Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment

Version 1.9 (revised January 20, 2003)

Li Bee Seah

June 30, 2003

Table Of Content

Abstract

This is a practical paper submission for GCFW certification. The version for this GCFW practical assignment is 1.9. The content of this document has been written based on an imaginary company called GIAC Enterprises that plans to setup a secure e-business architecture to sell its fortune cookie saying via the Internet.

There are 4 related parts within this assignment.

1. Security Architecture
   To design a security architecture that suits GIAC Enterprises's business needs. The security design should include studies on access requirements, network diagrams, IP addressing scheme and explanations on the purpose, security function and placement of all perimeters defense components.

2. Security Policy and Tutorial
   Security policy for the network components (border router, firewall and VPN) are detailed with an inclusion of a separate tutorial for one of the network components mentioned above.

3. Verify the Firewall Policy
   Provide plans and approaches to audit the security policy in the firewall. Analysis of the audit is presented with recommendations for further improvements.

4. Design Under Fire
   To choose a network design from any GCFW practical posted in the previous 6 months and perform 3 type of attacks against it.

Assignment 1 – Security Architecture

Company Background

GIAC Enterprises is a medium size company that has been selling fortune cookie sayings for many years. The positive growth in GIAC business has enabled the President to have adequate funds to take an advantage of the information age to operate his business through the Internet.

The new alignment in his business strategies was also made to provide conveniences to his partners and suppliers who had recently operated their businesses securely via the Internet.

We were advised by the President to build the e-business network with the basic security components. If the business grows positively, then the network shall be scaled with additional security components.

Business Operation Overview

A thorough study on the day-to-day business operation had enabled the team to translate the traditional business structure into an e-business architecture. We had identified 5 different groups of users who will be involved in this new online retail business.

Customers

Operating business via the Internet can help GIAC to enlarge its business not only locally but to the other parts of the world. Therefore, it is very important to built an e-business design that can attract and encourage more individuals and organizations to purchase fortune cookie sayings from GIAC.

The GIAC website is the first point of business contact with the customers or potential customers. It is a MUST to ensure that the website is user friendly, attractive and secure. Customers can establish their connections to GIAC in anyway (from a remote LAN or dial-up from home).

Below are the steps for a customer to establish an e-business contact with GIAC.

1. Firstly, the customer will browse the GIAC's website for company information and online catalog via the insecure http (tcp 80) protocol.

2. If the customer wishes to place an order, the backend e-business application shall then switch the web connectivity from the insecure http mode to a secure https (tcp 443).

I. Customer will first verify the authenticity or genuineness of GIAC Enterprises' website by viewing GIAC's server certificate issued by a trusted Certificate Authority eg. Verisign
II. Thereafter, the customer can then feel free to provide their name, postal address, email address, credit card number and the selected catalog number in order to place an order.
III. When payment is confirmed, a customer id and a password for the customer will be generated and sent to the customer's email address (smtp tcp 25)
IV. With the customer id and password, the customer can then
    - check the status of the order
    - download the purchased fortune cookie sayings
    - make changes to their details when the need arise
    - place future orders
    - provide valuable feedback about GIAC website

The exchange of information for step I, II and IV (except step III) are in https mode and encrypted with 128-bit (highest) or 40-bit (lowest) depending on customer's browser capabilities. Browsers normally communicate using the least denominator.
(SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.4, page 53)
There should be no restriction imposed on the access method. Customer should feel free to choose their desktop platform. If customers face difficulties, it will refrain them from revisiting GIAC's website. This will definitely cause a negative impact to GIAC's business growth.

Suppliers

GIAC has been working with a few loyal suppliers for many years. All these suppliers are well known local writers. As a token of appreciation for the long –term business partnership, GIAC's President had decided to provide them an Internet access account. This is a good plan as it aims to provide access convenience for the suppliers and the network administrator can restrict access to the GIAC's SSH server, private web server and mail relay server based on the pool of dialup IP that GIAC has reserved with the ISP.

Suppliers can establish connection to GIAC via client to gateway VPN mode. Secure VPN tunnel is highly recommended as data transmitted between GIAC and suppliers are strictly confidential and business oriented. We do not wish to leak business information to the hands of our competitors.
In addition to that, it is vital to make sure that every supplier's desktop is equipped with a personal firewall. The is because when a supplier's desktop is connected to GIAC's network, they are actually forming an extension of GIAC's network. If ever an attacker managed to take control of the supplier's system, the attacker can then make use of the VPN tunnel and attempt their

attacks on GIAC's corporate network. Therefore, we must make sure that the supplier's desktop is protected with a personal firewall.
Every supplier will be authenticated by GIAC's VPN gateway before a VPN tunnel can be established. They are required to login their username and password. If the supplier is successfully authenticated, the supplier will then be permitted to do the following tasks :-

