Global Information Assurance Certification Paper

GCFW Practical Assignment
Version 1.6a

By Patricia Siow

Contents

1 Security Architecture

1.1 Introduction

GIAC Enterprises is an e-business company that deals in online sale of fortune cookie sayings. It started as a small sideline business started by a group of homemakers and has blossomed into a business with an annual turnover of 3 million dollars.

With ever increasing number of intrusions and website defacement on the Internet, GIAC enterprises has employed the security consultancy services of WeSecureU consultants to beef up the network security architecture.

1.2 How GIAC business operations work

In the past, GIAC offered the sale of fortune cookie saying through their company website hosted remotely on a local ISP's server. The order forms are downloaded from the company website by the customer. The completed forms are then faxed over to the GIAC. Only upon receiving a money order or check are the orders fulfilled and the printed product is sent to the customer's mailing address.

All the paper work and additional data entry impeded the growth of the business. It also takes up to 4 weeks to deliver the goods to the customer's mailing address.

With a new expansion plan, the company has subscribed to a leased line from the local ISP for the office internal LAN and now hosts the company website on their own servers which is located in a secure technical centre.

1.2.1 Customers

Fortune cookie sayings in English and Mandarin are now offered for sale directly on GIAC's secure website and customers are able to place their orders online. Customers are able to browse samples of the products and select the quantity and product type they wish to purchase. Discounts are offered to those who purchase in bulk.

Instead of handling cheques and money orders, only credit cards are accepted as the mode of payment. Card details and personal details such as name and contact email address must be entered at the time of purchase when the customer is placing their orders online. In order to safeguard the sensitive information sent across the Internet, customers access GIAC's secure website by using an SSL enabled browser. This ensures that the connection between the customer's browser and the server is encrypted. Customers are also able to verify the authenticity of GIAC's website through the Verisign digital server certificate on GIAC's webserver before entering their information.

Upon confirmation of payment, a computer generated login and password will be sent to the customer's email address. This temporary account valid for 2 weeks will allow

the user to download their product at leisure. The text formatted fortune sayings file allows the customers to change the document to the specific format they like.

1.2.2 Suppliers

Chinese astrological authors located in Hong Kong or Taiwan supplies the fortune sayings to GIAC Enterprises. Authors connect to GIACs VPN through the use of a VPN client. A encrypted VPN connection is established between the author's PC and the VPN server. The authors could then logon to the Suppliers server to submit or update their works written in Mandarin.

The supplier server runs a web application that allows authors to upload their works, manage their own accounts, read a web-based e-mail for use with GIAC and edit their works. These works are then translated and reformatted by GIAC Employers to English to be reformatted for sale online.

1.2.3 Partners

GIAC Enterprises also liaise with reseller partners to translate these works into other languages such as French, Spanish, Italian and German. These sayings are then repackaged and sold by their partners. GIAC needs to exchange product information with their partners. The partners log on to the Partner server place their orders and preview the product. They also upload customers information to GIAC as part of the agreement.

Partners also need access Partner server through a VPN connection. Similarly, they use a VPN client software to connect to the GIACs internal network. They then access the Partner server to view the products and upload customers information.

1.2.4 GIAC employees

GIAC employees maintain multiple servers such as the Partner, application, GIAC web and ACE Servers within the DMZ and Server LAN. GIAC employees also access the application server for the translation of the sayings to English.

The employees need to be able to access the Internet for Http and Https browsing, ftp. Company's mail is downloaded from the Internet to the mail server. It is also responsible for sending the company's mails.

1.3 Proposed Security Architecture

Consultants at WeSecureU drafted the following proposed infrastructure to strengthen the security of the architecture.

A layered approach is used to segregate the network into zones with different levels of risks for its exposure to the Internet and the type of traffic it receives.

A border router, Cisco 2610 with IOS version 12, provides the first line perimeter defense to the network. Access list implemented on a router before the firewall helps reduce the number of unnecessary or unauthorized packets that the firewall has to filter based on its policy. This improves the throughput and efficiency in processing the packets. A properly configured router is also able to defend the firewall against denial-of-service (DoS) attacks.

Checkpoint Firewall-1 4.1 is chosen as the firewall. It is built on Sun machine running Solaris 8. VPN option is also purchased to provide the VPN capability. The primary external firewall further filters the Internet traffic that reaches the GIAC's web, mail and DNS servers. Network Address translation is also performed to hide the private internal network addresses to avoid conflicts routing and addressing conflicts.

VPN-1 option purchased for the external firewall provides VPN capability integrated with firewall functionality. It allows partners and suppliers to connect to the application server to either download or upload the product. Combining VPN together 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.

NAT is performed at the perimeter firewall to allow external connections to reach the GIAC webserver. It is common to perform NAT nowadays as legal internet IPs are rare and limited. Private addresses are used to allow possible expansion of the network to cater to more points.

Within the DMZ LAN is the Mail, Web and DNS server. Since these servers are being exposed to the Internet and there is inflow of traffic from the public, it raises the risk of these servers being attacked and compromised. Similarly with suppliers and partners, though they are trusted users and there are cooperative relations with GIAC, it should still be handled as a 3rd Party access from an external entity. There should not be any direct access possible from the DMZ/3rd Party to the internal/servers LAN.

Even with a perimeter firewall already installed, it is still important to further limit the traffic access from the 3rd Party LAN to GIAC internal server and office lans. An internal firewall segregates the third-party LAN from GIAC's internal and servers network. This layered security approach serve to prevent intruders have compromised the DMZ to gain further access into GIACs sensitive database and application servers.

Should the suppliers or partners server be compromised for any reason, it is still segregated within the its own LAN with both external and internal firewalls controlling traffic to either DMZ, Internet, GIAC Servers and GIAC office network.

Caution should be taken when access to servers on a network is given to partners. The internal firewall limits access to servers in server LAN. All access to GIAC office and internal server LAN is denied. There are strictly confidential data that are not shared

with partners or suppliers.

The internal firewall also protects GIAC's internal servers from the office LAN, limiting only authorized employees to access the servers. To monitor any suspicious network activity on the DMZ, VPN and Server LAN, Network Intrusions Detection systems (NIDs) are implemented.

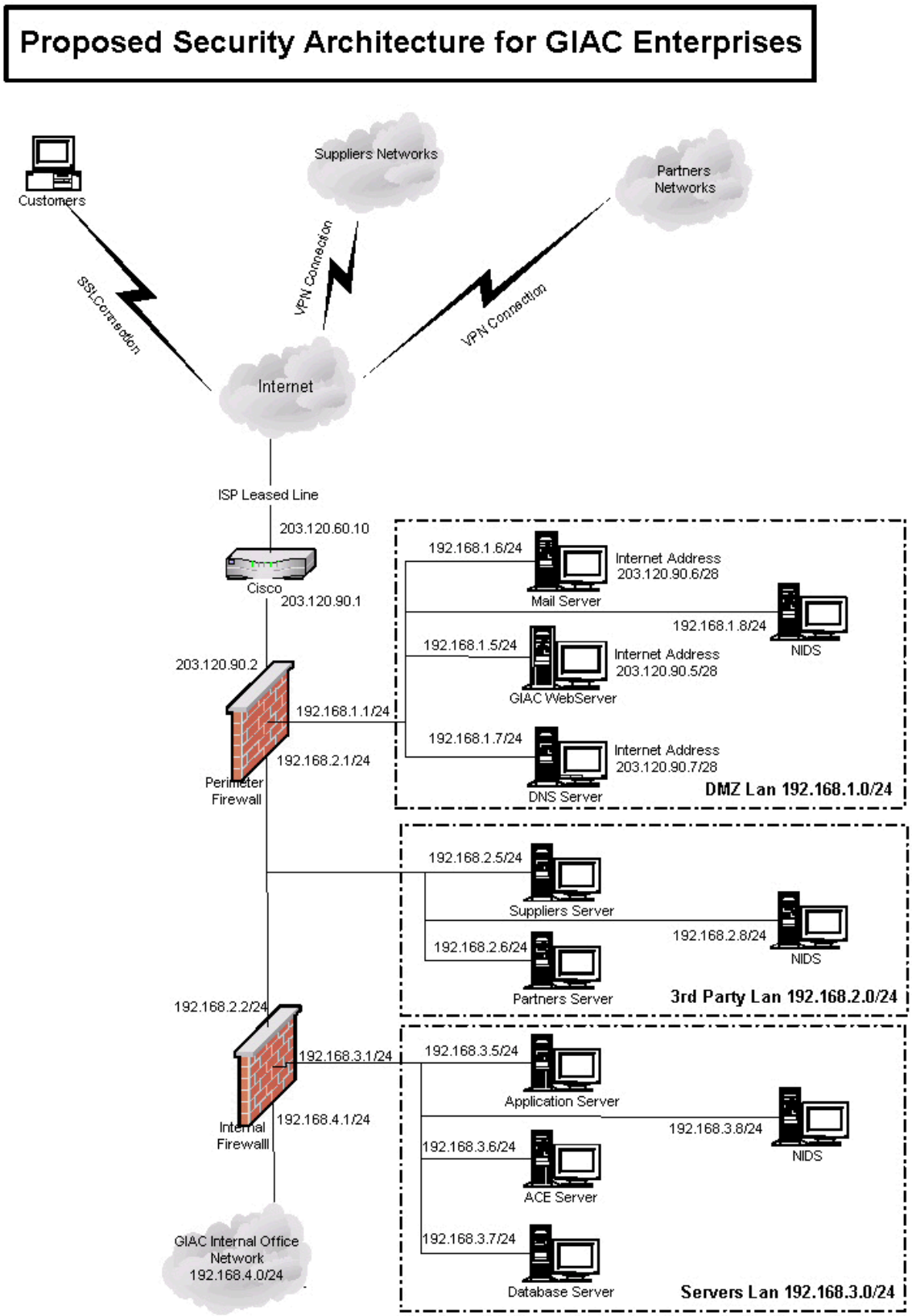
SecurID authentication was chosen to be the authentication method for VPN users to access the internal LAN. Advantage lies in better control over the quality of passwords. It is proposed that both GIAC employees and 3rd party users – Suppliers and Partners use SecurID authentication to access the various servers.

