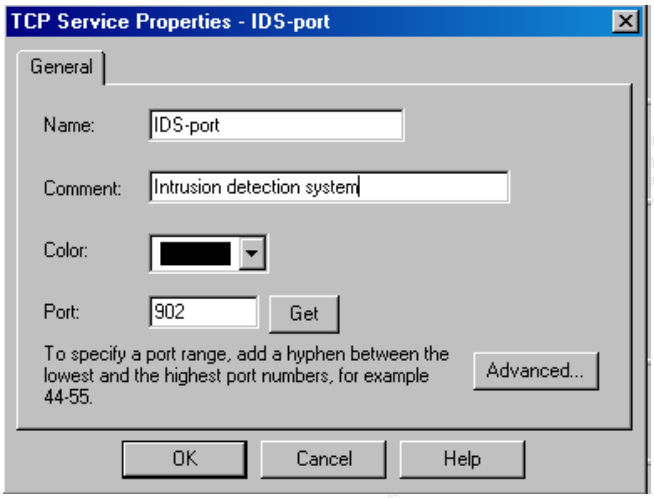


Figure 9: Creating a new service/port

Once the objects have been created, rules can be produced in the firewall using those workstations or network objects in the source and destination fields and the ports in the services field. Figure 10. To do this, you click on add new rule and determine if you want it above or below an existing rule. In the source, column right mouse click and select add. If the source is to be the universe then leave the column with the default (* Any) in it. Choose the object(s) that you want to be the source (where the traffic is coming from). Repeat the same steps for the destination column (where the traffic is going to).

In the service column, limit the ports that the source and destination objects are allowed to use. Allowing the default (* Any) service permits all the ports available to be used. This is extremely dangerous because it does not restrict the services thus allowing unlimited access between the systems for trojans and other malicious code to transfer between them. There should only be few occasions that this is allowed such as short term testing or allowing traffic to pass through your firewall to another firewall.

The action column allows the opportunity to determine what should be done with the traffic that matches this rule. The basic types of actions are accept, drop, reject, and encrypt. These are selected based on the appropriate action that is to be taken. For drop or reject it must be determined if the firewall is to respond to the source or not, if the action is to deny the traffic. It must be kept in mind that some services like TCP Ident, though we do not want to allow it in, will improve the response from the remote system, such as a SMTP server, if we reject the traffic rather than drop it. If the traffic is to be encrypted, the correct encryption properties must be checked to ensure that the encryption or decryption will succeed.

The track column provides the choice of how the traffic that matches that rule will be reported. The two major choices for this column are none and log. It is preferred to log all traffic that passes through the firewall but the amount of information that this produces must be weighed against the ability of the firewall administrator to review the logs on a consistent basis. With this need in mind, it is recommended that at a minimum any rule that allows traffic to and from the universe should be logged. The hot list, clean up rule and any other drop or reject rule must be logged unless we are specifically attempting to reduce the logs for a specific system or service. Rules that are more specific in their access will require less logging than a more general rule. Also, any critical system or service should be logged.

The time column is the next important column since it allows the firewall administrator to set up specific times that the rule is operational. This can be important if it is necessary to restrict access to systems during specific times only, such as business hours when the staff is available to monitor that system. The default (* Any) allows the rule to be available anytime; restrictions must be specifically set up.

The comment column can provide an important role in the firewall security. If rules are well commented it can be determined quickly if a rule was put in place for only a temporary test and needs to be removed on a specific date or is permanent. If it is a permanent rule then the comments aid the firewall administrator in the placement of the existing rule, or a new rule to maintain the integrity of the rule set.

With Check Point the order of the rules is important for both traffic flow and security. When Check Point validates the network traffic against the rules, it is done in a top to bottom sequence. Therefore, it is important to place the most used rule towards the top of the policy, thus minimizing the number of rules that traffic must be validated against. However, it is important to keep in mind the priority of security in the placement of the rules. It is necessary to place the most specific rules prior to the more general rules to ensure that they are enforced first. It is also critical to understand the impact of the placement of objects and their types so that inadvertent access is not created. Check Point will perform a basic validation of the policy to ensure that there are not significant security flaws in the rules, but a thorough evaluation comes with an in depth understanding of the rules and evaluation of the logs to verify they are operating as expected. In general, if rules are written as specific as possible, limiting access to and from specific systems and services, many potential problems can be avoided.

Figure 10: Check Point policy editor illustrating a portion of the GIAC rule-set

2.4.3 User VPN setup

To create a VPN for users of SecuRemote client software, several additional steps must be taken in the firewall configuration. The users must first be setup in the user manager. This is found under Manage in the tool bar and then selecting New -> User by Template -> Default. The required fields that must be filled out are the Login Name, see Figure 11, under the general tab. Under the Authentication tab, set the Authentication scheme, which includes various authentication methods including password setup, Figure 12, and the Encryption scheme, Figure 13. Under the Encryption tab select IKE, turn on log in the Successful Authentication Track field and verify the authentication and encryption. The remaining tabs allow for control of the users such as times and locations that they can login.

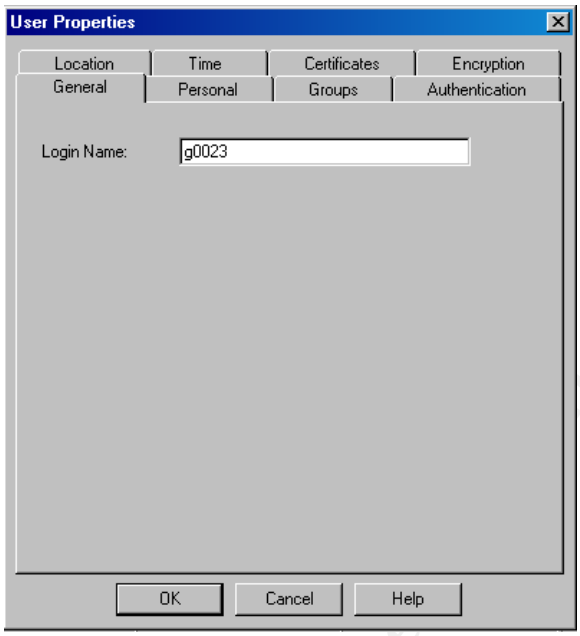
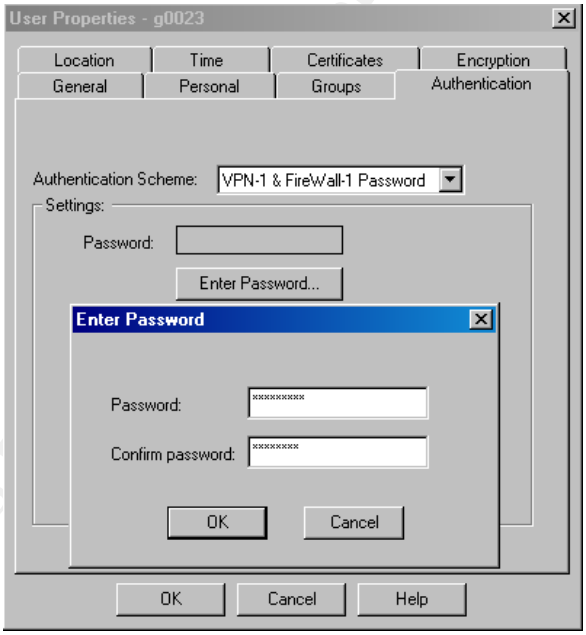


Figure 11: VPN user setup login ID



Figures 12: User setup authentication

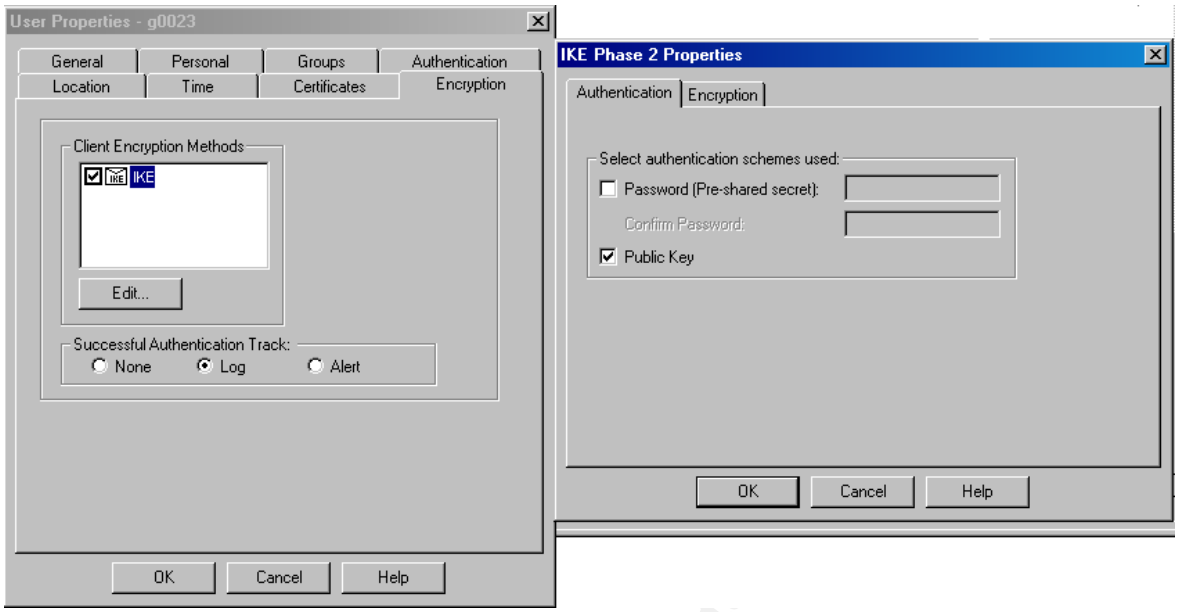


Figure 13: User setup encryption scheme

Once the user is set up, they must be added into a group, Figure 14. It is this group that is then used in the firewall rules. The rule is then created with the user group as the source, and the destination column includes the systems the users will be allowed to access. Services must be limited to the specific ports required and the authentication set to client encrypt, Figure 15. Once the rule is created and the user has loaded the SecuRemote software on their system, they will be able to connect to the site, authenticate and use the VPN. It is important that the firewall administrator fully understand the Check Point product and the various settings so that additional configuration on the Check Point properties, beyond the basic information presented here, can be implemented to enhance the security of the VPN.