- Upload their newly created fortune cookies into GIAC's SSH server (ssh tcp 22)
- Upload their invoices into GIAC's SSH server (ssh tcp 22)
- Suppliers can view new orders and invoices history or status via GIAC's private web server (http tcp 80 and https tcp 443)
- Access their webmail account via mail relay server which will proxy http tcp 80 request to the internal mail server (http tcp 80)
- Domain name resolution (domain-udp 53)

Partners

GIAC has many local and overseas partners. For the past few years, it has been quite inconvenient to deal business with the foreign partners as we had huge time differences and the high costs involve in exchanging business information and data. The President is well aware of these hindrances and therefore has decided to do business online. GIAC's partners are customers who will purchase new fortune cookies, translate these fortune cookies into several foreign languages and re-supply to GIAC with a minimal amount of charges.

All GIAC's partners are well-established corporate companies that had their business operated via the Internet. Having gateway-to-gateway VPN connection is nothing new to the partners but instead they have been practicing it as a way to deal business with foreign companies.

Partners can establish connection to GIAC via gateway-to-gateway VPN mode. Below are some tasks that a partner is permitted to do :-

- Download the new batch of fortune cookies from GIAC's SSH server (ssh tcp 22)
- Translate the new batch of fortune cookies into different languages and upload the translated fortune cookies back to the GIAC's SSH server (ssh tcp 22)
- Upload their invoices into GIAC's SSH server (ssh tcp 22)
- Partners can send orders and view invoices history or status via GIAC's private web server (http tcp 80 and https tcp 443)
- Send email to GIAC staff (smtp tcp 25) but using their own SMTP server

GIAC Internal Employees

There are system administrators, network administrators, sales administrators and clerical staffs working in GIAC's local office. Each group will perform certain job scopes in the company. The employees' job scopes will determine their access rights and services for the different sub-networks

Clerical Staffs

- access internal email server (smtp tcp 25 and pop3 tcp 110)
- browsing (http tcp 80 or https tcp 443)
- domain name resolution (domain-udp 53)

Systems Administrators

- access internal email server (smtp tcp 25 and pop3 tcp 110)
- browsing (http tcp 80 or https tcp 443)
- domain name resolution (domain-udp 53)
- Maintain servers at Service Network and Internal Network (ssh tcp 22)
- To perform ping to any hosts for administration purposes (icmp)

Network Administrators

- access internal email server (smtp tcp 25 and pop3 tcp 110)
- browsing (http tcp 80 or https tcp 443)
- domain name resolution (domain-udp 53)
- Telnet into the border router for maintenance (telnet 23)
- Maintain the firewall server via remote GUI client (CPMI tcp 18190)
- Maintain the hardware-based network IDS at the Internal and Service network (https tcp 443)
- To perform ping to any hosts for administration purposes (icmp)

Sales Administrators

- access internal email server (smtp tcp 25 and pop3 tcp 110)
- browsing (http 80 or https 443)
- domain name resolution (domain-udp 53)
- Upload invoices and marketing data into partners' SSH server via VPN tunnel (ssh tcp 22)

GIAC Mobile sales force and teleworkers

All mobile sales force and teleworkers will be using the Internet access account granted by the company. This makes work easier for the network administrators as they can restrict access to the GIAC's SSH server, private web server and mail relay server based on the pool of dialup IP that GIAC has reserved with the ISP.

Mobile employees can establish connection to GIAC via client to gateway VPN mode. Secure VPN tunnel is highly recommended as data transmitted between GIAC and these employees are strictly confidential and business oriented. We do not wish to leak business information to the hands of our competitors.
In addition to that, it is vital to make sure that every mobile employee's desktop is equipped with a personal firewall. The is because when a mobile employee's desktop is connected to GIAC's network, they are actually forming an extension of GIAC's network. If ever an attacker managed to take control of the mobile employee's system, the attacker can then make use of the VPN tunnel and attempt their attacks on GIAC's corporate network. Therefore, we must make sure that the mobile employee's desktop is protected with a personal firewall.
Every mobile employee will be authenticated by the GIAC's VPN gateway before a VPN tunnel can be established. They are required to login their username and password. If the mobile employee is successfully authenticated, they will then be permitted to do the following tasks :-

- access GIAC's private web server to view sales performance and marketing data (http tcp 80 and https tcp 443)
- upload sales, marketing and new customer's data into GIAC's SSH server (ssh tcp 22)
- Access their webmail account via mail relay server which will proxy http tcp 80 request to the internal mail server (http tcp 80)
- domain name resolution (domain-udp 53)

Below is the summary of users' access requirements.