Summary and type of traffic by users is characterized in the table below

Users Type	***Requirements***	***Service***	***Access on***	***Via***
Customers	Normal web browsing Secure web browsing	TCP 80 (http) TCP 443 (https)	GIAC Web server	Perimeter firewall 203.120.90.2
Suppliers	VPN – Access web-based application. Upload and download of product files	TCP 80 (http) TCP 21 (ftp) TCP 20 (ftp-data)	Suppliers Server	Perimeter firewall 203.120.90.2
Partners	VPN – Access web-based application. Upload and download of product files	TCP 80 (http) TCP 21 (ftp) TCP 20 (ftp-data)	Partners Server	Perimeter firewall 203.120.90.2
GIAC employees (From internal network 192.168.4.0)	Surf the Internet Download files	TCP 80 (http) TCP 443 (https) TCP 21 (ftp) TCP 20 (ftp-data)	Any server outside internet.	Internal firewall + Perimeter firewall
	Download and send mail	TCP 110 (POP-3) TCP 25 (SMTP)	Mail Server	
	Download upload files, Telnet	TCP 21 (ftp) TCP 20 (ftp-data) TCP 22 (telnet-ssh)	GIAC Web server	
	Download upload files, Telnet	TCP 21 (ftp) TCP 20 (ftp-data) TCP 22 (telnet-ssh)	Suppliers Server Partners Server	Internal firewall
	Download and upload files Telnet	TCP TCP 22 (telnet-ssh)	Application Database	Internal firewall

Additional Traffic between Servers and Internet going through firewalls

Server Type	***Requirements***	***Service***	***Via***
Mail	Send and Receive mails from Internet	TCP 25 (SMTP)	Perimeter firewall
Web	Serves WebPages to Internet	TCP 80 (http) TCP 443 (https)	Perimeter firewall
DNS	Receive and Distribute DNS updates	TCP 53 (DNS) UDP 53	Perimeter firewall
Supplier	Receive product file from Application Server	FTP	Internal firewall
Partner	Receive product file from Application Server	FTP	Internal firewall
Application	Send product file to Supplier, Partner and Web Server	FTP	Internal firewall + Perimeter
ACE	Allow SecurID authentication traffic to perimeter firewall for VPN connections	TCP (SecurID)	Internal firewall + perimeter
Database	SQL traffic between Suppliers and Partners Server	TCP (SQL)	Internal firewall



2 Security Policy

The network architecture can be well designed but without a sound and tight security policy, each perimeter defense fails to act to its full potential in defending the network against the external world.

2.1 Border Router Configuration

The router is the first perimeter system to handle all the packets from the Internet. When implemented correctly with right access-lists, helps to clear off most of the noise or unwanted traffic from entering the network.

Cisco IOS provides extensive commands and controls to allow the administrator to easily configure the way traffic is handled when it passes through into the network. It also has extensive security features to ensure the router is not compromised easily.

2.1.1 Security policy for Router

ISP has allocated us the public IP address subnet of 203.120.90.0/28
Connection to the ISP from our router is 203.120.60.10
Internal facing interface for border router: 203.120.90.1
Perimeter firewall interface facing router: 203.120.90.2
Internet address for web server: 203.120.90.5
Internet address for mail server: 203.120.90.6
Internet address for DNS server: 203.120.90.7

(Note The IP addresses chosen here are for example purposes. Coincidental with real networks are not reflective of those networks out there.

```
!Connection from ISP
Interface serial0/0
ip address 203.120.60.10 255.255.255.255
ip access-group 101 in
no ip redirects
no shutdown
no ip redirects
no ip directed-broadcast
no ip proxy-arp
no ip mroute-cache
ntp disable
no cdp enable

! Deny private and reserved addresses from even reaching the
servers
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.15.0.0 0.240.255.255 any log
access-list 101 deny ip 192.168.0.0 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 host 0.0.0.0 any log 0
```

```
! Deny own allocated IP addresses from entering in. Definitely
faked.
access-list 101 deny ip host 203.120.90.60 any log
access-list 101 deny ip 203.120.90.0 0.0.0.224 any log

! Deny incoming netbios traffic
access-list 101 deny ip any any range 135 139
access-list 101 deny ip any any eq 445

! Permit only packets going to DMZ Servers and perimeter firewall
! Access http and https for web server, smtp for mail and DNS
traffic

access-list 101 permit tcp any host 203.120.90.5 eq 80 log
access-list 101 permit tcp any host 203.120.90.5 eq 443 log
access-list 101 permit tcp any host 203.120.90.6 eq 25 log
access-list 101 permit tcp any host 203.120.90.7 eq 53 log
access-list 101 permit udp any host 203.120.90.7 eq 53 log

! Permit reply packets from Internet back to office LAN. NAT
performed at firewall to translate destination to office host.

access-list 101 permit tcp any host 203.120.90.2 eq 80 established
log
access-list 101 permit tcp any host 203.120.90.2 eq 443
established log
access-list 101 permit tcp any host 203.120.90.2 eq 21 established
log
access-list 101 permit tcp any host 203.120.90.2 eq 20 log

! Permit FWZ authentication to firewall
access-list 101 permit tcp any host 203.120.90.2 eq 264 log
access-list 101 permit udp any host 203.120.90.2 eq 259 log

! Deny all others
access-list 101 deny ip any any log

Interface fastethernet0/0
ip address 203.120.90.1 255.255.255.0
ip access-group 102 in
no shutdown
no ip redirects
no ip directed-broadcast
no ip proxy-arp
no ip mroute-cache
ntp disable
no cdp enable

! Deny outgoing netbios traffic
access-list 102 deny ip any any range 135 139
access-list 102 deny ip any any eq 445

! Prevent spoofed packets from own network from entering the
Internet
access-list 102 deny ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny ip 127.0.0.0 0.255.255.255 any log
access-list 102 deny ip 172.15.0.0 0.240.255.255 any log
access-list 102 deny ip 192.168.0.0 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 host 0.0.0.0 any log

! Access http and https for web server, smtp for mail, DNS traffic
access-list 102 permit tcp host 203.120.90.5 any eq 80 established
log
access-list 102 permit tcp host 203.120.90.5 any eq 443
established log
access-list 102 permit tcp host 203.120.90.6 any eq 25 log
access-list 102 permit tcp host 203.120.90.7 any eq 53 log
access-list 102 permit udp host 203.120.90.7 any eq 53 log
access-list 102 deny any log

! Permit FWZ key exchange and FWZ encrypted sessions
access-list 101 permit tcp host 203.120.90.2 any eq 264 log
access-list 101 permit udp host 203.120.90.2 any eq 259 log

! Used to deny any terminal access
access-list 103 deny   ip any any log
!
line vty 0 4
 access-class 103 in
login
```

2.2 Perimeter and Internal Firewall

Check Point Firewall-1 4.1 offers HA capability. Additional license must be purchased for Firewall-1 HA option. To implement load balancing, clustering software like StoneBeat Fullcluster could be used. However, likewise license for use of such software comes at a much higher price. Due to cost constraints, only a single firewall is implemented. The platform chosen for this implementation is Solaris 8.

Perimeter machine is installed with a quad FastEthernet that comes with 4 ports.

- Eth0 : 203.120.90.2
- Eth1 : 192.168.1.1
- Eth2 : 192.168.2.1
- Eth3 : Not used

Internal machine is installed with a quad FastEthernet that comes with 4 ports.

- Eth0 : 192.168.2.2
- Eth1 : 192.168.3.1
- Eth2 : 192.68.4.1
- Eth3 : Not used

2.2.1 Security Policy for Perimeter Firewall

No.	Src	Dest	Service	Action
1	Any	203.120.90.5 Web Server	TCP 80 (http) TCP 443 (https)	Permit

2	Any	203.120.90.6 Mail Server	TCP 25 (smtp)	Permit
3	Any	203.120.90.7 DNS Server	TCP 53 (DNS) UDP 53 (DNS)	Permit
4	192.168.3.6 ACE Server	192.168.2.1 Internal facing Perimeter firewall	SecurID	Permit
5	Suppliergrp@Any	192.168.2.5 Suppliers Server	TCP 80 (http) TCP 21 (ftp)	Client Encrypt
6	Partnergrp@Any	192.168.2.6 Suppliers Server	TCP 80 (http) TCP 21 (ftp)	Client Encrypt
7	192.168.3.5 Application	192.168.1.5 Web Server	FTP 21 (ftp)	Permit
8	192.168.4.0/24	Any	TCP 21 (ftp) TCP 80 (http) TCP 443 (https)	Permit
9	192.168.4.0/24	192.168.1.7 DNS Server	TCP 53 (DNS) UDP 53 (DNS)	Permit
10	192.168.4.0/24	192.168.1.6 Mail Server	TCP 110 (POP3) TCP 25 (SMTP)	Permit
11	Any	Any	NETBIOS	Deny
12	Any	Any	Any	Deny

2.2.2 Security policy for Internal Firewall

User authentication is another feature provided by CheckPoint Firewall that allows filtering based on the type of users and the address from which they come from.

In our policy rules shown below, source limits a particular user coming from the office LAN network. The type of user authentication is set when the user object is created on the firewall. In our case, we imposed a policy that all user authenticating through the firewall must be done via SecurID authentication.

No.	Src	Dest	Service	Action
1	192.168.3.6 ACE Server	192.168.3.1 Internal FW 192.168.2.1 Perimeter FW	SecurID	Permit
2	192.168.4.0/24	192.168.1.6 Mail Server	POP3 SMTP	Permit
3	192.168.4.0/24	Any	Http Https FTP	Permit

4	GIACuser@192.168.4.0/24	192.168.3.5 Application server	FTP Tel - SSH	User authentication
5	Dbadmin@192.168.4.0/24	192.168.3.7 Database Server	FTP Tel - SSH	User authentication
6	Supplieradmin@192.168.3.5	192.168.2.5 Suppliers Server	FTP Tel – SSH	User authentication
7	Partneradmin@192.168.3.5	192.168.2.6 Partners server	FTP Tel - SSH	User authentication
8	192.168.3.5 Application server	192.168.2.5 Supplier Server 192.168.2.6 Partner Server 192.168.1.5 Web server	FTP	Permit
9	192.168.3.7 Database Server	Application Server Supplier Server	SQL	Permit
10	Any	Any	NETBIOS	Deny
11	Any	Any	Any	Deny

2.2.3 Network Address Translation

Network Address Translation (NAT) is performed at the firewall to translate the internet addresses of the following servers to internal addresses of servers.

Server	Internet IP	Internal IP	Comments
Web Server	203.120.90.5	192.168.1.5	Performed on destination address for incoming connections.
Mail Server	203.120.90.6	192.168.1.6	Performed on destination address for incoming connections. And source address for outgoing connections
DNS Server	203.120.90.7	192.168.1.7	
Office LAN	203.120.90.2	192.168.4.0/24	Performed on source address for outgoing connections. Office LAN hides behind Internet facing interface

Translation rule set on Perimeter Firewall

(No translation of addresses was necessary on the Internal Firewall)

Src	Dest	Service	XSrc	XDest	XServ
Any	203.120.90.5 Web Server	TCP 80 (http) TCP 443 (https)	= original	192.168.1.5	= original
Any	203.120.90.6 Mail Server	TCP 25 (smtp)	= original	192.168.1.6	= original
Any	203.120.90.7 DNS Server	TCP 53 (DNS) UDP 53 (DNS)	= original	192.168.1.7	= original

192.168.4.0/24 Office LAN	Any	TCP 80 (http) TCP 443 (https) TCP 21 (ftp)	203.120.90.2 firewall interface	= original	= original

2.3 VPN

Check Point VPN-1 is used with Firewall-1 as it's easier to integrate into the firewall functionality and promote a more integrative front.

2.3.1 User Authentication method

Several kinds of authentication methods are available on the firewall. It includes SecurID, firewall username and passwords, RADIUS and others. The use of SecurID cards with ACE Server was chosen as the authentication method. The obvious advantage of using token authentication lies in preventing the use of weak passwords and greater control on the quality of password. It may be more expensive then just maintaining the users via a simple username password but it is worth the added security and control.

ACE server is placed behind the internal firewall on the server LAN 192.168.3.x to protect it from possible attacks. It is not be internet addressable and specific rules on both firewall permit only SecurID traffic between the perimeter firewall and ACE server.