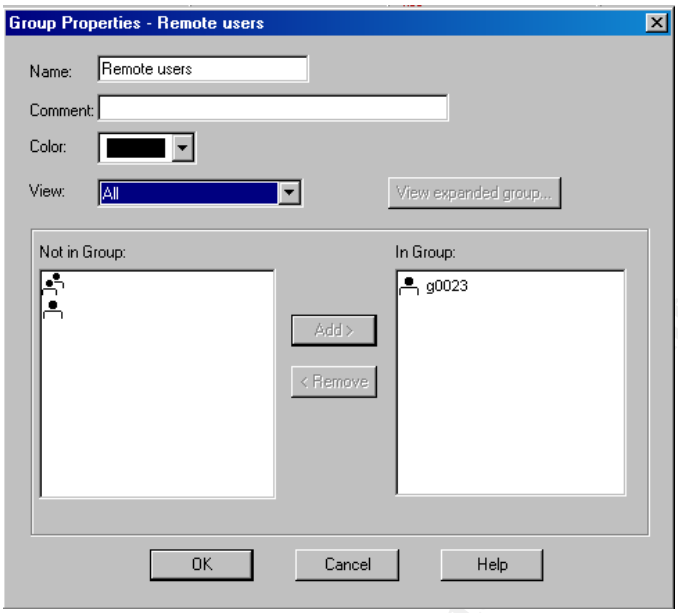


Figure 14: User setup, user group.

Figure 15: Remote user access rule.

2.4.4 Firewall-to-firewall VPN setup

The implementation of a firewall-to-firewall VPN to a remote site managed by another firewall administrator will require the cooperation of that administrator to successfully establish the scheme of the VPN. If this remote site is using a firewall product other than Check Point some additional research into that products implementations of VPN's may be required. The required information that the administrators will have to exchange and agree upon is the secret key, the encryption and authentication method, the encryption domain and the firewall's IP address.

The creation of the VPN begins with the verification and set up of the local firewall settings. These settings are accessed by editing the object representing the firewall and clicking on the topology tab, see Figure 16. It is critical that the correct topology is defined at the interfaces of the firewall since this information is then used to create the encryption domain unless specified otherwise. If the interfaces are correctly setup, then the "All IP Addresses behind Gateway based on Topology information" can remain checked under the VPN Domain header.

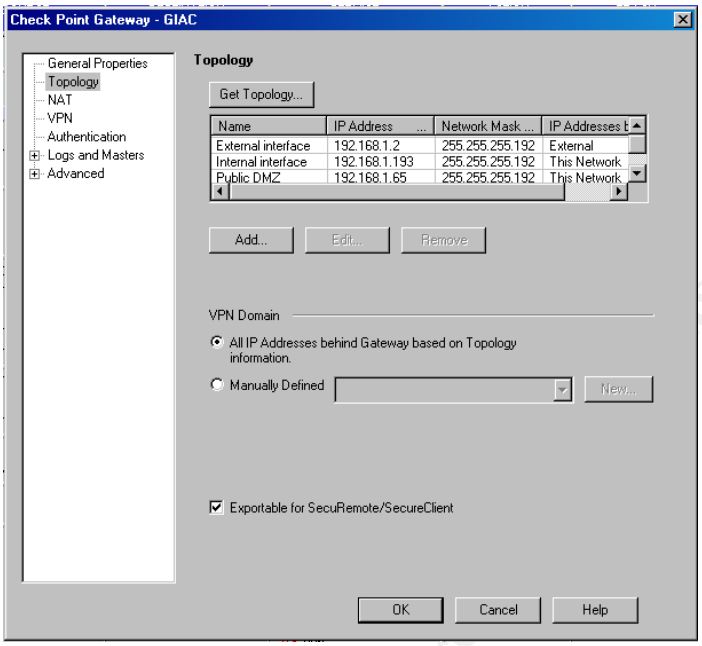


Figure 16: VPN domain setup

Once the VPN Domain is defined, click on the VPN tap to setup the specifics for the firewall. Within the VPN setup select IKE as the encryption scheme and click on edit, see Figure 17. Select the key exchange and data integrity options; be sure to include those settings needed to support other products. Pre-shared secret must be checked but cannot be setup until the other firewall is defined.

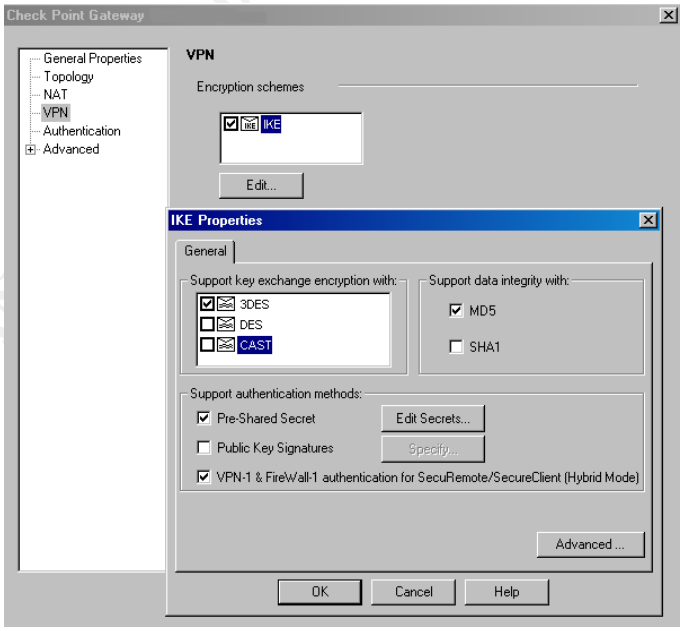


Figure 17: IKE properties

Once the local firewall is configured, a firewall object must be created to represent the other firewall of the VPN. In the GUI, the other firewall is created as an externally managed firewall. The external IP address for the firewall is entered in the IP address area. Under the topology tab, in the VPN Domain section, the manually defined option is selected and the network behind the other firewall is defined as the encryption domain. As with the local firewall, the VPN tab is then selected and the IKE properties set. This time however once the Pre-shared Secret is selected click on Edit Secret and select the local firewall and set the secret password that has been established with the remoter firewall administrator, see Figure 18.

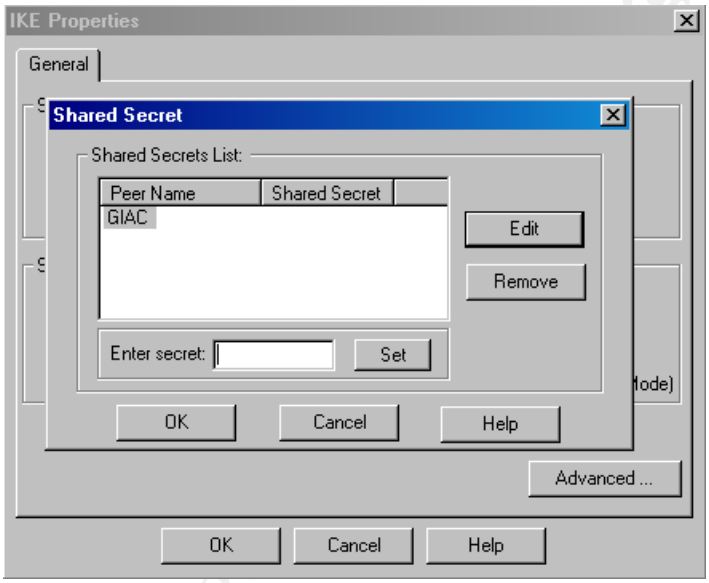


Figure 18: Pre-shared secret.

This completes the settings for the firewall and will establish a VPN once a rule to encrypt and decrypt the traffic that is to be placed in the VPN is defined. The rule is created as outlined earlier, except for in the action column encrypt is selected. See Figure 19. Once the encrypt action is selected it can be edited to set the specific parameters for that specific connection including the encryption scheme and the specific firewall the VPN is to be established to, see Figure 20.

Figure 19: VPN rule

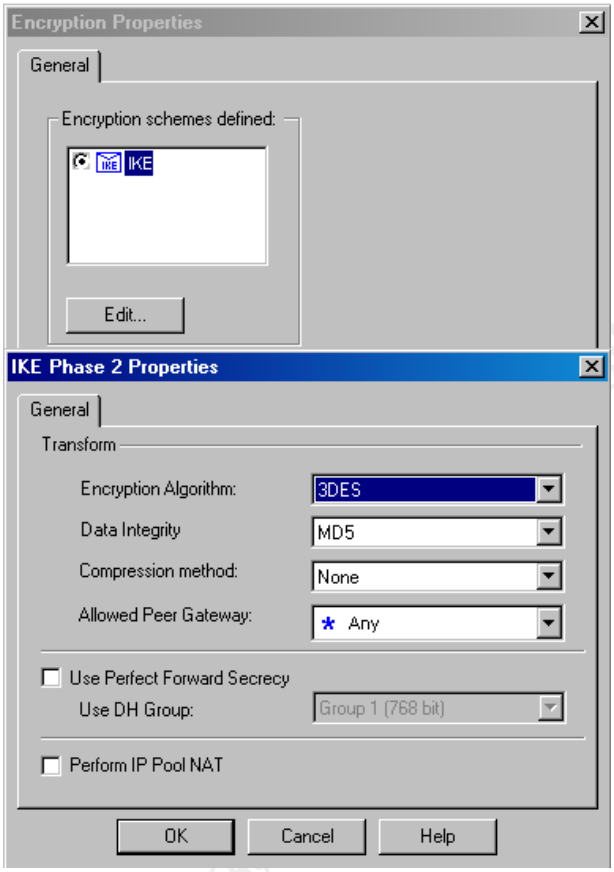


Figure 20: VPN rule properties

It is critical that the properties at both ends of the VPN match or else the VPN will fail and traffic will not traverse the network between the two sites. The IKE key exchange process and the encryption and decryption of the data can be monitored in the logs.