Group	Access Requirements	Service	Ports
Customers	- access GIAC Public web server - send email to GIAC - domain name resolution	http https smtp domain-udp	tcp 80 tcp 443 tcp 25 udp 53
Suppliers	- access GIAC Private web server - upload data to GIAC SSH server - webmail access via mail relay which proxy http port 80 to internal mail server - domain name resolution	http https ssh http domain-udp	tcp 80 tcp 443 tcp 22 tcp 80 udp 53
Mobile Sales & Teleworkers	- access GIAC Private web server - upload data to GIAC SSH server - webmail access via mail relay which proxy http port 80 to internal mail server - domain name resolution	http https ssh http domain-udp	tcp 80 tcp 443 tcp 22 tcp 80 udp 53
Partners	- access GIAC Private web server - download and upload data to GIAC SSH server - send email to GIAC - domain name resolution	http https ssh smtp domain-udp	tcp 80 tcp 443 tcp 22 tcp 25 udp 53
<u>GIAC Internal Employees</u> All Internal Employees	- send and retrieve email on internal mail server - domain name resolution - browse internet - to grab dynamic IP and to store files on the Internal DHCP & File server	smtp pop3 domain-udp http https dhcp ftp	tcp 25 tcp 110 udp 53 tcp 80 tcp 443 tcp 135 udp 67, 68 tcp 20 tcp 21

System Administrators	- Access all servers on service network and internal network for system administration - to perform ping to any hosts for administration purposes	ssh ICMP	tcp 22
Network Administrators	- to manage to the border router - to manage the firewall - to manage the network IDS on internal network - to manage the network IDS on service network - to perform ping to any hosts for administration purposes	telnet CPMI https https ICMP	tcp 23 tcp 18190 tcp 443 tcp 443
Sales Administrators	- to upload invoices and marketing data into partner's SSH server	ssh	tcp 22

Below are servers and router access requirements.

Servers	Access Requirements	Service	Ports
External DNS	- to enable external DNS server to do external domain name queries	domain-udp domain-tcp	udp 53 tcp 53
Internal Mail Server	- to enable internal mail server to send email out via Mail Relay	smtp	tcp 25
Mail Relay	- to enable mail relay to forward incoming email to internal mail server	smtp	tcp 25
Internal DNS	- to enable internal DNS to do queries with the external DNS	domain-udp domain-tcp	udp 53 tcp 53
Backup Database	- to perform periodic backup from Database server at Service Network	sql	tcp 1521

Border Router	- to allow the border router to send it's log file to the Syslog server that resides at the Internal Network	syslog	udp 514
All Servers on Internal Network	- to synchronous network time from NTP server at Service Network - to perform ping to any hosts for administration purposes	ntp ICMP	udp 123
All Servers on Service Network	- to synchronous network time from NTP server at Service Network - to perform ping to any hosts for administration purposes	ntp ICMP	udp 123

Description For Figure 1

Figure 1 depicts the network security design for GIAC Enterprises. Network security MUST not be overlooked or neglected in the design as GIAC's network has an external link to the Internet. Having business operated through the Internet can potentially help GIAC to generate more business opportunities but at the same time it will also attract uninvited hackers and crackers from the Internet.

A thorough and carefully planned security design can effectively help to deter hackers and crackers who are intrigued by challenge from gaining ownership to some confidential data and from compromising GIAC's valuable resources.

Although business needs is the major concern in every security design, other factors such as cost, the level of risks and the balance of access and convenience must be equally evaluated.

The complexity of our network design becomes greater as GIAC has the need to exchange business data over some non-trusted paths such as the partners' network and remote VPN connection with suppliers and mobile employees.

To address these issues, we have incorporated 4 different types of perimeter defense components into our design. These components are the filtering router (border router), firewall, VPN and Intrusion Detection System. Description below explains the specific brand and version of each component, its purposes, security functions or roles it carries and how the placement of each component on the network can fulfill its role.

Border Router

Brand : Cisco Router Model 2610
Version : Cisco IOS version 12.2

Purpose :

- To connect GIAC network to the Internet and vice versa
- To route inbound packets from the Internet into GIAC's network (before the firewall)
- To route outbound packets from GIAC's network to the Internet (after the firewall)
- It contains a set of routing table for all accessible network paths. Packets will be routed based on the best route or path defined. Additional routes can be manually configured.

Security Function or role :

- To filter all outgoing and incoming packets with its static packet filtering function.
- The border router will examine every packet that reaches to the ingress or egress port. The packet may be permitted or denied. It is all based on the access control list (ACL) defined at the ingress or egress port.
  Both the ingress and egress port can have the same or different set of access control list. The ACL is a set of permit and deny rules with matching criteria of source IP, destination IP, protocol, udp or tcp port number and icmp.