2.3.2 VPN Client configuration

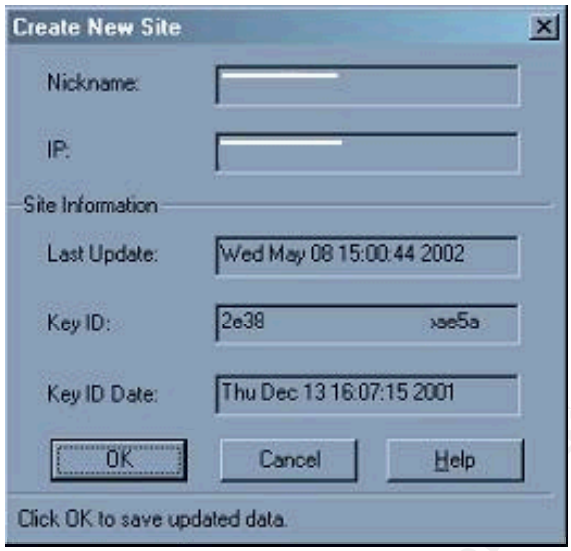
Users can either use a VPN client – SecurClient or SecuRemote to connect to the GIAC's networks. The difference between a SecuRemote and a SecurClient lies in SecurClient has the ability to impose a desktop security policy on the users connecting to your internal network.

Firewall administrators are able to filter the type of traffic coming into the Internal networks via VPN as well as impose a stricter policy on the user's desktop to prevent that as the weak point in the perimeter defense.

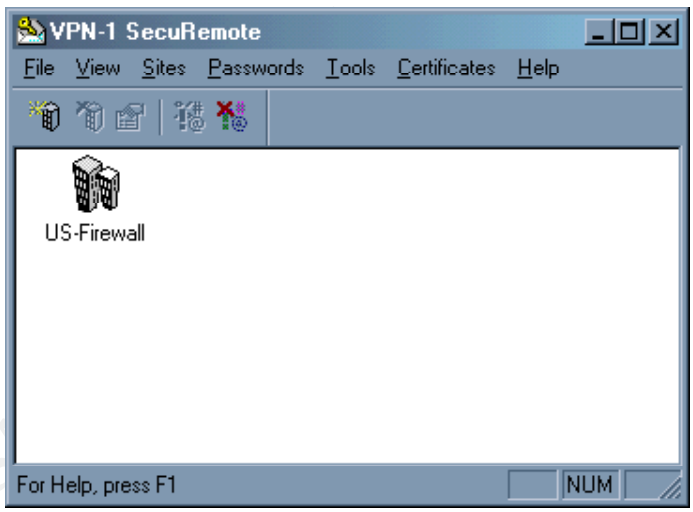
To configure the VPN client, a site is first added on the client. This site is generally referred to the management server of the firewall. If the management server resides on the same machine as the firewall module, the IP address of the firewall is used. However, if the management server resides on a different machine, as in the case when implementing clusters and HA solution. It is necessary to ensure that the VPN clients are able to contact the management server to download the server encryption keys.

To add a site, the user gives the site a name e.g. US-FW or EU-FW. Next, add the IP of the management server. Like mentioned, it is necessary that the VPN client is able to route to this address. If the management server resides behind the firewall and there are no direct routable paths between the VPN client and the management server, a policy and address translation rule could be added to ensure the key retrieval traffic is routed to the management server. SecurClient contacts management station on TCP Port 264 to fetch the encryption keys and the network topology.
SecurClient and Firewall also use UDP Port 259 to manage the FWZ encrypted

sessions.
An example of the screenshot is shown below on the next page. The IP and Key ID are blanked out anonymity purposes.



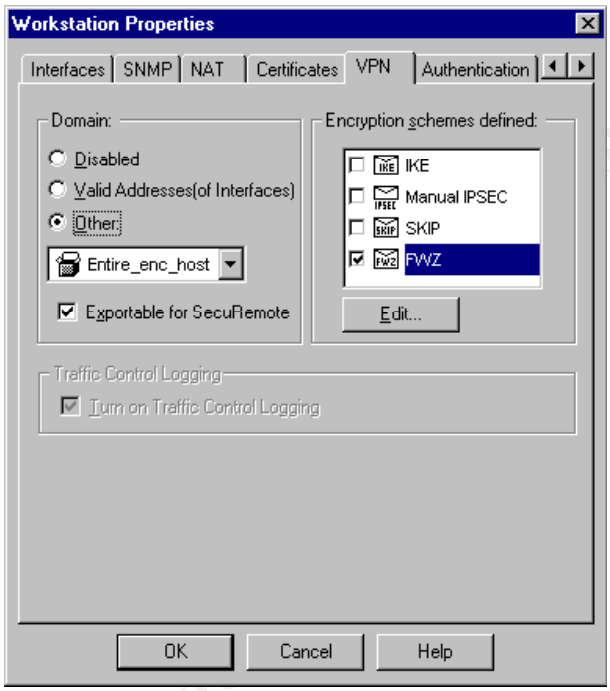
Once added, the VPN client will contact the management server to retrieve the server keys. This key is used in tunnel encryption between the client and firewall. The user should check that the server key is correct to ensure that they are connecting to the right firewall and not a bogus one. The firewall administrator could relay the server key string to the user prior setup. FWZ is selected as the encryption scheme.



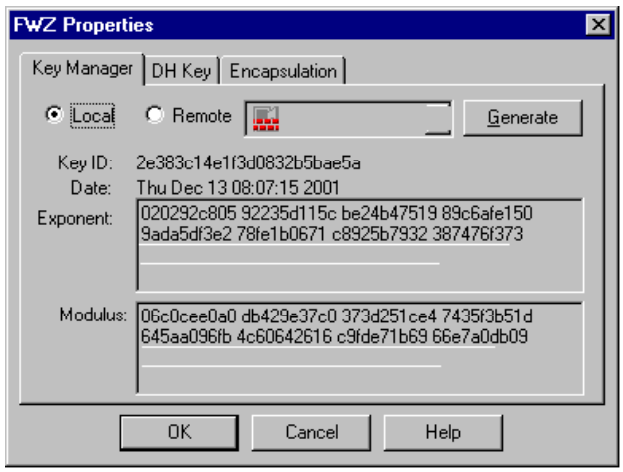
2.3.3 VPN configuration on Firewall object

To enable the use of VPN, an encrypted domain must first be created. By definition, encrypted domain is the area within the network which needs protected by VPN. This group of servers, Entire_enc_host is then specified in the firewall configuration under the VPN tab.

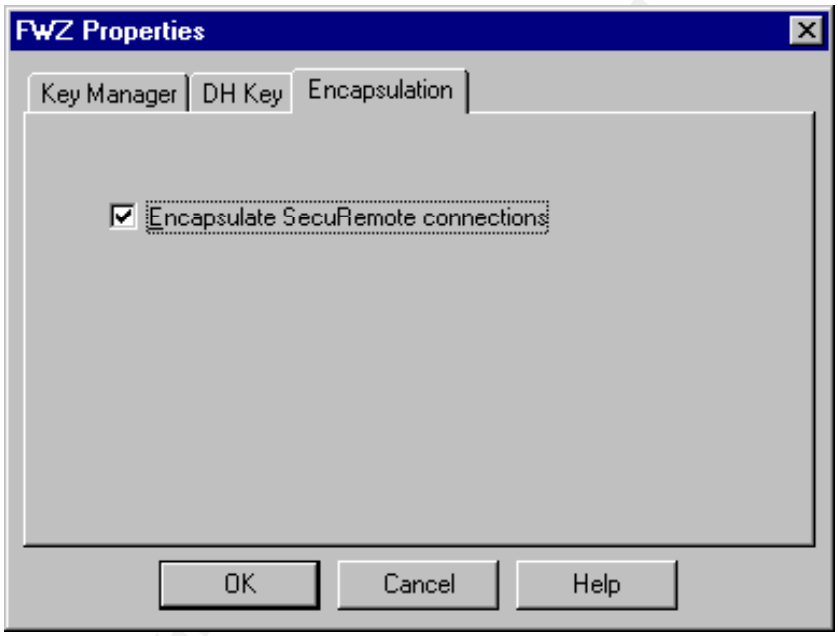
Specify the group of encrypted host as the domain and select "Exportable for SecuRemote". Next choose the type of encryption scheme and in our case, is FWZ. The screen capture is shown below



- Click "Edit" under the encryption scheme defined. Use the generate button to generate server keys. Similarly, under the DH Key tab, use the generate button. To generate a pair of DH key.



- And lastly, remember to select "Encapsulate SecuRemote connections" under the Encapsulation tab.



2.3.4 SecurClient or SecurRemote

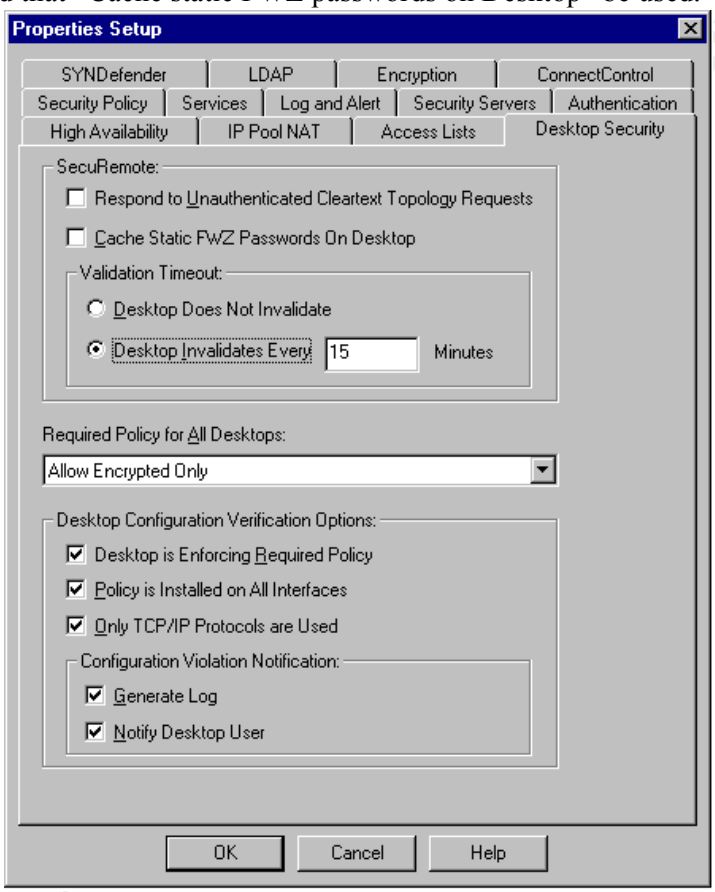
Maintaining vendor/partner relations has always been tricky. While there is obvious collaboration between both parties, there should not be a compromise in GIAC's security.

It is recommended that Desktop policies be imposed on any 3rd party VPN connections. While it is difficult to rationalize with some vendors, this is to prevent their computers from being used as a launch board for attacks on GIAC's networks.