The firewall administrator, to ensure the security of the firewall, should explore additional configuration options available beyond the steps defined in this basic tutorial. After the firewall has been configured and a rule set created for the firewall, it is important to test the firewall for vulnerabilities prior to placing it on the network.

3. VERIFY THE FIREWALL POLICY

A regular audit of all systems is important to the security of the entire network. However, because of the critical role that the firewall plays in GIAC Enterprises, the GIAC IT staff has requested an audit of the firewall. In order to carry out a thorough audit on the firewall, the auditors must first understand the requirements and constraints of their audit. The primary steps in conducting the audit include planning the audit, conducting the audit and evaluating the audit.

3.1 Audit plan

Planning the audit must include the technical approach to assess the firewall, the time and length of the audit, cost, level of effort, tools used, the risks to the network in conducting the audit and the level of reporting of the vulnerabilities found.

For the GIAC firewall audit the IT manager decided that an outside auditor would be contracted to provide an impartial evaluation of the firewall.

3.1.1 Coordination

Before an audit can be conducted, it is important that the various groups that could be affected are informed and agree with the scope of the audit. Management must be informed prior to the audit of the schedule, scope, requirement and cost, and approve of the plan. Once the plan has been approved co-ordination with the IT staff must be made so that a minimum of two staff members are available to participate in the audit. This is both beneficial in learning from the auditor and to providing emergency support.

The audit is scheduled for off hours, at a time when the traffic is normally minimal. It has been determined that Monday night from 10:00 pm to 2:00 am Tuesday morning is the best time to conduct the audit. This has typically been the maintenance window used by GIAC and therefore foreign partners and suppliers have come to expect the possibility of downtime. This schedule also allows for additional staff to be called in early in order to get systems operational in an emergency prior to the normal business hours.

3.1.2 Cost

The cost of the audit is a major concern of management and requires the agreement of the managers to the amount of the budget they will to set aside for the audit. The amount to be spent will have a direct determination on the length and extent of the audit. The maximum the GIAC managers decided to budget is $13,000 which includes the following:

Contractor	40 hours x $200	$8,000
IT staff extra hours	20 hours x $50	$1,000
Emergency staffing	80 hours x $50	$4,000
Total		$13,000

Management expects that the actual cost of the audit should not exceed approximately $6,800 under normal circumstances. The IT manager wants the staff to learn from the auditor and be able to use the audit tools on their own in the future. Though the auditor has a number of proprietary tools available, to reduce the cost of the audit tools, GIAC has requested the auditor use public accessible tools.

3.1.3 Scope

The objective of the audit is to validate that the firewall is actually implementing the GIAC security policy. It has also been agreed upon, prior to the audit, that this is an evaluation audit only and no brute force or red team type audit will be conducted at this time. During this audit, any additional information obtained or security concerns are to be noted in the report by the auditor but are not to be pursued.

The auditors will:

- Scan for vulnerabilities with the firewall to validate the hardening of the OS.
- Port-scan the interfaces of the firewall to validate the rules on the traffic to or from the firewall.
- Port-scan the networks behind the firewall to ensure the rules are working properly.
- Review the logs of the firewall, IDS and syslog server to verify that the logging was operating correctly and detected the scans.

3.1.4 Tools

Though various tools are available for the audit. GIAC has requested the auditor use public accessible tools. This will allow the IT staff to use the knowledge gained during the audit and continue to use them in the future for conducing self-audits. As a result the auditors have chosen to use Nessus and Nmap as the primary auditing tools.

3.1.5 Risks and report

Risks to the network should be minimum. The audit is scheduled to take place during off hours and during a regularly scheduled maintenance window. The IT staff has personnel participating in the audit and will monitor the network for unexpected impact caused by the audit and will attempt to minimize this impact or stop the audit. If an emergency occurs in which systems have been effected, the IT staff has the authorization from management to call upon those they need to return the system back to normal operating level.

A detailed report of the audit and its findings is to be provided to the IT staff and an overview report to the GIAC management by the auditor. If serious vulnerabilities are found, the auditor is to report those to the IT staff immediately so they can be researched and addressed.

3.2 Conducting the audit

It is important to conduct the actual audit with in the scope of the plan to ensure that the firewall security policy is validated. To do this, both the firewall OS and the firewall rules must be tested. The auditor has chosen to use Nessus for verification of the OS hardening and Nmap for scanning of the firewall to validate its rules.

3.2.1 Checking the vulnerability of the firewall OS

The auditor is using Nessus version 1.2.6 as the vulnerability scanner to search for and exploit the systems vulnerabilities. This scanner remotely audits the system in an effort to determine if there are exploits that would allow someone to break in or misuse the system in any way. The Nessus scanner does not assume that services will be used on standard ports but tests for service vulnerabilities on all ports on the system.

The Nessus server and client are loaded on the same machine running the Redhat Linux OS. Prior to the audit of the system, the latest plugins are downloaded from the Nessus website to ensure that the system will analyze the most recent vulnerabilities available for the scanner software. This is done with the command #nessus-update-plugins.

Certain scripts of the Nessus software have the ability to cripple the network or bring the system down. These plugins are well identified as dangerous and a warning is provided at the initial login. It is important to take the necessary precautions to ensure that the system can be recovered if the scan causes the system to crash.

The Nessus server is started with the command #nessusd &. Once this process is started, the user interface is started by executing the #nessus command and then the user can log into the system, see Figure 21. Since the server and client reside together on the same system, the Nessusd host is localhost. The user accounts are setup on the Nessus server when setting up the login accounts.

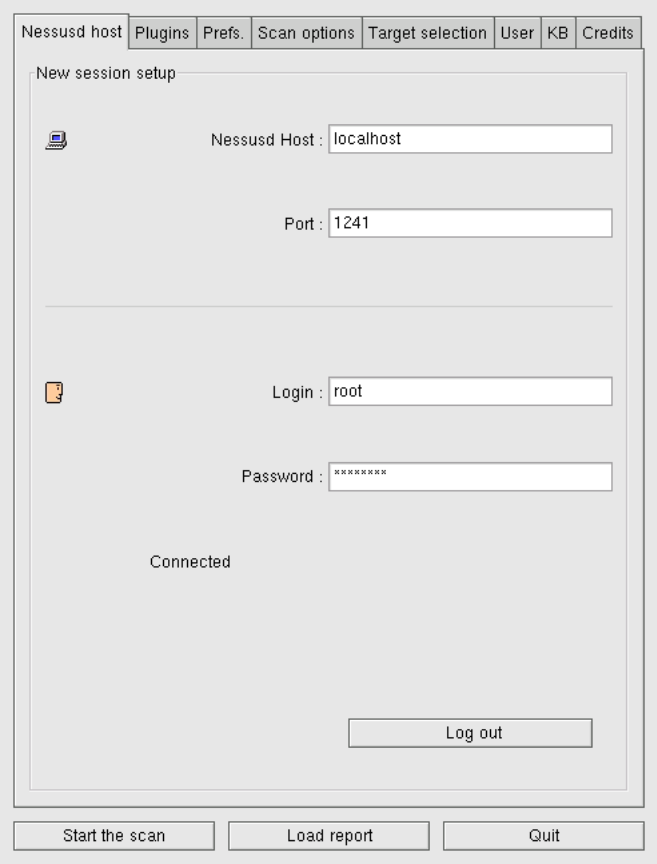


Figure 21: Nessus login

The various scripts that are used by the Nessus scanner are identified in the client program as plugins. The plugins are categorized by the platform, software or vulnerability that they will attempt to exploit, see Figure 22. The user can run all the scripts or choose those that best fit the platform that is to be tested. For the firewall, it is recommended that at minimum categories which need to be selected are: firewall, general, gain a shell remotely, gain root remotely and denial of service. In each category the specific vulnerability scripts can be chosen and are listed in the lower window. It is in this area that the administrator will also see the warning symbol associated with the more dangerous scripts. If additional information on a specific vulnerability exploit is desired, the script name can be clicked to review what will be reported about the vulnerability if it is successful against the system.

For the GIAC firewall audit, the majority of the categories were selected with only a few unchecked that were determined to not pertain to the firewall system.