Placement :

- The border router is the first point of connection with the Internet. Therefore, it should be placed in between the Internet and the external interface of the firewall.
- With such placement, packet interception at router can help to filter off some of the unnecessary packets before it reaches to the firewall. Thus this helps to reserve and offload some of the firewall resources.

Firewall & VPN
(integrated in one server)

Brand : CheckPoint VPN-1/Firewall-1 NG
Version : NG Feature Pack 1 (installed on a hardened Windows 2000 server SP3)

Integrated Firewall and VPN

Purpose :

- This integrated firewall & VPN solution is the second level of defense after the router. It enforces security rules that static packet filtering in a router could not perform.
- Need not maintain firewall and VPN functions as 2 different perimeter defense components. This greatly simplifies the implementation.
- To protects all private resources on GIAC's network from malicious attack, for example the database server.
- To forward the allowed packets between the 3 segments. (internal, service and external). Combining the firewall and VPN as an integrated solution greatly simplifies the routing. Need not maintain different set of routing tables.
- To enable GIAC to enjoy the lower cost of secure connection (VPN) with partners, suppliers and mobile employees via the Internet infrastructure.

Security Function or role :

- All traffic routed between the external, service and internal network will be examined against a set of security policy configured as rule base.
- To drop and log any unauthorized access or entry.
- Perform static NAT (Network Address Translation) for servers on Service Network.
- Perform hide NAT (Network Address Translation) for the internal network.
- Impose strict control on the level of access by partners, suppliers, customers and employees on the applications in each servers and other valuable resources.
- Provide strong authentication schemes on partners', suppliers' and mobile employees' login before access can be granted.
- Provide data integrity check with SHA-1 and MD5 (data authentication).
- Provide data privacy by having strong data encryption and decryption (DES, 3DES, IPSec/IKE standards) for all GIAC's data transmitted via the VPN tunnel.
- It can perform split tunneling. All network traffic with partners, suppliers and mobile employees will be encrypted while normal Internet traffic are not encrypted. With this method, it delivers better performance than to encrypt all traffic.
- It is able to do policy distribution to all remote dialup VPN users with the pre-configured desktop security rules. Network administrator can carry out configuration updates for all remote VPN clients' firewall (applicable to suppliers' and mobile employees' desktops only)

Placement :

- The best location to place the firewall and VPN server is after the border router but before the Service and Internal network. With such placement, the firewall and VPN server can intercept every single packet that flows between the 3 segments – thorough inspection

Service Network IDS
Internal Network IDS
Brand : Intrusion SecureNet 2245
Version : SecureNet IDS ver 4.4

Purpose :

- The network-based intrusion detection systems (NIDS) can help to increase the security level of each sub network as the functionality of an NIDS compliments the role of a firewall. Firewall only helps to block unauthorized entry while NIDS have the capability to detect and send alert for any attacks on the network.
  (SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.3, page 140)
- The NIDS will constantly monitor network traffic that goes into GIAC's Service network and Internal network. Each network traffic has a pattern that an NIDS able to distinguish if it is an attack or a normal traffic.

Security Function or role :

- To detect and trigger immediate response for any intrusion that occurred. This is done on a real time basis.
- Each suspected intrusion will be checked and compared against the NIDS internal database that contains up-to-date attack patterns or signatures.
- When an attack had occurred, the NIDS can initiate various responses such as sending an alert via email, the administrator's pager or SNMP trap.

Placement :

- Should be placed at the service network and internal network as an added protection from intrusion. It monitors network traffic for potential misuse by customers, partners, suppliers or even GIAC's employees themselves

We have segmented GIAC Enterprises's network into 3 segments. The 3 segments are the External, Service and Internal network. The border router and the integrated firewall and VPN server are the only devices that are placed on the external network.

All publicly accessible servers are placed on the service network
Service Network :

- External DNS
  We are implementing the split DNS concept. The External DNS will only accept and replies DNS queries from the Internet and all nodes in the Service Network. The External DNS will only holds external records that contain Public IP addresses and there should be no Internal IP addresses configured in it. Zone transfer is disabled in this server and at the firewall.
- Mail Relay

The actual email system is located in the Internal Network. The role of the mail relay is to accept all inbound and outbound mail for the internal mail server. This help to safeguard the internal mail server from establishing direct contact with systems from the Internet. The Mail Relay server is also a proxy server, which is able to proxy http tcp port 80 requests to internal mail server for webmail access by suppliers and mobile employees.