For example, in the firewall preference tab, it is possible to impose either outgoing and/or incoming traffic to be encrypted. This means the firewall administrator is able to prevent the remote user from connecting to the GIAC 3rd party servers and Internet at the same time.

It was found that it is possible to discover the topology of the encrypted domain by attackers sending SecuRemote topology request packets. It is recommended that the option "Respond to Unauthenticated cleartext topology request" be **unselected.**

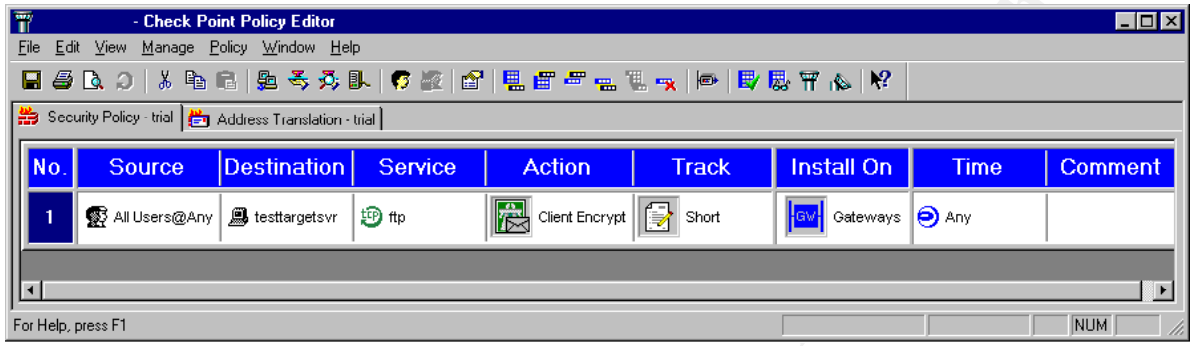
In general, if static passwords are used as authentication method, it is not recommended that "Cache static FWZ passwords on Desktop" be used.



2.3.5 Policy rule

Based on the rule on the firewall, policy rule of a typical VPN connection is of the following format

Source	Destination	Service	Action	Installed on
User@Network address	Target Server	Service type e.g.. Telnet or FTP	Client Encrypt	Perimeter gateway



Authentication takes place at the perimeter firewall. When the user initiates a connection with the server they wish to contact in the encrypted domain, the SecurClient contacts the firewall.

The firewall checks the incoming packet based on 2 criteria - 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 when the user authenticates successfully.

The packet is encapsulated and sent within the tunnel between the SecurClient and the firewall. By encapsulation, it means that the packet is encrypted and "wrapped" within a packet and a new header with the firewall address as the destination. This allows a user to connect to the server behind the firewall whose address not routable on the Internet. Only upon reaching the firewall, it is then unwrapped and the packets' destination address is once again the real IP of the target. The firewall also changes the source of the packet to the internal interface of the firewall (i.e. 192.168.1.1) before it is routed towards the target server.

- When client attempts to connect to target server (196.168.2.2) within encrypted domain

Source	Destination	Service	Location of packet
Remote user's PC address 196.10.1.156	Target Server IP address 192.168.2.2	FTP	At VPN Client on desktop user
Remote user's PC address 196.10.1.156	Firewall's internet address 203.120.90.2	IPSEC	Encapsulated within the tunneled traffic. In transition to firewall

Internal facing Firewall's interface 192.168.1.1	Target Server IP address 192.168.2.2	FTP	Unwraps at firewall interface. Emerges from encrypted tunnel

- Similarly, when the reply packet undergoes similar encapsulation to reach the remote user at the other end of the VPN tunnel.

Source	Destination	Service	Location of packet
Target Server IP address 192.168.2.2	Internal facing Firewall's interface 192.168.1.1	FTP	Reply packet from target server to user.
Firewall's internet address 203.120.90.2	Remote user's PC address 196.10.1.156	IPSEC	Encapsulated within the tunneled traffic. In transition to VPN client on user's desktop
Target Server IP address 192.168.2.2	Remote user's PC address 196.10.1.156	FTP	Unwraps and emerges from tunneled traffic. Passed to application software for processing.

This method is useful as it does not require additional address translation rules on the firewall to resolve address conflict and routing problems. The encapsulation of traffic is handled by the Firewall-1 VPN component. It allows a user to connect to the real IP of the server and establish the connection required.

Naturally this method assumes that from the point of the firewall to the target server, the address unwrapped at the end of the firewall is routable. The routing table should be checked to ensure that the packet is able to route to the target server.

2.4 Implementing border router

2.4.1 Logins & Passwords

Cisco 2610 router allows configuration via several methods. However, it is highly recommended that the router be managed via local console only. Logins to routers should be strictly controlled as it is the first line of perimeter defense from the Internet and remote logins are not recommended.

Command "**service password-encryption**" is used to encrypt and password ensure that the password is not stored in clear text, hence even if someone manages to read the configuration on the router, it would prevent them from easily reading the password.

"**enable secret**" command is used to set a password to grant access to the privileged command level. It should be noted that if no **enable secret** password were set, anybody with remote terminal access to the router would be able to gain privileged access. Hence, it is important to deny remote terminal login if unnecessary. This is prevented by **not** configuring a password for the VTY line. Without a password applied, no one will be able telnet to the router.

2.4.2 Physical Security

Only authorized personnel should be permitted access to the router and strong password should be chosen and well kept. Physical security of the router is also important as one is able to gain control of a Cisco router if physical access via the console is obtained. A BREAK signal sent via console port permits a password recovery procedure. Hence an attacker with the ability to disrupt power and induce a system crash can gain control if a

The equipment should be kept in a secure room with restricted login access via smart card or other secure means.

2.4.3 Loading configuration

Administrators can connect to the console port on the Cisco 2610 via RS232 rollover cable from the serial port of a PC. Using a terminal program such as Hyperterm, login through the console allows the user to configure the router using specific Cisco commands.

Alternatively, the administrator can load a configuration as shown in Appendix I. After login in and enabled for configuration access and entering "**conf t**" at the prompt, use "**send text file**" option in hyperterm to download the full configuration text file to the router.

2.4.4 Global Configuration

The following configuration switches off unnecessary services such as finger and dhcp in our setup. By a basic security principle, all unnecessary services should be removed.

```
no service finger
no service dhcp
no cdp run
no service udp-small-servers
no service tcp-small-servers
no ip bootp server
no ip http server
no snmp-server
no ip source-route
no ip domain-lookup
enable secret secretpw
service password-encryption
service tcp-keepalives-in
service timestamps log datetime
logging buffered 32768
scheduler interval 500
```

Setting a banner warns intruders of illegal attempts to access the router when they login and when the router starts up.

```
banner login #
This system is private.
Legal Action will be taken against anyone attempting
unauthorised access.
This system is subject to monitoring at any time.
#
banner exec #
This system is private.
Legal Action will be taken against anyone using this
system without authorisation.
This system is subject to monitoring and logging at any
time
#
```

2.4.5 Interface Configuration

```
ntp disable
no ip directed-broadcast
no ip proxy-arp
no ip redirects
no ip unreachables
no ip mroute-cache
ip verify unicast reverse-path
```

2.4.6 Routing

There are a few security issues to take note of:

- static routing is always safer than dynamic routing and should be used by default.
- where a router is connecting to several different client networks ensure that the routing is not allowed between the clients. ACLs should disallow inter-client network connections
- if using dynamic routing, make use of route authentication (md5 key) where possible
- use `distribute-list list in` to restrict route to prevent their routers from accepting clearly incorrect routing information.

2.4.7 Logs

Logging capability is available on the routers and logs are useful for troubleshooting. Logs can be stored in the memory and they are output to the console by default. The following commands can be used and are explained as follows

- Logs useful for troubleshooting saved in buffer memory

```
logging buffered 32768
```

- Logs are pointless without a reliable timestamp.

```
service timestamps log datetime
```

- Channeling the logs to a remote system is also possible. Where it is necessary to log to a syslog server (e.g. 10.1.1.1) :

```
logging 10.1.1.1
logging trap debugging
logging facility local7
```

Syslog daemon on Solaris can be configured in etc/syslog.conf.

2.4.8 Access Control List (ACL)

There are a few types of ACLs that the IOS accepts: Dynamic, CBAC (only with Cisco IOS FW) and Reflexive. Standard/extended static access lists with TCP Intercept to prevent DOS attacks, is used in this border router implementation.

The aim of ACLs is to provide access control between networks. Access is usually based on:

- source ip and port
- destination ip and port

The default access control is to deny all traffic unless specifically allowed.
The syntax is:

Step	Command	Purpose	
1	**access-list** *access-list-number* **{deny | permit} tcp any** *destination destination-wildcard*	Define an IP extended access list.	
2	**ip tcp intercept list** *access-list-number*	Enable TCP intercept.	
3	**ip access-group** *{access-list-number | name}* **{in | out}**	Apply to interface	OR
	access-class *access-list-number* **{in | out}**	Apply to line	

The following points are noted when creating the access-list

- Rules are compared sequentially, place most frequently access rules first.
- Rules permit only authorized services while denying all others
- Apply access-group in to each interface.
- Rules should be of sufficient granularity in defining IPs, ports, protocols and flags. See examples.
- TCP intercept available on IOS
- Make use of TCP flags like **established** to prevent active connection backwards (i.e. TCP handshake from the other side).
- Apply deny all rule to vty. If no passwords are applied to vty, telnet will be unsuccessful.
- HTTP access should be **denied**. This is because http does not provide sufficiently strong authentication for remote management.
- Be careful of destination wildcards. Wildcards are the opposite of netmasks.

- When providing a service to the public on Internet where any is used as the source, insert ACLs to prevent reserve addresses from being passed on.

  E.g..

```
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip 224.0.0.0 7.255.255.255 any
access-list 101 deny   ip host 0.0.0.0 any
```

- There is an implicit deny all when ip access-group is applied to interface. The reason for explicitly defining it is to allow logging.

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

- When there is potential for false positives (e.g. caused by Microsoft Netbios), place the denys before the last line and do not log

```
access-list 101 deny ip any any eq 139
access-list 101 deny ip any any log
```

3 Audit of Primary Firewall

In order to carry out a thorough audit on the primary firewall, the auditors must first understand the requirements and constraints of the firewall. A discussion is held between the auditors, IT managers and firewall administrators to understand what the system is running and how it is being run.

3.1 Audit Plan

In order to fully understand the requirements, the system design and architecture documents and network diagrams are reviewed. Based on the requirements, only those service ports required are opened. Random tests are drawn up to ensure that the firewalls are operating as designed.

Next, a closer look will be also done on the configuration of the underlying operating system. Minimal services should be start up and permissions properly configured to allow only those authorized to make proper changes.

Configuration on what to log and how the logs are maintained are also taken into consideration. Recommendations will be given to the IT managers and firewall administrators to improve the firewall configuration based on the audit results.

With all the information needed, network diagram is reviewed and it is understood that the firewall is placed behind a border router. Hence a scan will be carried out on the internet address of the firewall from the Internet to. A port scan is also carried out behind the router just before the firewall.

It is planned that the audit of the systems will be conducted during after office hours preferably on weekends as security scans might significantly slow down the systems bringing operations to a halt. Certain scans such as port scans may take significantly longer time to complete as it covers all 65535 ports. The machines required for the scans will be prepared a day in advance by the auditor.