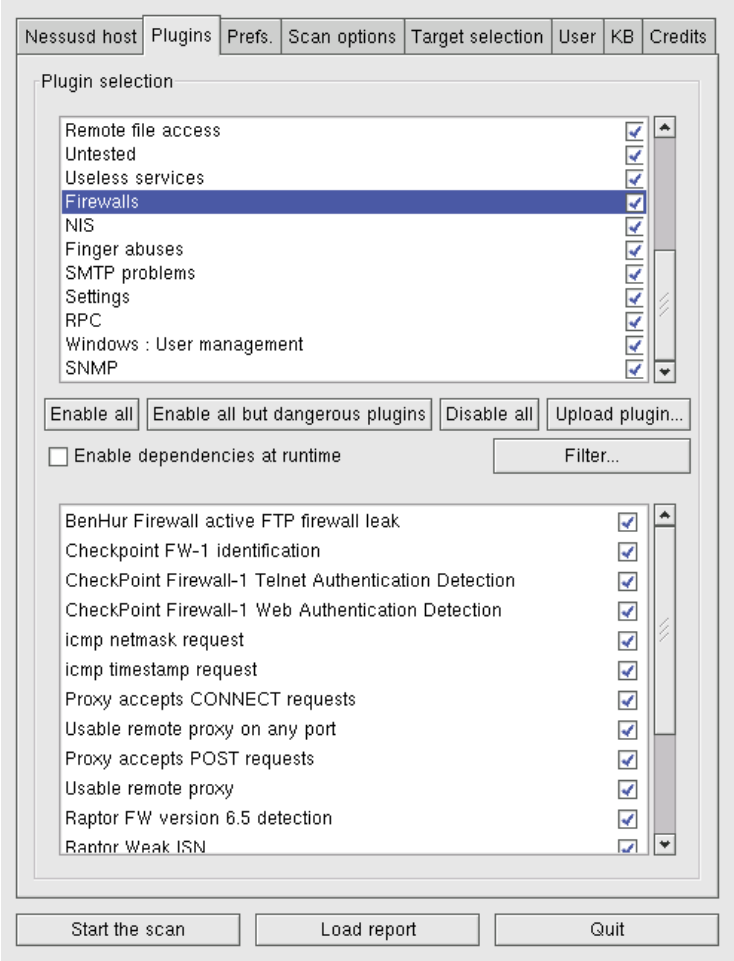


Figure 22: Vulnerability plugins

The remaining tabs must be reviewed and set according to what needs to be accomplished with the scan. For the Preferences tab, see Figure 23, the TCP scanning technique is chosen. For the GIAC firewall test, the SYN scan was chosen because of the typical use of this type of scan by hackers. In the scan options tab the options are set for port scanning. These include the port range and the type of scanner that Nessus is to use, see Figure 24. For the GIAC firewall audit, it is decided to allow for the scanning of port 1 – 15000 with the tools available to Nessus.

On the target selection tab the IP address of the GIAC firewall is entered. Once this has been entered, the Nessus program is ready to check the GIAC firewall. Prior to starting the vulnerability test the firewall must be configured to allow the scanner system through the firewall rules, otherwise the firewall OS will not be verified and tested. Once the rule is created to allow the scanner access to the firewall for any service, the scan can be started.

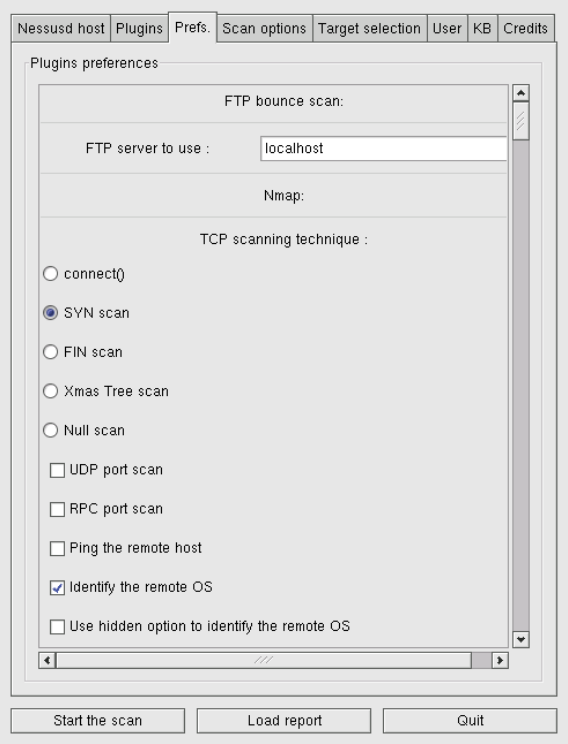


Figure 23: Scanning techniques

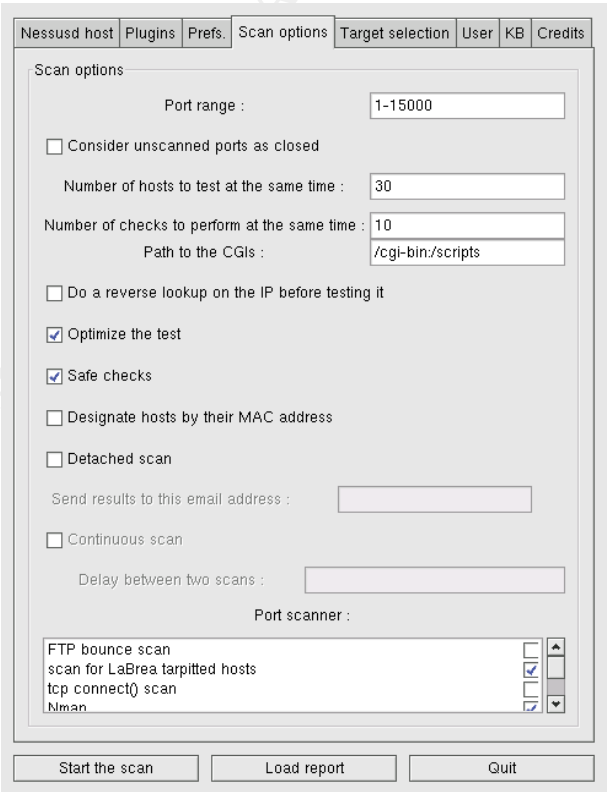


Figure 24: Scan setup

At the completion of the scan, Nessus provides several options for reports. The on screen report, see Figure 25, allows the auditor to explore the exploits that were found by clicking on the details of that vulnerability. A full file version of the report can also be created and saved as a file. A sample of this report is found in appendix A.

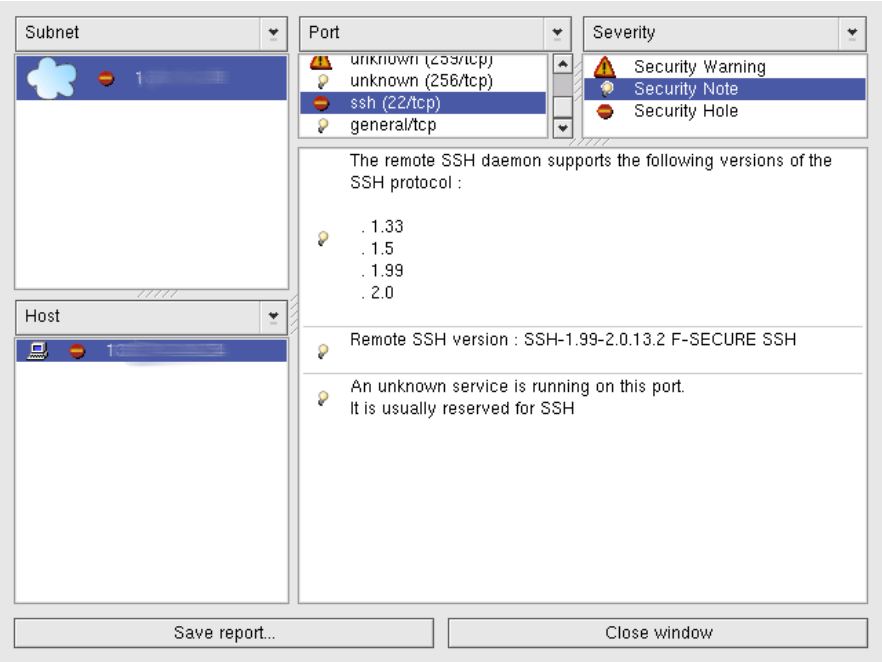


Figure 25: Nessus report

3.2.2 Checking the ports and firewall rules

To validate the firewall rules, the tool Nmap is used to verify the open and closed ports on all the interfaces. This will check to ensure that only the ports, according to the GIAC security policy and business needs are the ones open.

The Nmap tool is a free network-scanning tool that is very powerful and flexible, allowing various configurations to produce the desired test of the network or system. For the GIAC firewall testing, Nmap version 3.0 is loaded on a system running the Redhat Linux OS. Nmap can be either run from the command line using various options to select the desired scan and output, or a GUI window can be used by executing the #nmapfe & command, see Figure 26.

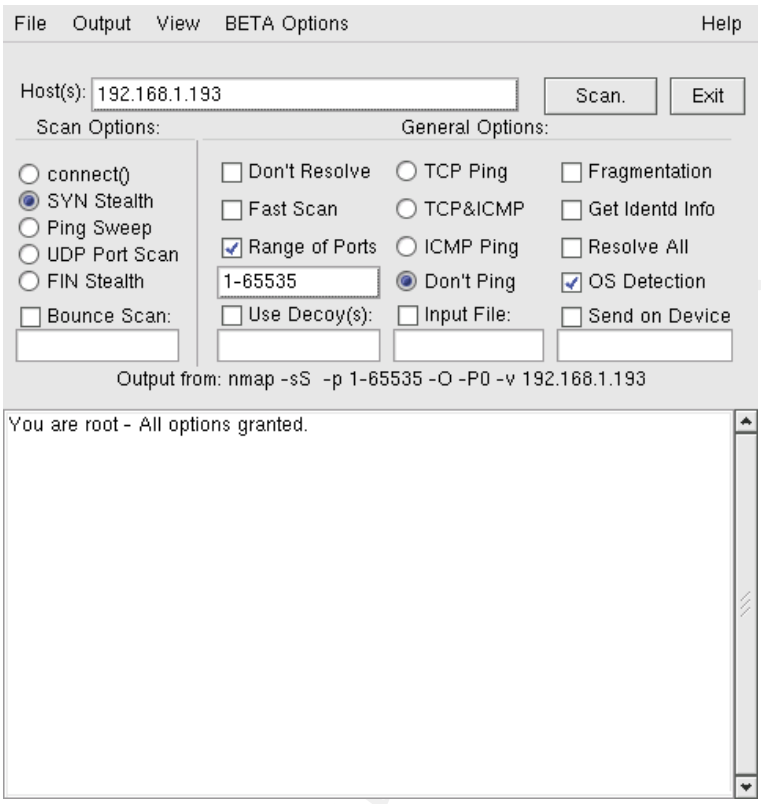


Figure 26: Nmap GUI interface

By directing the scans at both the interface of the firewall and at the networks behind the firewall, the rules of the firewall can be validated. This requires several scans to be preformed against the firewall interface and against each GIAC network, Public DMZ network, Supplier/partner network and internal network. The different types of scans that should be run against the GIAC firewall interfaces and networks include:

#nmap –sS –p 1-65535 –P0 –v –oN scan_ss.txt 192.168.1.193
#nmap –sU –p 1-65535 –P0 –v –oN scan_su.txt 192.168.1.193
#nmap –sT –p 1-65535 –P0 –v –oN scan_st.txt 192.168.1.193
#nmap –sF –p 1-65535 –P0 –v –oN scan_sf.txt 192.168.1.193

-Ss indicates a stealth SYN TCP scan
-sU indicates a UDP port scan
-sT indicates a TCP connect scan
-sF indicates a stealth FIN TCP scan. This scan will send a FIN packet causing certain ports that would normally not respond to the other scans to send a RESET packet.