- Public Web Server
  The Public Web Server is GIAC's main web server that accepts http 80 (clear text) or secure https 443 (ssl) request from the Internet. This web server will extract some business data from the database server when processing a customer's request.
- Private Web Server
  The Private Web Server is GIAC's private web server built only to provide information for suppliers, partners and mobile employees. The information publish on this web server is highly confidential and each group is required to provide their valid username and password before they could view the information that are reserved for them. This web server will extract some business data from the database server when processing the partners', suppliers' or mobile employees' requests.
- SSH Server
  The GIAC's SSH server is a very crucial and important server. It is a file system for suppliers, partners and mobile employees. These groups of people will upload or download data to their own home folder. Each user will be authenticated by the SSH server before they are granted access rights to their own home folder. Newly written and translated fortune cookies are stored on this server and shall be loaded into the Database Server on a weekly basis. Other business data such as invoices, new customer records and sales records will be transferred to the Database Server on a daily basis. The System Administrators will perform all these tasks.
- Network Time Protocol (NTP) Server
  The NTP server provides time synchronization for all servers in the Service and Internal Network. This is to ensure the timestamps on all log files are consistent.
  The time clock for the border router, Internal network IDS and Service network IDS will be manually configured by the network administrators. They will try to configure the time clock on these components to be as accurate and consistent with the rest of the servers on the Service and Internal network. The network administrators will constantly monitor the time clock from these components. If they were to discover that the time is not synchronous, then they will reconfigure these components to fetch time from the NTP server at the Service network.
- Database Server
  The Database Server on the Service Network serves to store and provide business data for the public and private web server. This Database Server is placed on the same network as the web servers to achieve

faster data transmission between these servers. Due to security reason, the Database server is configured with only private IP. There is no public IP assign for this Database server. The content of the Database Server is periodically backup to the Backup Database Server at the Internal Network. The backup is done on a daily basis.

At the internal network, we have the syslog server, backup database server, internal mail server, internal DNS server, internal DHCP & File server and internal users' desktops.

Internal Network :

- Internal DNS
  We are implementing the split DNS concept. The Internal DNS will only accept and replies DNS queries from nodes in the Internal Network. The Internal DNS only holds internal records that contain internal IP addresses.
- Syslog server
  It acts as a central storage for log files generated by the servers and perimeter defense components. Exception is made for firewall & VPN server, Internal Network IDS and Service Network IDS as the network administrators choose to manually transfer the log files from these devices to the syslog server.
  The syslog server is only use to store log files. No other public services should be running on it. It only accepts syslog connection on udp port 514. With a syslog server, these log files are much more protected and in the event of an attack, we can do cross-references by reviewing all logs accumulated on this server. Syslog server is one of the most critical servers in our design and we must maintain it as secure as possible. Due to budget restriction, we cannot afford to have an internal firewall to create an isolated network solely for syslog server. Therefore we have decided to place the syslog server on the internal network, armored it with a personal firewall and had its operating system hardened.
- Backup Database Server
  Backup is essential for every business. It is very crucial for GIAC to spend additional money for replicating data from the production Database server to the Backup Database Server on a daily basis. A script stored in the Backup Database Server will initiate the backup process on a daily basis.
- Internal Mail Server
  The internal mail server stores mail account for GIAC's internal employees, mobile employees and suppliers. This Internal mail server has a web mail function that is enabled for the mobile employees and suppliers only. The Internal Mail Server is well protected and it does not make direct contact with the Internet when it sends or receives email. It relies on the Mail Relay server in the Service Network to perform these tasks.
- Internal DHCP & File System

This server is allocated to assign dynamic IP for internal users and for internal file storage.

Security Consideration for GIAC's Servers & Desktops

A good security design should not omit considerations to enhance the security level of all GIAC's nodes that are locally or remotely connected to corporate network. Vulnerabilities on every Internal server should be minimized.
Below are the armoring steps that we have performed :-
For All Servers :

- Install the most recent hotfixes, service packs and patches
- Some operating systems by default had turned on some services that may not be required by the users. Therefore we have turned off some of the services that we do not need.
- We have set it as a company policy for users to use only strong password and make them change the password periodically
- Restrict users access right
- Follow steps recommended by respective vendor to harden the software for example, remove script mapping on a web server, etc
- Perform vulnerabilities test on the e-business applications developed by a third party
- Review permission files
- Avoid banner grabbing and strip email headers