Prior to any audit or scans, the auditor request for a full system backup to be taken such that full recovery is available should the audit or scan crash the system. An alert is sent out a few days before the weekend informing users of the maintenance downtime.

3.2 Implementation of the Audit

3.2.1 Port Scan and Results

To run a port scan, Nmap tool by Fyodor is used for scanning. First check that the ports that opened are only those allowed in the architecture design.

Running the port scanner from a Redhat Linux machine, the following parameters are

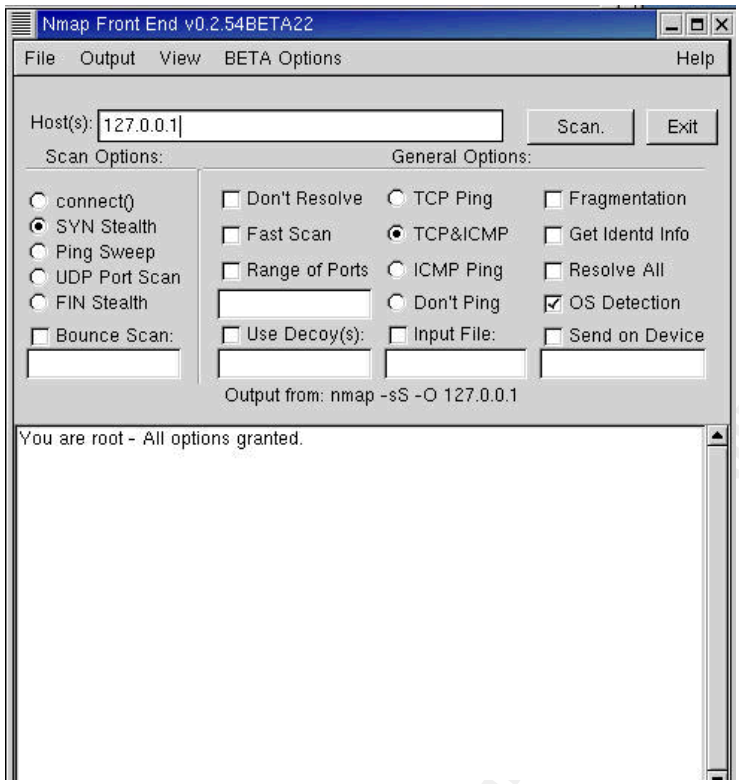
used. Apart from scanning the TCP ports, UDP ports are scanned as well.

nmap –sS –p 1-65535 –P0 –v -oN output_ss.txt 203.120.90.2
nmap –sU -p 1-65535 –P0 –v -oN output_su.txt 203.120.90.2
 # nmap –sT –p 1-65535 –P0 –v –oN output_st.txt 203.120.90.2
 # nmap –sF –p 1-65535 –P0 –v –oN output_st.txt 203.120.90.2

-sS	indicate a **Stealth SYN** TCP Scan.
-sU	indicates a **UDP Port** Scan.
-sT	indicates a TCP Connect Scan
-sF	indicates a **Stealth FIN** TCP Scan. Sometimes certain ports are filtered. Hence by sending a FIN packet, certain systems return a RESET packet hence betraying its presence.
-p 1-65535	indicates the port range to scan. Full number of ports = 65535
-P0	indications **Don't ping**. This option was chosen because many firewalls do not respond to ping. Hence this would force the scan to go ahead regardless.
-v	verbose output.
-oN	create an output text readable file.

A Nmap Front-End GUI interface is also available for use.

nmapfe &



3.2.2 Vulnerability Scan

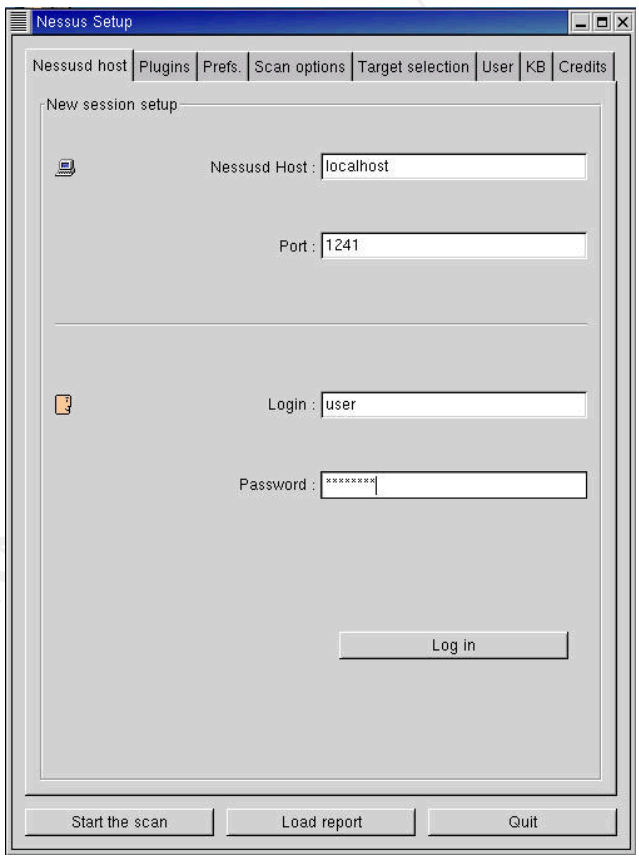
Apart from scanning for open ports on the firewall, vulnerability scanning could also be done to discover any unknown vulnerability. Nessus is a free popular security scanner used by administrators to audit their own systems. It can be downloaded for free and runs on both Linux and Windows platform.

The scanner works in a server engine - client GUI mode. A database of vulnerability test plugins is loaded onto the server engine. The client with a GUI interface connects to the server to configure and activate the scan need. Different group categories such as Windows platform, CGI abuses etc can be chosen. The scanner also includes an inbuilt Nmap scanner that allows the user to perform TCP and UDP scans.

In this case in our audit, the Nessus server and client reside on the same machine running on Redhat Linux 7.2. Version of Nessus used is 1.2.0. The latest plugins are downloaded and used.

Logging in using the Nessus client

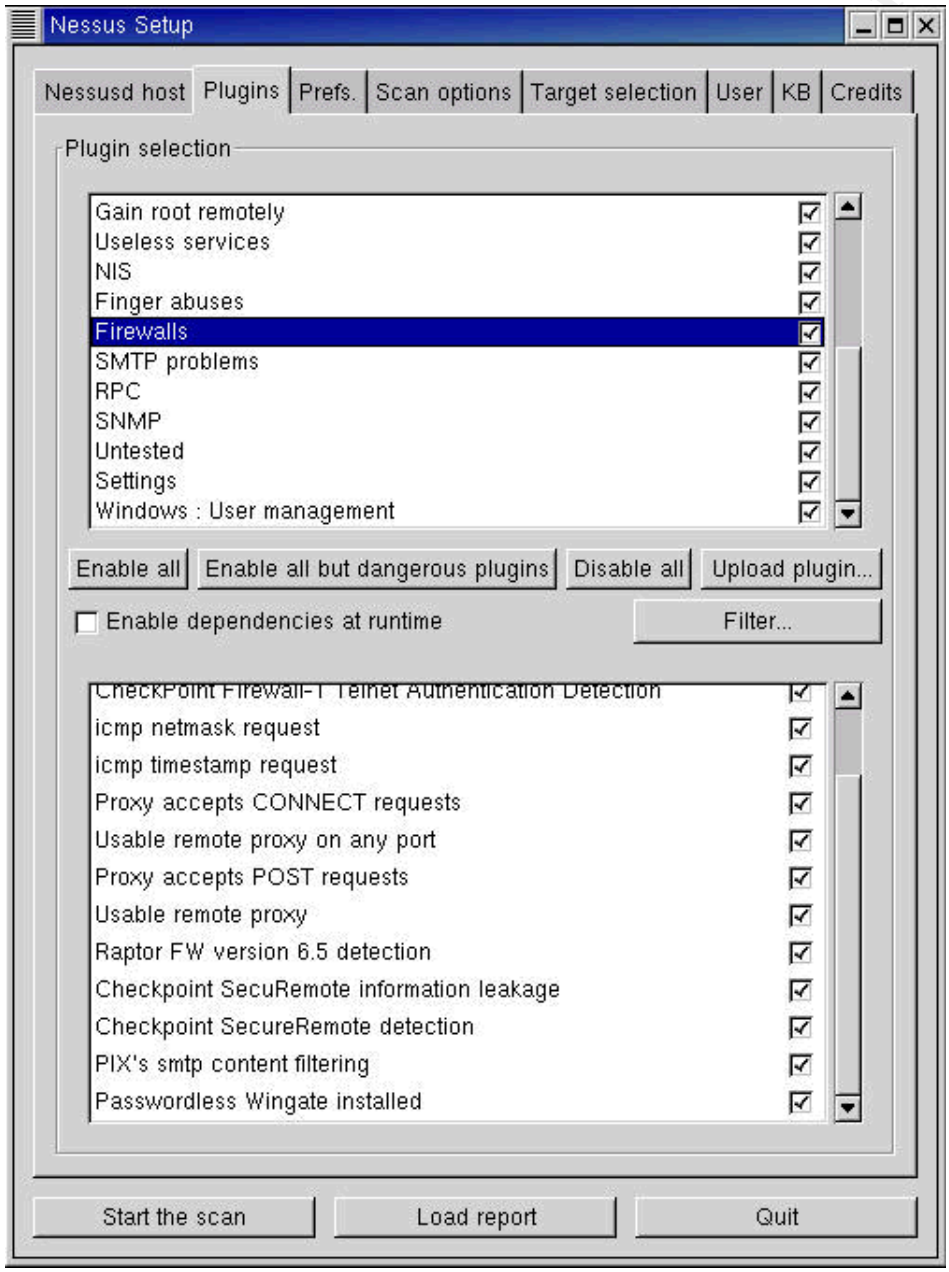
The following shows the screenshot of the Nessus client. Nessusd host refers to the server and in this case it resides on the same machine. When setting up the login accounts on the Nessus Server, users are created.



Selection of Plugins Page

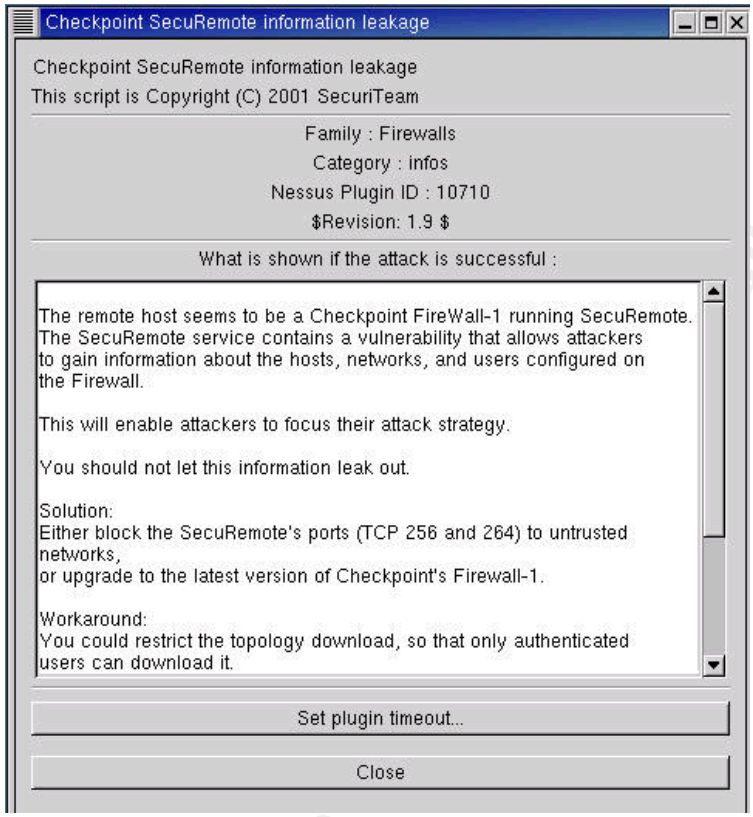
The Plugins page refers to the attack scripts that will be launched on the selected target. Plugins are generally categorized into different areas usually specific to certain platform, software or vulnerabilities.