The other options set the port range (-p 1 –65535), turn off ping (-P0) since the firewall does not respond to pings forcing the scan to proceed, a verbose output (-v) and a output to a file (-oN <filename>).

Prior to the scan with the Nmap tool, the rule allowing the Nessus to access the firewall was removed so that the firewall rules are being tested and not the firewall OS ports. Each of the various scans are performed on each network of the firewalls interfaces and the results collected for analysis. A sample of the Nmap scan reports is found in appendix B.

3.2.3 Inspection of the firewall

To make a complete and thorough audit of the firewall and its rules, the auditor must also collect information from the firewall software, system OS, and the firewall policy.

Configuration files for the Check Point software primarily reside in the $FWDIR/conf and $FWDIR/database directories and the logs are in the $FWDIR/log directory. Within these directories, the auditor can collect information on the policy and address translation rulebase, firewall configuration, VPN configuration, administrator access and privileges, firewall objects, and firewall logs. A sample of some of these file names is listed below:

<filename>.W & rulebase.fws	Policy and address translation rule base
Fwauth.NDB	Firewall users/administrators
objects.C	Network objects
fw.log	Firewall logs

The Solaris 8 OS must be evaluated for network information, patch level, administrator access and privileges, and system performance. A sample of where this information is located or obtained by running certain commands is listed below:

/etc/shadow & /etc/password	List of users
/etc/services	List of services
/etc/hosts	File for resolving host name and IP addresses
/etc/defaultrouter	Check for default router IP
/etc/notrouter	Turn off the Solaris router function
/etc/resolve.conf	Where to send DNS
/etc/nsswitch.cof	How host names are resolves
/etc/networks	Network configuration
/etc/inetd.conf	What services will start on bootup
/etc/rcS.d, /etc/init.d, /etc/rc0.d, /etc/rc1.d, /etc/rc2.d and /etc/rc3.d	Location of startup scripts
/etc/cron.d	Location of cron jobs
ifconfig –au	List network interfaces
netstat –an	Routing informaion
df –k	Disk space ussage

The firewall policy is best viewed through the GUI interface. Here the auditor can visually inspect the rules and objects noting anything that appears as a security concern. Also

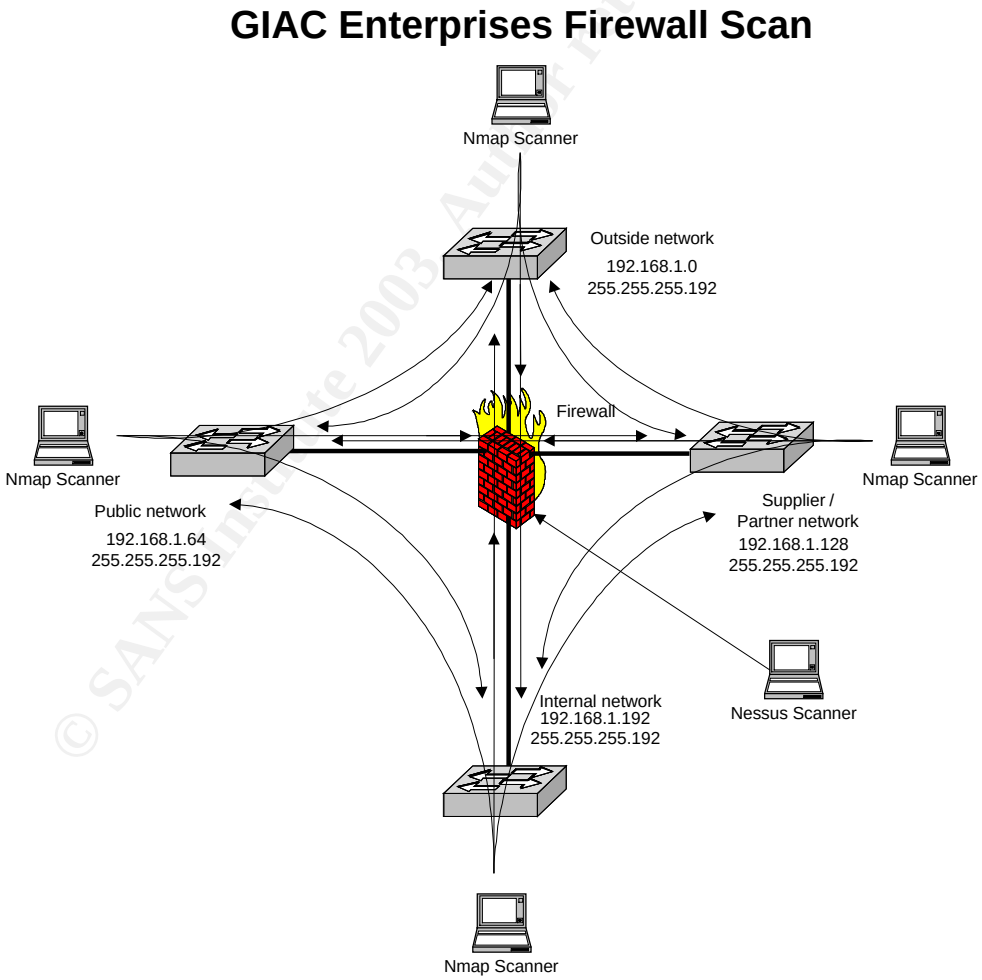
available to the auditor in the GUI client are the logs and global policy settings that can be verified.

3.3 Evaluating the audit

Once the information has been gathered from the various types of audits, each one must be evaluated and correlated with the firewall, syslog and IDS logs. Based upon the assessment of the logs and the overall evaluation of the firewall security policy, the auditor can make recommendations for improvements in the firewall or other supporting parameter defense systems.

A diagram of the audit, see Figure 27, indicating the various scans performed during the audit and the target of each of those scans aids in the evaluation of the audit to ensure that it is complete and thorough.

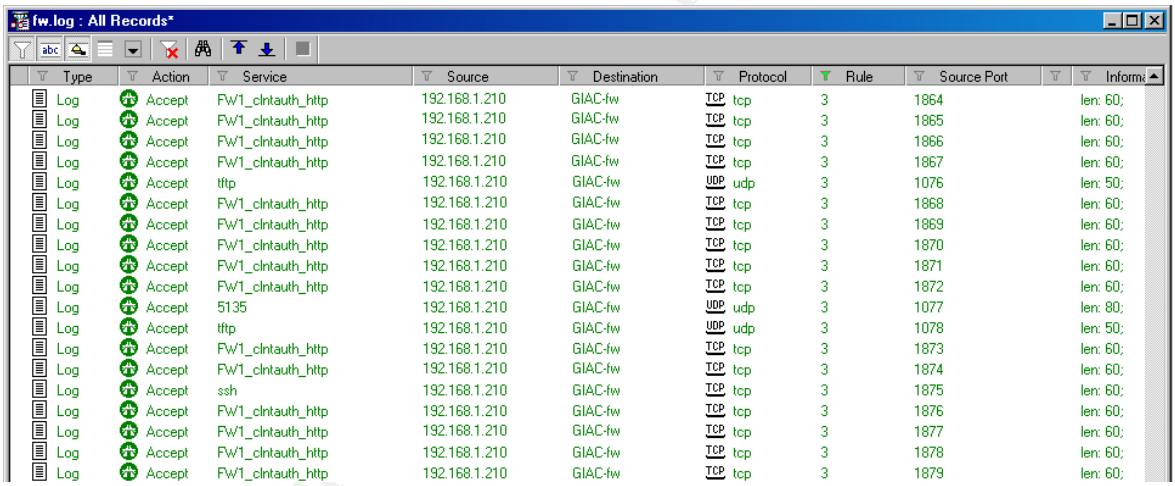
Figure 27



3.3.1 Evaluation of the Nessus scan.

The Nessus scan provides the auditor with a full description of the vulnerability and a recommendation or link to a recommendation on the web of how to improve security. Refer to the Nessus report in appendix A. It must be kept in mind that the vulnerabilities were discovered as a result of allowing the system with the scanning tool directly into the system bypassing the firewall. Based on the evaluation of the firewall rules the auditor noted that this is not allowed under normal circumstances and attempts to the firewall would have normally been dropped. The only connections allowed to the firewall OS is by the administrators on port 22.