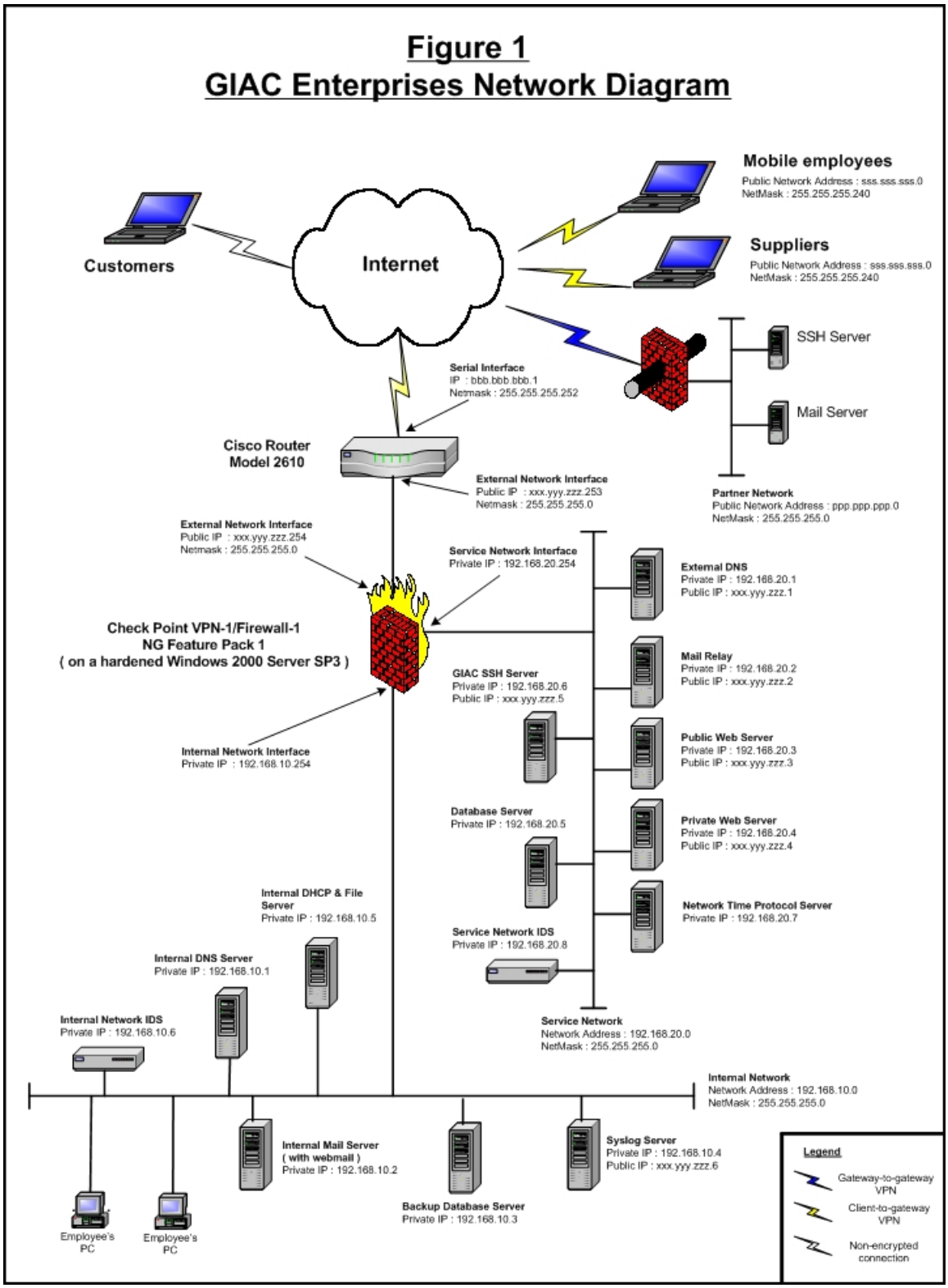
For Internal Desktops

- Install the most recent hotfixes, service packs and patches
- Install virus protection software

For Mobile Employes' and suppliers' Desktops

- Install the most recent hotfixes, service packs and patches
- Install virus protection software
- Install the SecureClient VPN software from Check Point. This software enabled the remote clients to establish client-to-gateway VPN connection with GIAC's firewall. The SecureClient software has a built-in personal firewall and feature to download desktop policies defined in GIAC's firewall

Figure 1
GIAC Enterprises Network Diagram



IP Addressing Scheme

The internal IP addresses assigned for GIAC Enterprises are strictly based on known non-routable addresses listed in RFC 1918. This can be found at http://www.isi.edu/in-notes/rfc1918.txt

All Public IP addresses use in this practical paper has been sanitized to fulfill the requirement set in GIAC Certification Administrivia. Therefore, all Public IP used in this assignment are represented with alphabets eg. xxx.yyy.zzz.0, bbb.bbb.bbb.0, ppp.ppp.ppp.0 and sss.sss.sss.0.

Below is a list of addresses allocated for GIAC Enterprises.