As shown in the screenshot below, there are specific tests targeted at firewalls. Security administrators that don't wish to waste too much time running through all the redundant scripts might just want to select this category only.



Plugins Information window

Administrators can even select specific vulnerability and read more about it in the plugins information window.



Run command #nessus-update-plugins prior to activating the nessus client. This command activates a script to automatically download the latest plugins from the Nessus website.

Prior to any security and vulnerability testing, the auditor should ensure a full backup of the system is taken. This is to provide a recovery method should certain scripts used by Nessus to cripple the whole network or bring the system down. Such plugins are highlighted as dangerous and used with extra care.

If time permits, the auditor should run all the scripts available to discover all possible vulnerabilities. However, with limited time some recommended options used to audit the primary firewall are:

Plugin Categories :

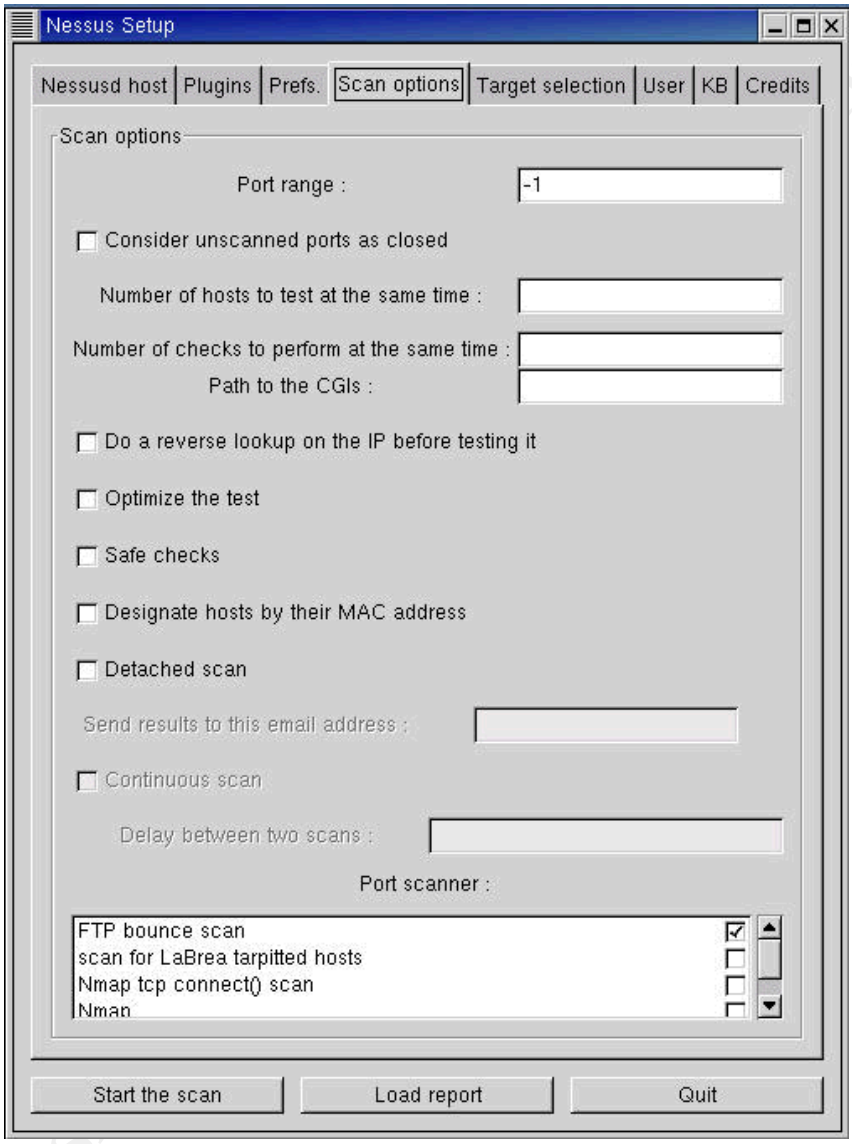
- Firewall
- General
- Gain a shell remotely
- Gain root remotely

- Denial of Service

Scan options configuration page

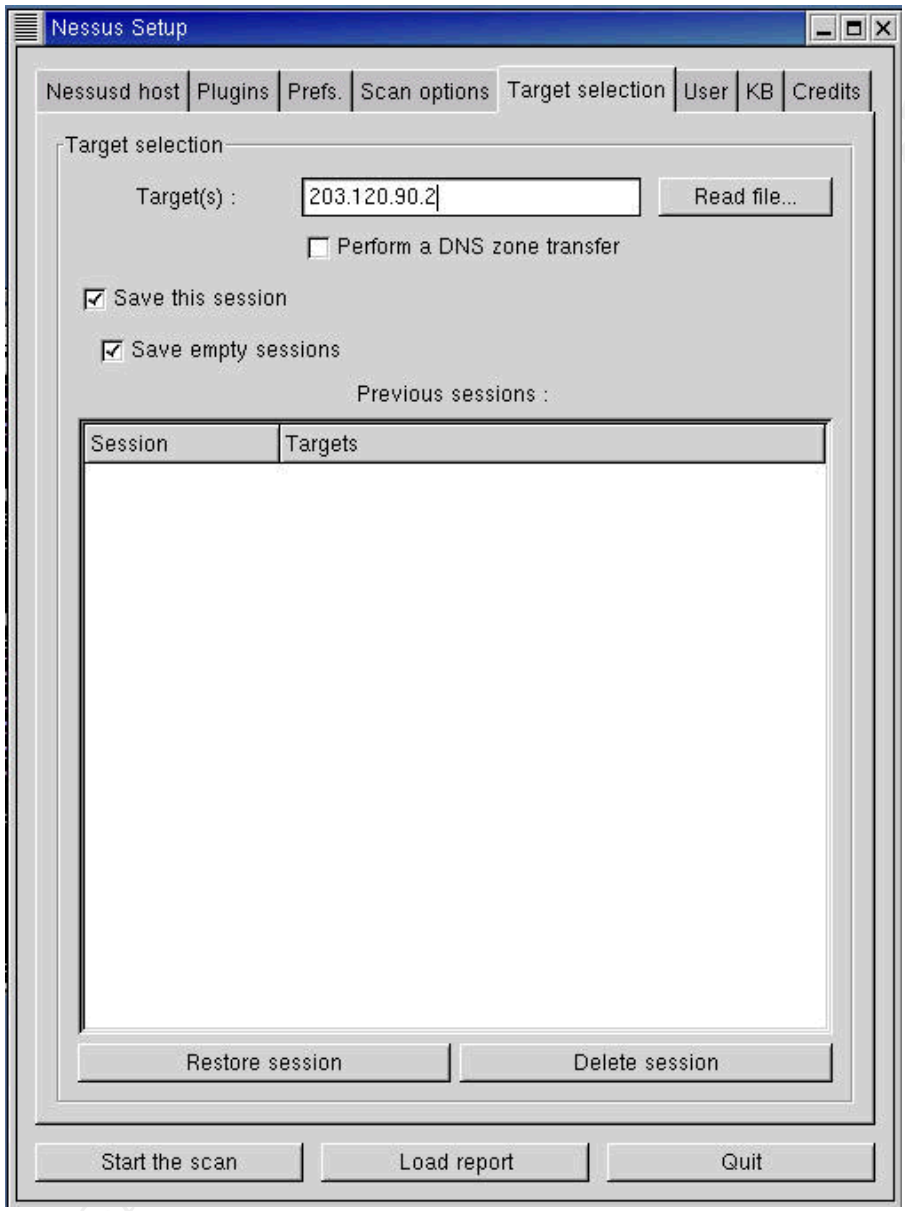
Naturally, not all scripts within these categories are targeted for the right system. Auditors can choose according to the description of the script if it's suitable. Those not mentioned are left as default or blank.

Auditors may choose to use Nessus to carry out the scans as well.



Target Selection page

The target can be IP, FQDN hostname, or a network. Input method includes text file with each target separated by a comma or line. Nessus client also allows user to load previous report files for reviewing.



The output of nessus scans can either be in HTML, Text or their nessus proprietary reporting nbe format. Results usually show the particular vulnerability associated with which host, on which port and a brief explanation together with a recommendation. There are also links to other websites for clearer explanation on the vulnerability.

3.2.3 Check Point Firewall Configuration / information collection

Auditors should collect information on the following from the $FWDIR/conf or $FWDIR/database directory:

- Policy and Address translation rulebase.
  - Configuration files with extension.W or rulebase.fws
- General firewall configuration preferences.
  - Collected from GUI.
- VPN configuration.
  - Collected from GUI.
- Users and network objects.
  - Configuration files : fwauth.NDB and objects.C
- Customized Services.
  - In configuration rile objects.C
- Log configuration and logs files.
  - Found in $FWDIR/log. E.g.. Fwd.elg, fw.log

3.2.4 OS Security Audit

The underlying OS is a Solaris 8. A script combining all these command can be run to check the a few important system parameter information used for evaluation and recommendations later.

- List of users : in /etc/shadow and /etc/password
- List of services : /etc/services
- disk space : **df –k** was issued to check the disk space available. This was to ensure that the disks are not too full.
- Routing : **netstat –an** checks all the routing information as well as the routes available on the unix machine. This is vital to check where the traffic is routing.
- Network interface : **ifconfig –au**
- Startup scripts in **/etc/rcS.d, /etc/init.d, /etc/rc0.d, /etc/rc1.d, /etc/rc2.d, /etc/rc3.d**
- Check cron jobs in **/etc/cron.d**
- OS Patch levels
- Network Information

Configuration file	***Comments***
/etc/hosts	Checks the hosts file that resolves host names to IP addresses.
/etc/defaultrouter	Checks what is the default router is there is any.
/etc/notrouter	
/etc/resolv.conf	Checks where is the DNS set to.
/etc/nsswitch.conf	Checks the configuration how hostname are resolved.
/etc/gateways	Checks what is the
/etc/networks	Checks what networks are configured

/etc/inetd.conf	Check which services are started during system boots up

3.3 Evaluation

Based on the port scan, nessus scans, OS security information collected, recommendations can then be made.

3.3.1 Evaluating Port Scan Results

Results of the port scans would usually show the type of ports opened. The ports should match the sort of traffic required to pass through.