A review of the firewall log in Figure 28 indicated that the entire scan was accepted and the results will be accurate. These results are evaluated and compared against the findings in the OS audit. It is recommended the GIAC firewall administrators make it a priority to update their version of SSH since it is their means of accessing the system. It was also recommended that they evaluate the OS packages, which are installed on the system and remove any of those not needed for the operation of the Check Point software.


fw.log : All Records*

Type	Action	Service	Source	Destination	Protocol	Rule	Source Port	Informa
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1864	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1865	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1866	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1867	len: 60;
Log	Accept	tftp	192.168.1.210	GIAC-fw	udp	3	1076	len: 50;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1868	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1869	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1870	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1871	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1872	len: 60;
Log	Accept	5135	192.168.1.210	GIAC-fw	udp	3	1077	len: 80;
Log	Accept	tftp	192.168.1.210	GIAC-fw	udp	3	1078	len: 50;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1873	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1874	len: 60;
Log	Accept	ssh	192.168.1.210	GIAC-fw	tcp	3	1875	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1876	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1877	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1878	len: 60;
Log	Accept	FW1_clntauth_http	192.168.1.210	GIAC-fw	tcp	3	1879	len: 60;

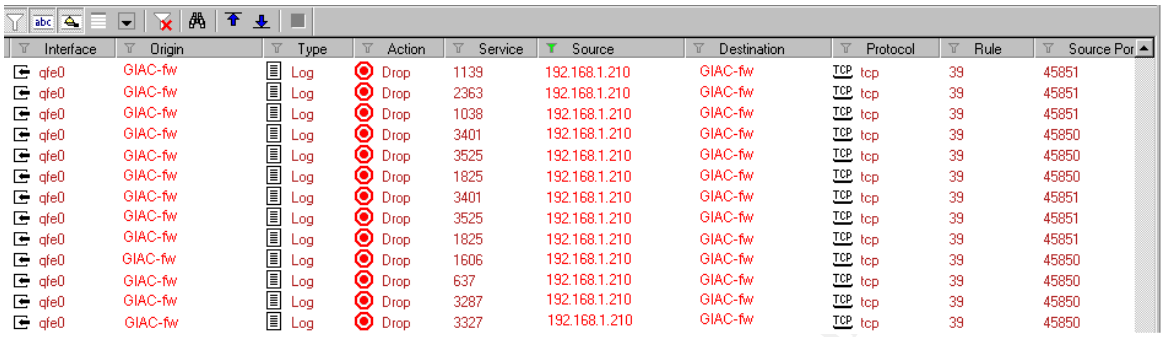
Figure 28: Firewall log of Nessus scan

3.3.2 Evaluation of the Nmap scans

The results of the Nmap port scans, reference appendix B, show what the scanning tool found as open ports on the firewall. The results are different for the scans against the firewall interface versus the networks and systems through the firewall.

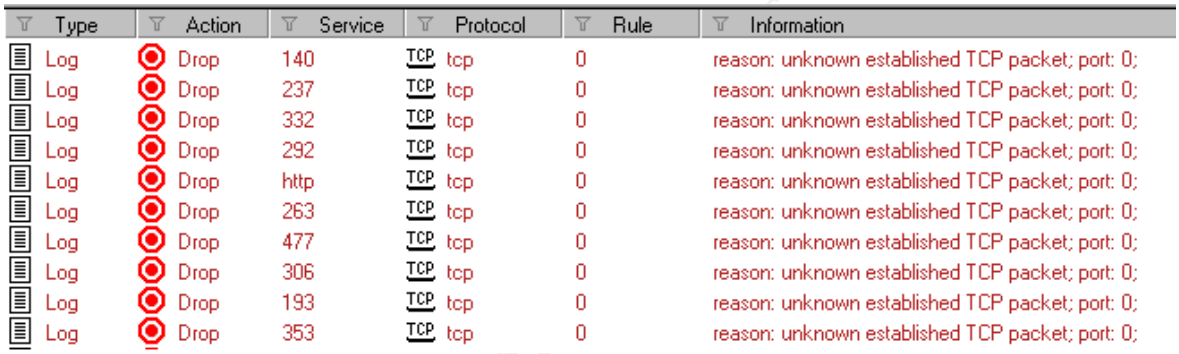
The scans against the interface confirm that the actual firewall does not have ports accessible and that the vulnerabilities noted in the Nessus scan, though are of some concern, are not accessible once the firewall rules are in place. The results of the scan are also verified with the firewall logs in Figure 29, showing the attempted connections were

dropped with the clean up rule. With the FIN stealth scan, the Check Point rule 0 indicates that Check Point has detected a packet out of state with its state tables. See Figure 30.



Interface	Origin	Type	Action	Service	Source	Destination	Protocol	Rule	Source Por
qfe0	GIAC-fw	Log	Drop	1139	192.168.1.210	GIAC-fw	tcp	39	45851
qfe0	GIAC-fw	Log	Drop	2363	192.168.1.210	GIAC-fw	tcp	39	45851
qfe0	GIAC-fw	Log	Drop	1038	192.168.1.210	GIAC-fw	tcp	39	45851
qfe0	GIAC-fw	Log	Drop	3401	192.168.1.210	GIAC-fw	tcp	39	45850
qfe0	GIAC-fw	Log	Drop	3525	192.168.1.210	GIAC-fw	tcp	39	45850
qfe0	GIAC-fw	Log	Drop	1825	192.168.1.210	GIAC-fw	tcp	39	45850
qfe0	GIAC-fw	Log	Drop	3401	192.168.1.210	GIAC-fw	tcp	39	45851
qfe0	GIAC-fw	Log	Drop	3525	192.168.1.210	GIAC-fw	tcp	39	45851
qfe0	GIAC-fw	Log	Drop	1825	192.168.1.210	GIAC-fw	tcp	39	45851
qfe0	GIAC-fw	Log	Drop	1606	192.168.1.210	GIAC-fw	tcp	39	45850
qfe0	GIAC-fw	Log	Drop	637	192.168.1.210	GIAC-fw	tcp	39	45850
qfe0	GIAC-fw	Log	Drop	3287	192.168.1.210	GIAC-fw	tcp	39	45850
qfe0	GIAC-fw	Log	Drop	3327	192.168.1.210	GIAC-fw	tcp	39	45850

Figure 29: Dropped packets to the interface



Type	Action	Service	Protocol	Rule	Information
Log	Drop	140	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	237	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	332	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	292	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	http	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	263	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	477	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	306	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	193	tcp	0	reason: unknown established TCP packet; port: 0;
Log	Drop	353	tcp	0	reason: unknown established TCP packet; port: 0;

Figure 30: Dropped packets to the interface, not in Check Points state table

The Nmap scans through the firewall resulted in Nmap logs listing the various ports that were accessible from the scanning tool. By moving the scanning to various locations and acting as different IP addresses, it was relatively easy to verify the ports that were open. These results were then correlated with the firewall logs and the firewall policy to verify that no access was obtained, which were not expected. If more time were available, it would have been possible to test the firewall from all the various users and networks that were expected to access the various systems. However, the scope of the audit did not permit this.

3.3.3 Evaluation of the firewall system and rules

An important part of the audit is knowing what to look for in the various files and settings in the GUI of the OS and firewall software and also the current vulnerabilities of the OS and firewall system. These current vulnerabilities can be found at various sites on the web, some of which are listed in the reference section.

Items that the auditor evaluated in the system included a search for unnecessary or unauthorized user accounts, sufficient space for log storage avoiding the risk of insufficient

disk space bringing the server down, unnecessary services, routing information, and OS logging of logins.

By correlating the information from the Nessus scan and the audit of the actual OS of the firewall, the auditor was able to make several recommendations on tightening up the firewall OS. These recommendations included that the GIAC firewall administrators make it a priority to update their version of SSH and that they evaluate the OS packages that are installed on the system and remove any of those not needed for the operation of the Check Point software.

From the visual inspection of the firewall rules and the results of the Nmap scan, the auditor verified that the policy in place on the firewall was secure and did not allow inadvertent access to any system that was not authorized. Other things the auditor also evaluated included: verifying that the network objects had the correct IP addresses, customized ports were correctly created and the rules are in a secure order. Based on this information, the auditor verified that the firewall rules are well written and balance the business needs of GIAC Enterprises with tight firewall security.

4. DESIGN UNDER FIRE

The design chosen to come under fire is by Patricia Siow located at http://www.giac.org/practical/Patricia_Siow_GCFW.zip. Figure 31 provides a diagram of this network. The primary firewall is identified as a Check Point Firewall-1 version 4.1. No service pack was identified. Three different types of attacks will be attempted against this design. These include an attack against the firewall, a denial of service attack and an attack against an internal system.