Group	Network Addresses	Net Mask
External serial interface of the border router	bbb.bbb.bbb.0 (represent serial IP address assign by the ISP)	255.255.255.252
External network	xxx.yyy.zzz.0 (represent the public IP address assign by the ISP)	255.255.255.0
Service network	192.168.20.0	255.255.255.0
Internal network	192.168.10.0	255.255.255.0
Partner Network	ppp.ppp.ppp.0 (assumption that these are the known public IP address of the Partners' network)	255.255.255.0
Suppliers & Mobile Employees	sss.sss.sss.0 (a pool of dial-up public IP purchased by GIAC from the ISP for suppliers and mobile employees. sss.sss.sss.0 –	255.255.255.240

	sss.sss.sss.15)	
Customers	Any	Any

Server	Private IP Address	Public IP Address
External serial interface of the border router		bbb.bbb.bbb.1
External Ethernet interface of the border router		xxx.yyy.zzz.253
Firewall external interface		xxx.yyy.zzz.254
Firewall interface at Service Network	192.168.20.254	
External DNS	192.168.20.1	xxx.yyy.zzz.1 (static NAT)
Mail Relay	192.168.20.2	xxx.yyy.zzz.2 (static NAT)
Public Web Server	192.168.20.3	xxx.yyy.zzz.3 (static NAT)
Private Web Server	192.168.20.4	xxx.yyy.zzz.4 (static NAT)
Database Server	192.168.20.5	
GIAC SSH Server	192.168.20.6	xxx.yyy.zzz.5 (static NAT)
NTP Server	192.168.20.7	
Service Network IDS	192.168.20.8	
Firewall interface at Internal Network	192.168.10.254	
Internal Network	192.168.10.0	xxx.yyy.zzz.254 (hide NAT)
Internal DNS Server	192.168.10.1	
Internal Mail Server	192.168.10.2	
Backup Database Server	192.168.10.3	
Syslog Server	192.168.10.4	xxx.yyy.zzz.6 (static NAT)
Internal DHCP & File Server	192.168.10.5	
Internal Network IDS	192.168.10.6	
System administrator	192.168.10.7	xxx.yyy.zzz.7 (static NAT)
Network administrator	192.168.10.8	xxx.yyy.zzz.8 (static NAT)
Sales administrator	192.168.10.9	xxx.yyy.zzz.9 (static NAT)

Assignment 2 – Security Policy and Tutorial

In our design, we have chosen to use a Cisco router Model 2610 with IOS version 12.2 as the border router. The border router is the first line of defense before the Check Point VPN-1/Firewall-1 NG FP 1 server.

Our methodology is to utilize the border router to do "absolute" filtering with static packet filtering. This helps greatly as it eliminates all possible "noise" from entering GIAC network at the very first point. With this first front inspection, the internal firewall will receive fewer loads and can reserve its expensive resources to do more advance firewall & VPN tasks efficiently. Besides filtering inbound packets, the border router will also perform outbound filtering to ensure that only legitimate packets leave GIAC's network.
(SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.2, page 67 and 83)

This section will explain how we could achieve the aforesaid methodology and also to define the security policy for the 3 main defense components (border router, firewall and VPN).

At the end of this assignment, a tutorial to implement the VPN policy will be defined.

Border Router Rules

To perform static packet filtering on the border router, we need to generate the access control lists (ACL). The access control list is a set of permit and deny rules that can be enforced at the border router for either ingress (inbound) or egress (outbound) filtering.

There are a few type of access control list that we can configure, namely the standard access list, extended access list and reflexive access list. Standard access list is simple and it only examines the source IP address of a packet. Therefore it is faster compare to extended and reflexive. Although Standard access list is the fastest, but we have decided to use Extended access list for the ingress and egress filtering as it impose better control than Standard access list. Extended access list can analyze additional criteria such as the source IP address, destination IP address, protocol, udp/tcp port & icmp types. We are not going to use Reflexive access list for stateful packet filtering, as it will use up a lot of CPU and memory processing power in our border router. It is more effective and efficient to perform the stateful filtering at the firewall.
(SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.3, page 14, 28 and 53)

Below are the general configuration, interface configuration and access control lists (ingress and egress filtering) that we had configured for GIAC with references and guides obtained from NSA/SNAC Router Security Configuration Guide at http://www.nsa.gov/snac/cisco/guides/cis-1.pdf, http://www.nsa.gov/snac/cisco/guides/cis-2.pdf, http://pasadena.net/cisco/secure.html , http://www.sans.org/infosecFAQ/firewall/egress.htm and http://www.iana.org/assignments/ipv4-address-space

To explain the general purpose of each rule, we have broken down the configuration into several portions with annotation.

General Configuration

The general configurations enable us to harden the border router.

It is very important to configure the password in a secure manner. The service password-encryption command will protect and store the enable secret password with MD5-based algorithm.

service password-encryption
enable secret <password>

These are small services for echo, discard, chargen and daytime. We must make sure that these services are disabled.