Naturally the actual port scan on the firewall would turn out different ports. But it should show minimal ports opened. A sample results of a Nmap TCP SYN Stealth port scan on an University website is attached in Appendix II. The IP was changed for anonymity purposes.

The scan reveals that the host is up. It also summarizes which ports are opened. The auditor should then check with IANA (Internal Assigned Numbers Authority) on what are the common possible services opened. 25 refers to SMTP, 80 refers to HTTP

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
 Host  (155.X.X.156) appears to be up ... good.
Initiating SYN Stealth Scan against  (155.X.X.156)
Adding TCP port 6103 (state open).
 Adding TCP port 2301 (state open).
 Adding TCP port 1027 (state open).
 Adding TCP port 3372 (state open).
 Adding TCP port 3837 (state open).
 Adding TCP port 25 (state open).
 Adding TCP port 2922 (state open).
 Adding TCP port 1063 (state open).
 Adding TCP port 80 (state open).
 The SYN Stealth Scan took 1109 seconds to scan 10000 ports.
```

Sometimes, the results shows that the ports are filtered indicates that there is a firewall present filtering the packets.

3.3.2 Evaluating Nessus Report Scan

Auditors should remember that speed of security scans depend much on

- CPU power of the scanning machine. If the machine is a highly powered CPU machine, it can carry out more tests concurrently. This option can be configured in the Scan options page.
- Bandwidth of the network connection to carry out the scan. Often if the scanning machine resides on a network many hops away, it slows down the scan significantly. It also causes time-out programs and may not give an accurate result.

Results usually carry a description of the vulnerability and a recommendation or link

to advise users how to improve the security.

3.3.3 Evaluating Firewall configuration

A few options in the preferences should be checked.

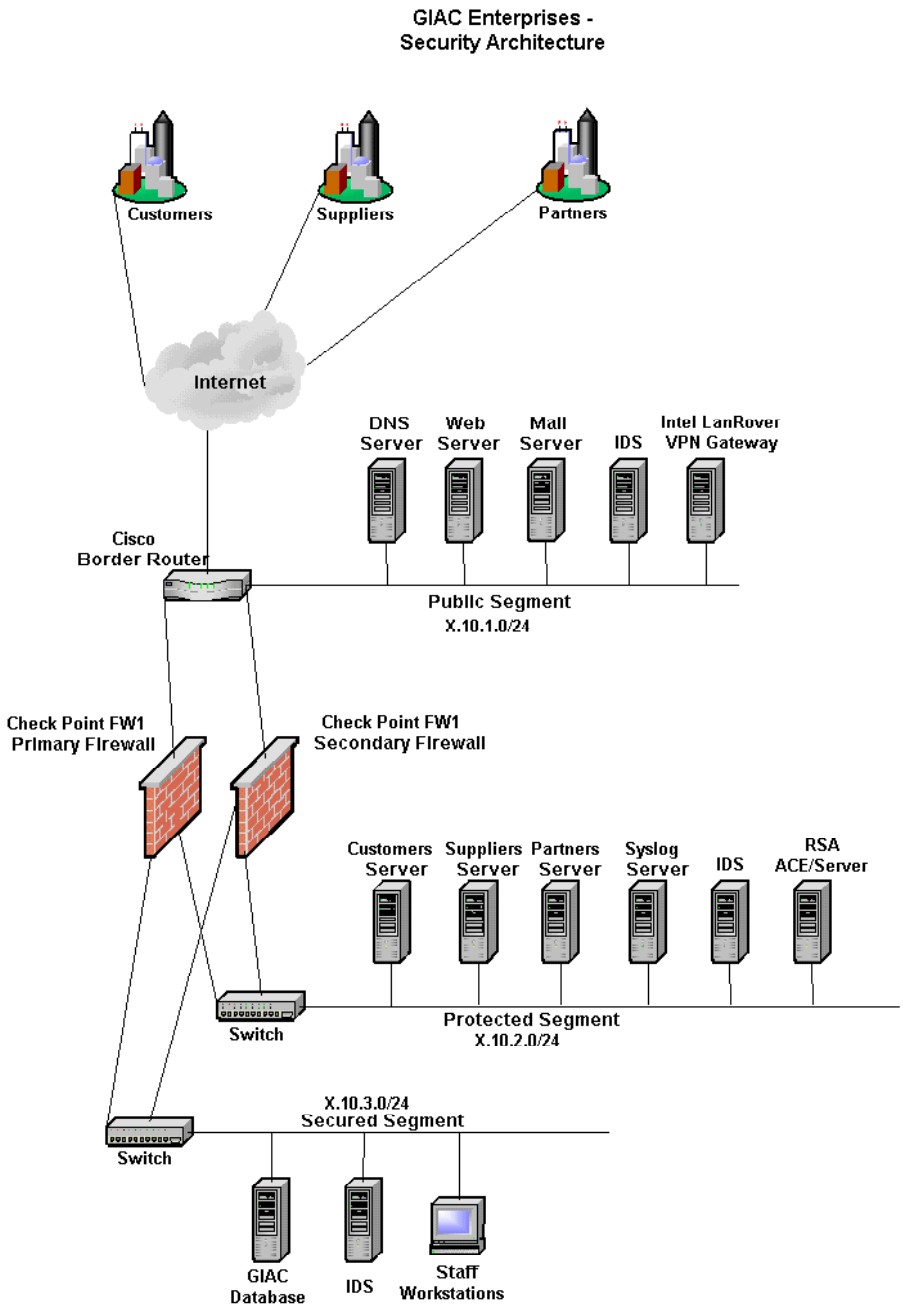
- Firewall administrator should check that all packets that do not match any filter rule should be dropped. As the rules are matched from top to bottom of the list, "Any – Any drop" should always be included at the end of the rulebase if it is not already created in the implicit rules.
- Check whether ICMP and other routing information like RIP should be allowed and received by the firewall. The firewall can be configured to be dropped or accept such information.
- List of all the users created on the firewall. This is important in matching the group of users to the correct access rule.
- Verify the IP address and information of the network objects match the servers.
- Verify the service ports created in customized service are valid to the connection required.
- Impose desktop policy for SecurClient. Ensure that firewall **do not** "Respond to unauthenticated topology request". This is to prevent a possible DOS attack on port 264 (for firewall-1 topology traffic) and prevent sensitive internal information from leaking.

3.3.4 Evaluating OS Security

- Review users list and remove unnecessary users
  Solaris generally comes with list of users e.g. lp that is normally not necessary in dedicated systems like a firewall. Remove and leave the bare minimal.
- Remove unnecessary services from starting in /etc/inetd.conf
  Prevent unnecessary services from starting. Those like telnet, ftp should be disabled.
- Check that there is sufficient disk space for logs storage.
  Insufficient disk space can potentially bring a firewall down.
- Check routing information, determine how the firewall is obtaining its route updates. Is it the use of dynamic routing protocol like RIP, OSPF or static routing. What are the networks connected to the firewall.
- Check that login information is logged.
- Apply the latest recommended patch cluster by Sunsolve.
- Use ready tightening scripts like TITAN or YASSP to tighten the OS for a more complete audit and tightening job.

4 Design under fire

The design chosen to come under fire belongs to MeauHuat Tan.
http://www.giac.org/practical/MeauHuat_Tan_GCFW.doc



4.1 Attack on Firewall

CheckPoint Firewall-1 from CheckPoint Software Technologies was chosen as the firewall. There are 3 known vulnerabilities listed here.

4.1.1 Format-Strings Vulnerability

Format Strings vulnerability exists on the Check Point firewall-1 management station that allows a valid and authenticated connection from a remote management client to send specially constructed format strings to printf* function and insert code to system's operating stack on management station. This could lead to read-only administrators from gaining elevated privileges on the machine, thus the compromise and gaining control of the whole system.

4.1.2 RDP Bypass Vulnerability

CERT® issued an advisory CA-2001-17 Check Point RDP Bypass Vulnerability on 9th July 2001 warning of a vulnerability in the software that could allow intruder to pass traffic through the firewall on UDP port 259.

Discovered by Inside Security GmBH, Firewall-1 management rules allow arbitrary RDP connections to traverse the Firewall by default. By simply faking the UDP packet with a RDP header, the firewall allows it to pass through port 259 bi-directionally without any controls imposed.

This vulnerability potentially exposes the system to the intruder exploiting other vulnerabilities existing on the firewall thus compromising the system and allowing the attacker to sniff the network traffic.

4.1.3 IP Fragmentation Denial-of-Service

CERT® issued a Vulnerability Note *VU#35958 IP Fragmentation Denial-of-Service Vulnerability* in FireWall-1 describing a vulnerability that allow remote attackers to cause a denial of service attacks by sending a large number of malformed fragmented IP packets.

This vulnerability was first discovered by Lance Spitzner and posted on the BugTraq mailing list. Versions affected include Checkpoint 4.0 and 4.1.

An attacker exploits the vulnerability by sending a stream of large IP fragments to the firewall. Extensive CPU power is used to log the IP fragmentation anomalies hence depriving further packets from being processed and passing through the firewall.

Firewall-1 only filters reassembled packets from fragments against the rule-base to prevent them from passing through the firewall and violating the rulebase. The firewall does not drop legally formed fragments until they are fully assembled.

Processing large number of fragments utilizes all the CPU time before the packet can be reassembled completely.

Hence an attacker could cause a denial-of-service on the firewall by simply sending large number of fragments to monopolize the CPU of the firewall. Other authorized and legal packets, whether incoming or outgoing, will be denied from processing and passing through the firewall.

4.2 Denial-Of-Service Attacks

4.2.1 Type of attack

The design was subjected to a TCP-SYN flood attack. TCP-SYN attacks occupy huge bandwidth consumption when coordinated efforts are launched from the 50 cable modems/DSL hence achieving its aim. It also hogs resources of the target as TCP connections require systems to track and maintain connection states, significantly reducing the ability to handle more incoming connections.

A TCP-SYN flood attack works by an attacker sending a SYN packet to the victim using a spoofed address. The victim then returns with a SYN/ACK packet and waits for the ACK reply packet to complete the TCP 3 way handshake. However, since the address was spoofed, there would not be any ACK reply packet from the expected address. This "half" connection is queued and timeouts. Hence when 50 cable modems churns out multiple spoofed SYN/ACK packets at high speed, the victim's resources are expended, denying other legitimate connections from establishing.

Such attacks could be launched on any systems such as the web server, DNS server, and firewall. There are never true ways to fully defend against DDoS as the packets are properly formed SYN packets with spoofed source addresses that can be sent from thousands of bots all over the world.

Tools used to launch such attacks could be easily downloaded from the Internet. Searching for such tools with search word "DDoS" on Google yield countless easy links. Tribal Flood Network (TFN) is one of such tools that could be used to launch TCP-SYN flood.

4.2.2 Counter measures

To defend the network against DDOS and minimize the degree of damage of a DDoS attack requires different strategies. It requires cooperation from both ISPs and our own networks to form effective defense against such attacks.

On our own effort, the border router should perform address filtering to prevent unnecessary traffic from passing into or out of the network. As a good security principle, all unnecessary services should be removed.

1. Packets sent to broadcast and Private IP addresses should be filtered off. Private IP addresses are non-routable on the Internet and does not belong to anybody. They are often used within a company network and not valid internet addresses. RFC 1918 details the following address range.

Class	Network Address	Address Range
A	10.0.0.0 /8	10.0.0.0 – 10.255.255.255
B	172.16.0.0/12	172.16.0.0 – 172.31.255.255
C	192.168.0.0/16	192.168.0.0 – 192.168.255.255

Attackers often spoof source using private IP addresses. Since such addresses are non-routable onto the Internet, firewalls and routers should be configured drop such packets be it incoming from or outgoing to the Internet.

Others include reserved IP addresses never assigned to public networks. Packets with such source address should be dropped as well.

Reserved for	Address range
Historical broadcast address	0.0.0.0/32
Loopback	127.0.0.0/8
Link-local Networks	169.254.0.0/16
TEST-NET	192.0.2.0/24
Class D Multicast address range	224.0.0.0/4
Class E Experimental address range	240.0.0.0/5
Unallocated	248.0.0.0/5
Broadcast	255.255.255.255/32

2. Egress filtering at the border router or firewall ensures that outgoing packets source network ID indeed belongs to the network. This helps to prevent systems within the internal network from being used as a springboard to launch DDoS attacks on other external systems. This is further explained in RFC2267.

3. External networks shouldn't be allowed to send broadcast message to all host on the internal network. Access list filtering should limit packets to broadcast address. Similarly, disable IP directed broadcast on all interface of the routers to prevent internal hosts from being used to launch Smurf-style attacks.

4. Configure and update the Network IDS with the latest patches and signature files to detect unusual data patterns and raise alerts early.

Internet Service Providers (ISPs) also play an important role in defense against DDoS attacks. Only they can prevent the "bad" packets from infiltrating the network.

1. ISP should drop packets with source IP addresses from private or reserved addresses as mentioned above. This would significantly drop reduce the number

of "bad" packets being routed into or out of the network.

2. Similarly, perform ingress filtering on their perimeter routers or firewalls to prevent downstream networks from inserting spoofed packets into the Internet. Ensure that packets routed from customer's networks carry source address that match their network addresses. This would make DDoS attacks harder to succeed and easier to trace to the attacker.

3. Encourage customers to perform egress filtering on their routers. Defense against DDoS requires the cooperation of everybody.

References

[1] Check Point support documents
http://www.checkpoint.com/

[2] PhoneBoy website on Check Point firewall FAQ
http://www.phoneboy.com

[3] Cisco IOS Release 12.0 Security Configuration Guide
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/index.htm

[4] Creating a VPN between Cisco Router and Checkpoint Firewall using manual IPSec
http://www.imtek.com/IPSec.html

[5] NSA Router Security Configuration Guides
http://nsa2.www.conxion.com/cisco/

[6] Improving Security on Cisco Routers
http://www.cisco.com/warp/public/707/21.html

[7] From the Cisco Documentation CD
Cisco IOS 12.0:
Security Configuration Guide
Security Command Reference
Configuration Fundamentals Configuration Guide
Configuration Fundamentals Command Reference
Cisco IOS Interface Configuration Guide
Cisco IOS Interface Command Reference
Network Protocols Configuration Guide, Part 1
Network Protocols Command Reference, Part 1
Enhanced IP Services for Cisco Network

[8] Nmap Port Scanner
http://www.insecure.org/nmap

[9] Nessus - Security Scanner
http://www.nessus.org

[10] IANA – Internet Assigned Numbers Authority
http://www.iana.org/numbers.html

[11] TITAN
http://www.fish.com/titan

[12] YASSP
http://www.yassp.org/

[13] IP Fragmentation Denial-of-Service Vulnerability
http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html
CERT Vulnerability Note VU#35958 IP Fragmentation Denial-of-Service Vulnerability in FireWall-1. http://www.kb.cert.org/vuls/id/35958

[14] Check Point Firewall-1 RDP Bypass Vulnerability
http://www.checkpoint.com/techsupport/alerts/rdp.html
CERT Advisory CA-2001-17, http://www.cert.org/advisories/CA-2001-17.html

[15] Check Point Firewall-1 Format Strings Vulnerability
http://www.checkpoint.com/techsupport/alerts/format_strings.html
http://www.iss.net/security_center/static/6849.php

[16] Defenses Against Distributed Denial of Service Attacks. Gary C. Kessler
Nov 29, 2000
http://rr.sans.org/threats/DDoS.php

[17] DDoS is neither dead nor forgotten. By Rik Farrow. Feb 5, 2001
http://www.networkmagazine.com/article/NMG20010125S0003

[18] DDoS: Internet Weapons of Mass Destruction. By Brooke Paul. Jan 8,2001
http://www.networkcomputing.com/1201/1201f1c2.html

[19] Distributed Denial-of-Service (DDoS) attack tools
http://staff.washington.edu/dittrich/misc/ddos/

Appendix I - Sample of nmap output