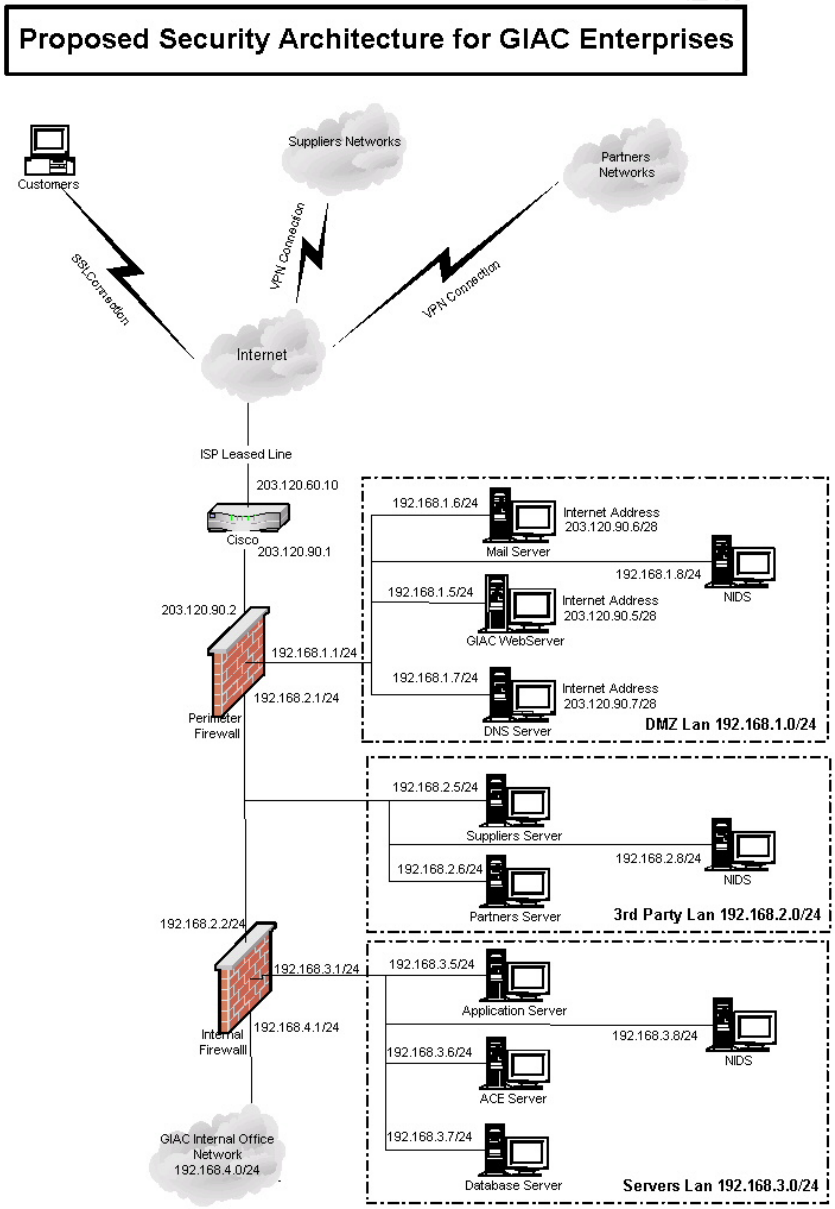


Figure 31: GIAC Enterprises by Patricia Siow

4.1 Attack against the firewall

4.1.1 Firewall vulnerability

Typically an attacker would have to determine what type of firewall that is in place in order to attempt to use a known vulnerability against that system and have a successful attack. Since this information was obtained from a GIAC Enterprises document on the web, it eliminates the need to discover this information and possible detection by the GIAC IT staff, and allow us to refine our attack to a specific vulnerability.

Check Point Firewall-1 Version 4.1 is indicated as the type of firewall in the GIAC Enterprises design. Since there was no service pack defined in the network document for this firewall, it could be vulnerable to several different attacks. A search of www.cert.org results in several attacks including RDP bypass vulnerability. Further research leads us to the information about this vulnerability at online.securityfocuse.com/bid/2952, www.checkpoint.com/techsupport/alerts/rdp_comms.html, and from www.inside-security.de/fw1_rdp.html which also includes the proof of concept code.

Based on the information gathered, if this attack is successful, the attack should be able to transverse the firewall on port 259 by using false Check Point RDP headers on UDP packets. This effectively creates a tunnel and opens up the opportunity to gain access to restricted systems, exploit other vulnerabilities, or launch denial-of-service attacks. According to Check Point, this vulnerability may affect system stability causing errors that affect the management functions such as logging and administrative communications. Check Point does assure the user that at no time is the security policy compromised and they do supply a hotfix to correct the problem.

4.1.2 Attack using the vulnerability

From the proof of concept and other information gathered from online there is enough information to create the attack. Following the example code at www.inside-security.de/uploads/media/fw1_rdp_poc.c a program is compiled on a Linux system to produce the crafted incorrect packets. Ensuring that our Linux system is using a spoofed IP address, our attack is launched at the firewall and systems in the DMZ network. The hope is to make it through the firewall and have a tunnel created to provide undetected access to the systems in the DMZ. This would provide the opportunity to do additional probes and information gathering about those systems and potentially allowing a system to be compromised. At a minimum, it is hoped that the attack will cause the firewall to become unstable and inaccessible to the administrators.

4.1.3 Results of the attack

Our attack was unsuccessful. It is apparent that during the audit of the GIAC Enterprises firewall this vulnerability was identified and the hotfix from Check Point was applied to

the system. A typical hacker would be undeterred by this failure and would research other vulnerabilities of the Check Point firewall and test them also.

4.2 Denial of service attack

The next attempt of attack against the GIAC enterprise network is a distributed denial of service attack. By using a master to conduct and coordinate a number of agents, it is hoped that the increased traffic destined for the target system will overwhelm it or a system in its path. This will then not allow the system to respond to legitimate requests and effectively block access to that system or the entire network.

The attack against GIAC will use 50 compromised cable modem and DSL systems. These are easily found by scanning the cable modem and DSL networks and placing a trojan program on the compromised systems. The trojan chosen to execute the denial of service is the tribal flood network 2000 (TFN2K) program. This program will be used to coordinate the 50 agents against the GIAC web server using SYN packets. The TFN2K agents are loaded on the compromised systems and communicate back to the master using TCP, UDP or ICMP and are encrypted. Since responses are not expected back from the target system, the clients can use spoofed IP addresses. Once the client agents are in place and communicating with the master, the attack can be executed. The command is executed identifying from a file; the hostnames of the agents, the type of attack (TCP/SYN flood), the target IP of the GIAC web server and the port number to attack (80).

Sample command: #./tfn –c 5 –f tfn_clients –I 203.120.90.5 –p 80

Distributed denial-of-service attacks are hard to mitigate. Depending upon the processing power of the firewall, it is only a matter of having enough agents attacking the systems on the inside networks before the firewall will be overcome by the SYN flood. According to www.kb.cert.org/vuls/id/539363, an article on the vulnerability of state-based firewalls, Check Point is still vulnerable to these types of attacks especially older versions that have not incorporated the newer defenses.

GIAC Enterprises has put in place a number of defenses against distributed denial-of-service attacks including ingress and egress filtering of reserved and private IP address ranges on the router and firewall, minimizing their potential use as spoofed addresses. They have also maintained their IDS systems allowing the early detection of an attack. Thus providing the administrators an opportunity to begin countermeasures including contacting their ISP to attempt to filter or minimize the amount of traffic received.

Other defenses against distributed denial-of-service include increased memory in the firewall system to allow larger state tables, maintaining separate initial and established session time out values, and setting the initial session timeout value low to clear out those connections that do not connect. In Check Point 4.1 these settings can be found in the SYN defender tab of the global properties.

4.3 Compromise of an internal system

Attacks against public servers are common and should be expected by the IT staff. However, these systems are often neglected and allowed to remain unpatched increasing the risk of discovery and exploit. Since private systems are often well protected by a firewall, the attention is then focused on the public systems in hopes of leveraging vulnerabilities and using that as a platform for a disruption to the network or for further attacks. To determine what systems might be available to attack various queries such as DNS lookups and whois will give us the network that these systems may reside on. This would provide the potential information that is needed to scan that network for systems that are available to attack.

Since web servers are so prevalent in many networks and they often use the Microsoft Internet Information Services (IIS), a system that has had numerous vulnerabilities, the attack will search for and attempt to exploit that type of system. To identify the web server, Nmap is used to scan for the web server.

By executing the command nmap –sS –P0 –p80 –v –randomize_hosts 203.120.90.* the entire GIAC Enterprises network can be searched in a random order, to decrease detections, for an open port on 80. This scan provides the IP address of 203.120.90.5 as the potential web server. Since the scan may have been detected by the IDS, the IP address of the system should be changed prior to coming in again to determine if this system is running IIS.

This IP address is then verified as running web services by connecting to the HTTP port. Additional information about the system is gathered by examining the headers that are returned and through the use of a sniffer. No information as to the type of web server used in the GIAC design by Patricia Siow was provided, so it is assumed that GIAC used the popular Microsoft IIS and that it is version 5.0. This information can be obtained several ways. One, of which is with the use of the tcpdump sniffer command tcpdump –lenx –I eth0 –w scan.txt. The output of this file could be searched manually or run through a tool such as tcpshow to find the desired information.

Once it has been confirmed that this server is running Microsoft IIS version 5.0, a search of the web turns up a number of exploits against this version of IIS. A search of http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl provides a pair of similar exploits that could be used to map out the file structure and view scripts on the system. They are the Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability and Microsoft IIS CodeBrws.asp File Extension Check Out By One Vulnerability. Detailed information on these exploits are found at http://online.securityfocus.com/bid/4525 and http://online.securityfocuse.com/bid/4543.

The original intent of the CodeBrws.asp file was to allow viewing of source code in the sample directory of the system. However, the script does not correctly filter the Unicode representations of directory transversals. This allows the substitution of '..' within the URL.

This vulnerability is attempted against the GIAC web server with the following command:

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

The web server returned a 404 Not Found message indicating the GIAC administrators have followed good security practices and had removed the sample scripts from the web server.

5. REFERENCES

Router
http://www.cisco.com
http://pasadena.net/cisco/secure.html
http://nsa1.www.conxion.com/cisco/guides/cis-2.pdf
http://www.cisco.com/warp/public/707/21.html
http://www.iana.org/assignments/ipv4-addess-space

Hardening the Sun OS
http://www.enteract.com/~lspitz/
http://wwws.sun.com/software/security/jass/
http://wwws.sun.com/software/security/blueprints/
http://www.checkpoint.com/techsupport/documentation/certdocs/

Check Point firewall software installation and configuration
http://www.checkpoint.com/techsupport/installation/ng/preinstall.html
http://support.checkpoint.com/public
http://www.checkpoint.com/support/technical/documents/index.html
http://support.checkpoint.com/kb/docs/public/firewall1/5_0/pdf/sic.pdf
http://www.phoneboy.com

Vulnerability Research Sites
http://www.securityfocuse.com
http://online.securityfocuse.com/cgi-bin/sfonline/vulns.pl
http://xforce.iss.net
http://online.securityfocuse.com/archive/1
http://www.securepoint.com
http://www.cert.org
http://www.cisco.com/warp/public/707/newsflash.html
http://packetstrom.decepticons.org/distributed/indexdate.shtml
http://www.denialinfo.com
http://grc.com
http://www.checkpoint.com/techsupport/alerts
http://www.inside-security.de/

Vulnerability Tools
http://www.nessus.org
http://www.nmap.org
http://www.pgp.com/products/cybercop-scanner/default.asp
http://www.iss.net
http://www.tripwire.com

APPENDIX A - Nessus scan report

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 7
 - Number of security warnings found : 6
 - Number of security notes found : 6



TESTED HOSTS

 192.168.1.193 (Security holes found)



DETAILS

+ 192.168.1.193:
 . List of open ports :
   o ssh (22/tcp) (Security hole found)
   o unknown (256/tcp) (Security notes found)
   o unknown (259/tcp) (Security warnings found)
   o unknown (264/tcp) (Security warnings found)
   o unknown (265/tcp)
   o unknown (900/tcp) (Security hole found)
   o general/tcp (Security notes found)

 . Vulnerability found on port ssh (22/tcp) :



    You are running a version of SSH which is
    older than version 3.1.5 or 3.2.2.