```
TCP SYN Stealth scan was performed on the target from ports 1 -
10000. Its IP was changed for anonymity purposes.

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
 Host  (155.X.X.156) appears to be up ... good.
Initiating SYN Stealth Scan against  (155.X.X.156)
Adding TCP port 6103 (state open).
 Adding TCP port 2301 (state open).
 Adding TCP port 1027 (state open).
 Adding TCP port 3372 (state open).
 Adding TCP port 3837 (state open).
 Adding TCP port 25 (state open).
 Adding TCP port 2922 (state open).
 Adding TCP port 1063 (state open).
 Adding TCP port 80 (state open).
 The SYN Stealth Scan took 1109 seconds to scan 10000 ports.

For OSScan assuming that port 25 is open and port 179 is closed
and neither are firewalled
Interesting ports on  (155.X.X.156):
(The 8963 ports scanned but not shown below are in state: closed)
Port       State       Service
1/tcp      filtered    tcpmux
2/tcp      filtered    compressnet
3/tcp      filtered    compressnet
4/tcp      filtered    unknown
5/tcp      filtered    rje
6/tcp      filtered    unknown
7/tcp      filtered    echo
8/tcp      filtered    unknown
9/tcp      filtered    discard
10/tcp     filtered    unknown
11/tcp     filtered    systat
12/tcp     filtered    unknown
13/tcp     filtered    daytime
14/tcp     filtered    unknown
15/tcp     filtered    netstat
16/tcp     filtered    unknown
17/tcp     filtered    qotd
18/tcp     filtered    msp
19/tcp     filtered    chargen
20/tcp     filtered    ftp-data
21/tcp     filtered    ftp
22/tcp     filtered    ssh
23/tcp     filtered    telnet
24/tcp     filtered    priv-mail
25/tcp     open        smtp
26/tcp     filtered    unknown
27/tcp     filtered    nsw-fe
28/tcp     filtered    unknown
29/tcp     filtered    msg-icp
30/tcp     filtered    unknown
31/tcp     filtered    msg-auth
32/tcp     filtered    unknown
33/tcp     filtered    dsp
34/tcp     filtered    unknown
35/tcp     filtered    priv-print
36/tcp     filtered    unknown
```

```
37/tcp     filtered    time
38/tcp     filtered    rap
39/tcp     filtered    rlp
40/tcp     filtered    unknown
41/tcp     filtered    graphics
42/tcp     filtered    nameserver
43/tcp     filtered    whois
44/tcp     filtered    mpm-flags
45/tcp     filtered    mpm
46/tcp     filtered    mpm-snd
47/tcp     filtered    ni-ftp
48/tcp     filtered    auditd
49/tcp     filtered    tacacs
50/tcp     filtered    re-mail-ck
51/tcp     filtered    la-maint
52/tcp     filtered    xns-time
53/tcp     filtered    domain
54/tcp     filtered    xns-ch
55/tcp     filtered    isi-gl
56/tcp     filtered    xns-auth
57/tcp     filtered    priv-term
58/tcp     filtered    xns-mail
59/tcp     filtered    priv-file
60/tcp     filtered    unknown
61/tcp     filtered    ni-mail
62/tcp     filtered    acas
63/tcp     filtered    via-ftp
64/tcp     filtered    covia
65/tcp     filtered    tacacs-ds
66/tcp     filtered    sql*net
67/tcp     filtered    bootps
68/tcp     filtered    bootpc
69/tcp     filtered    tftp
70/tcp     filtered    gopher
71/tcp     filtered    netrjs-1
72/tcp     filtered    netrjs-2
73/tcp     filtered    netrjs-3
74/tcp     filtered    netrjs-4
75/tcp     filtered    priv-dial
76/tcp     filtered    deos
77/tcp     filtered    priv-rje
78/tcp     filtered    vettcp
79/tcp     filtered    finger
80/tcp     open   http

< SNIP >

8080/tcp   filtered    http-proxy
8888/tcp   filtered    sun-answerbook

Remote operating system guess: FreeBSD 2.2.1 - 4.1
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=16168 (Worthy challenge)
IPID Sequence Generation: Busy server or unknown class)

Nmap run completed -- 1 IP address (1 host up) scanned in 1143
seconds
```

Appendix II- Sample of Nessus Scan output

```
Nessus Scan Report
```

```
------------------

SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 1
 - Number of security warnings found : 2
 - Number of security notes found : 7

TESTED HOSTS

 www.xxx.edu (Security holes found)

DETAILS

+ www.xxx.edu :
 . List of open ports :
   o http (80/tcp) (Security hole found)
   o smtp (25/tcp) (Security notes found)
   o unknown (2301/tcp) (Security warnings found)
   o general/tcp (Security notes found)
   o general/udp (Security notes found)

 . Vulnerability found on port http (80/tcp) :

    The dll '/_vti_bin/_vti_aut/dvwssr.dll' seems to be present.

    This dll contains a bug which allows anyone with
    authoring web permissions on this system to alter
    the files of other users.

    In addition to this, this file is subject to a buffer overflow
    which allows anyone to execute arbitrary commands on the
    server and/or disable it

    Solution : delete /_vti_bin/_vti_aut/dvwssr.dll
    Risk factor : High
    See also : http://www.wiretrip.net/rfp/p/doc.asp?id=45&iface=1
    CVE : CVE-2000-0260

 . Warning found on port http (80/tcp)

    IIS 5 has support for the Internet Printing Protocol(IPP),
which is
    enabled in a default install. The protocol is implemented in
IIS5 as an
    ISAPI extension. At least one security problem (a buffer
overflow)
    has been found with that extension in the past, so we
recommend
    you disable it if you do not use this functionality.

    Solution:
    To unmap the .printer extension:
     1.Open Internet Services Manager.
     2.Right-click the Web server choose Properties from the
context menu.
     3.Master Properties
     4.Select WWW Service -> Edit -> HomeDirectory ->
Configuration
```

```
    and remove the reference to .printer from the list.

    Risk factor : Low
    CVE : CAN-2001-0241

 . Information found on port http (80/tcp)

    The remote web server type is :

    Microsoft-IIS/5.0

    We recommend that you configure your web server to return
    bogus versions in order to not leak information

 . Information found on port smtp (25/tcp)

    Remote SMTP server banner :
    0
    0


 . Warning found on port unknown (2301/tcp)

    Remote Compaq HTTP server version is:
     2.1

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