    There is a bug in that version which may allow
    a user to obtain higher privileges due to a flaw
    in the way setsid() is used.


    Solution : Upgrade to the latest version of SSH
    See also : http://www.ssh.com/company/newsroom/article/286/
    Risk factor : High

 . Warning found on port ssh (22/tcp)
```

```
   The remote SSH daemon supports connections made
   using the version 1.33 and/or 1.5 of the SSH protocol.

   These protocols are not completely cryptographically
   safe so they should not be used.

   Solution :
    If you use OpenSSH, set the option 'Protocol' to '2'
    If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

   Risk factor :
    Low


. Information found on port ssh (22/tcp)


   An unknown service is running on this port.
   It is usually reserved for
    SSH


. Information found on port ssh (22/tcp)


   Remote SSH version : SSH-1.99-2.0.13.2 F-SECURE SSH

. Information found on port ssh (22/tcp)


   The remote SSH daemon supports the following versions of the
   SSH protocol :

     . 1.33
     . 1.5
     . 1.99
     . 2.0

. Information found on port unknown (256/tcp)


   A time server seems to be running on this port


. Warning found on port unknown (259/tcp)



   A Firewall-1 Client Authentication Server is running on this port.

   Such an element allows an intruder to attempt to log into
   the remote network or to gather a list of valid user names
   by a brute-force attack.
```

```
    Solution : if you do not use this service, disable it.
    Risk factor :
     Low


  . Warning found on port unknown (264/tcp)



    The remote host seems to be a Checkpoint FW-1 running SecureRemote.
    Letting attackers know that you are running FW-1 may enable them to
    focus their attack or will make them change their attack strategy.
    You should not let this information leak out.
    Furthermore, an attacker can perform a denial of service attack on
    the machine.

    Solution:
    Restrict access to this port from untrusted networks.

    Risk factor : Low

    For More Information:

http://www.securiteam.com/securitynews/CheckPoint_FW1_SecureRemote_DoS.ht
ml


  . Vulnerability found on port unknown (900/tcp) :



    alya.cgi is a cgi backdoor distributed with
    multiple rootkits.

    Risk factor :
     Serious

  . Vulnerability found on port unknown (900/tcp) :


    The remote HTTP server
    allows an attacker to read arbitrary files
    on the remote web server, simply by adding
    dots in front of its name :
    Example:
     GET /../../winnt/boot.ini

    will return C:\winnt\boot.ini

    Solution : Upgrade your web server or change it.

    Risk factor : Serious
    CVE : CAN-1999-0776
```

```
. Vulnerability found on port unknown (900/tcp) :


   The Cart32 e-commerce shopping cart is installed.

   This software contains several security flaws :

    - it may contain a backdoor
    - users may be able to change the admin password remotely


   You should use something else.

   See also : http://www.cerberus-infosec.co.uk/advcart32.html

   Solution : use another shopping cart software
   Risk factor : High
   CVE : CAN-2000-0429

. Vulnerability found on port unknown (900/tcp) :


   The script /cart/cart.cgi is present.

   If this shopping cart system is the Dansie
   Shopping Cart, and if it is older than version 3.0.8
   then it is very likely that it contains a backdoor
   which allows anyone to execute arbitrary commands on this system.

   Solution : use another cart system
   Risk factor : High
   CVE : CVE-2000-0252

. Vulnerability found on port unknown (900/tcp) :


   The file /ncl_items.html or /ncl_subjects.html exist on the remote
   system.
   It is very likely that this file will allow an attacker
   to reconfigure your Tektronix printer.

   An attacker can use this to prevent the users of your
   network from working properly by preventing them from printing their
   files.

   Solution : Filter incoming traffic to port 80 to this
   device, or disable the Phaserlink webserver on the
   printer (can be done by requesting
    http://printername/ncl_items?SUBJECT=2097)
```

```
   Risk factor : Low
   CVE : CAN-1999-1508

. Vulnerability found on port unknown (900/tcp) :



   There may be buffer overflow in the remote cgi win-c-sample.exe.
   An attacker may use this flaw to execute arbitrary commands
   on this host.

   *** Nessus reports this vulnerability using only
   *** information that was gathered. Use caution
   *** when testing without safe checks enabled.

   Solution : delete it
   Risk factor : High
   CVE : CVE-1999-0178

. Warning found on port unknown (900/tcp)



   A Firewall-1 web server is running on this port and serves web
   authentication requests.


   This service allows remote attackers to gather usernames and
   passwords through a brute force attack.

   Older versions of the Firewall-1 product allowed verifying usernames
   prior to checking their passwords, allowing attackers to easily
   bruteforce a valid list of usernames.

   Solution : if you do not use this service, disable it
   Risk factor : Low

. Warning found on port unknown (900/tcp)


   Some Web Servers use a file called /robot(s).txt to make search
   engines and any other indexing tools visit their WebPages more
   frequently and more efficiently.
   By connecting to the server and requesting the /robot(s).txt file, an
   attacker may gain additional information about the system they are
   attacking.
   Such information as, restricted directories, hidden directories, cgi
   script directories and etc. Take special care not to tell the robots
   not to index sensitive directories, since this tells attackers
   exactly which of your directories are sensitive.

   Risk factor : Medium

. Warning found on port unknown (900/tcp)
```

```
    <html><head>
    <title>
      Authentication Form
    </title>
    </head>
    <p>
    <BODY BGCOLOR="#000000" TEXT="#00FF00">
    <FORM METHOD="POST" ACTION="http://131.74.248.254:900">

    <h3 align=left><font face="arial,helvetica">Client Authentication
Remote
    Service</font></h3>

    <INPUT TYPE="hidden" NAME="ID" VALUE="3df0c75e02fa"> <P>
    <INPUT TYPE="hidden" NAME="STATE" VALUE="1"><P>
    FireWall-1 message: User: <p> <P>

    Login : <INPUT NAME="DATA"> <P>

     press submit when done: <INPUT TYPE="submit"
    VALUE="Submit">. <P>

    </FORM>
    <p> <P>
    </BODY>
    </html>



 . Information found on port unknown (900/tcp)


    A web server is running on this port

 . Information found on port general/tcp


    Nmap found that this host is running Solaris 2.7 - 8 (SPARC)



-------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

APPENDIX B – Nmap scan reports

Sample of the SYN stealth scan against the firewall interface:
Command: nmap –sS –p 1-500 –P0 –v –oN scan_ss.txt 192.168.1.2

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
 Host  (192.168.1.2) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.1.2)
The SYN Stealth Scan took 248 seconds to scan 500 ports.
Warning:  OS detection will be MUCH less reliable because we did not find
at least 1 open and 1 closed TCP port
All 500 scanned ports on  (192.168.1.65) are: closed
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-linux-gnu%D=12/9%Time=3DF4C3A4%O=-1%C=25)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)



Nmap run completed -- 1 IP address (1 host up) scanned in 266 seconds
```

Sample of the FIN stealth scan against the interface.
Command: nmap –sF –p 1-500 –P0 –v –oN scan_ss.txt 192.168.1.2

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
 Host  (192.168.1.2) appears to be up ... good.
Initiating FIN Scan against  (192.168.1.2)
The FIN Scan took 601 seconds to scan 500 ports.
Adding open port 25/tcp
Adding open port 226/tcp
Adding open port 400/tcp
Adding open port 350/tcp
Adding open port 55/tcp
Adding open port 466/tcp
Adding open port 210/tcp
Adding open port 483/tcp
Adding open port 204/tcp
Adding open port 327/tcp
Adding open port 101/tcp
Adding open port 333/tcp
.
.
<cut>
.
.
Adding open port 282/tcp
Adding open port 428/tcp
```

```
Adding open port 317/tcp
.
.
<cut>
.
.
Adding open port 485/tcp
Adding open port 142/tcp
Adding open port 360/tcp
Adding open port 6/tcp
(no tcp responses received -- assuming all ports filtered)
 Warning:  OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
All 500 scanned ports on  (192.168.1.2) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-linux-gnu%D=12/9%Time=3DF4CD4F%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


Nmap run completed -- 1 IP address (1 host up) scanned in 822 seconds
```

Sample of the SYN stealth scan against the GIAC public DMZ:
Command: nmap –sS –p 1-500 –P0 –v –oN scan_ss.txt 192.168.1.66-70

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
 Host (192.168.1.68) appears to be up ... good.
Initiating SYN Stealth Scan against (192.168.1.68)
Adding open port 25/tcp
 The SYN Stealth Scan took 94 seconds to scan 500 ports.
Interesting ports on (192.168.1.68):
(The 499 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp
IPID Sequence Generation: Incremental

Host (192.168.1.69) appears to be up ... good.
Initiating SYN Stealth Scan against (192.168.1.69)
Adding open port 443/tcp
 Adding open port 80/tcp
 The SYN Stealth Scan took 94 seconds to scan 500 ports.
Interesting ports on (192.168.1.69):
(The 498 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https
IPID Sequence Generation: Incremental

Nmap run completed -- 5 IP addresses (5 host up) scanned in 229 seconds
```