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

The attackers can make use of the Simple Network Monitoring Protocol (SNMP) to understand GIAC internal network infrastructure and the devices used. It is advisable to disable it.

no snmp-server

There are no clients in GIAC that require bootp service from the router.

no ip bootp server

The web server may be vulnerable for attack if it is enabled. Should be disabled unless web-based administration is required. For GIAC, we do not need it.

no ip http server

Finger daemon can show users who are logged on. Hackers can then use the login names of the administrator or other users and plan the attack. We must disable it.

no ip finger

Disable ip domain-lookup helps to prevent the router from sending DNS queries.

no ip domain-lookup

If we do not disabled ip source-route, the attacker can perform IP spoofing and re-route a packet as the IP source route can show paths that a packet takes to traverse between nodes.

no ip source-route

CDP stands for Cisco Discovery Protocol. For GIAC, we do not need it, therefore we should disabled it.

no cdp run

Sending the router's logs to the Internal Syslog server at internal network and do not write log messages on the console. Our Internal Syslog server IP is represented by xxx.yyy.zzz.6.

logging on
logging xxx.yyy.zzz.6
no logging console

This banner login is to warn anyone who deliberately or accidentally trying to logon to GIAC router with no permission.

banner login / WARNING : Authorised GIAC admin only /

Interface Configuration

Beside having the above general configuration, the interface configuration listed below also helps to harden the border router on the interface level.

Disable ip directed broadcast helps to prevent Layer 3 to Layer 2 broadcast mapping and smurf amplification.
(SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.3, page 60)

no ip directed-broadcast

Disable ip unreachable, proxy-arp and mask reply can prevent network mapping by attackers.

no ip unreachables
no ip proxy-arp
no ip mask-reply

To ensure that the border router does not send an ICMP redirect.

no ip redirects

To disable interfaces on the router from sending and receiving NTP requests.

ntp disable

To apply the interface configuration on the serial and Ethernet interfaces.

```
interface Serial 0/0
 ip address bbb.bbb.bbb.1 255.255.255.252
 no ip directed-broadcast
 no ip unreachables
 no ip proxy-arp
 no ip mask-reply
 no ip redirects
 ntp disable

interface Ethernet  0/0
 ip address xxx.yyy.zzz.253  255.255.255.0
 no ip directed-broadcast
 no ip unreachables
 no ip proxy-arp
 no ip mask-reply
 no ip redirects
 ntp disable
```

Only allow specific host to telnet into GIAC router for administration purposes. Our network administrator's desktop IP is represented by xxx.yyy.zzz.8.

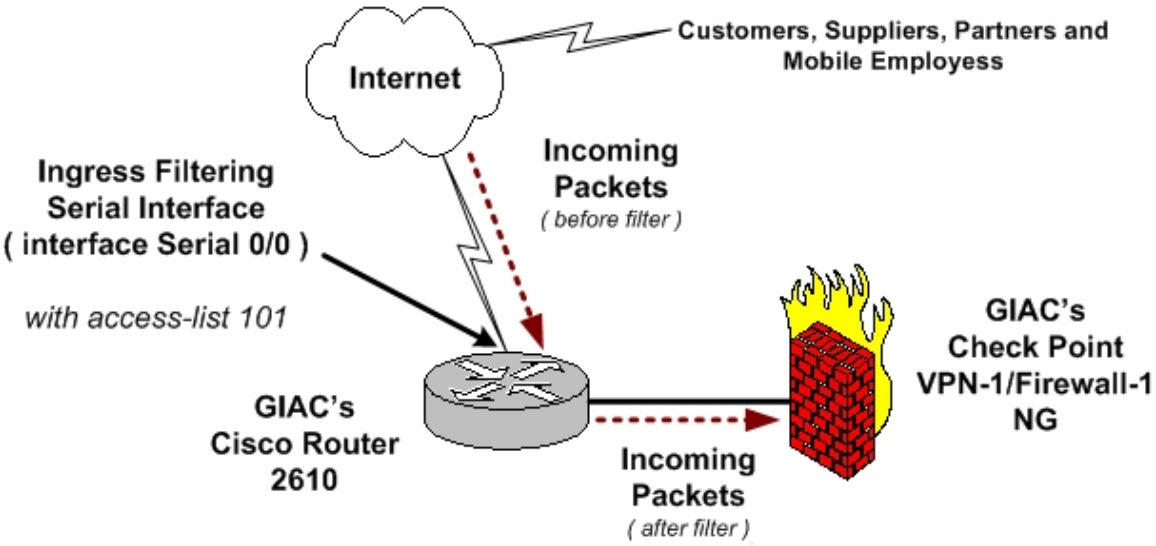
```
access-list 10 permit  xxx.yyy.zzz.8

line vty 0 4
access-class 10 in
password 7 0822455D0A16
login local
transport input telnet
```

Access Control List

Ingress Filtering Configuration

Extended access list 101 will be applied at the border router serial interface (serial 0/0) to filter inbound traffic from the Internet.



Block packets with source IP address of GIAC Internal and Service network address.

```
access-list 101 deny ip      192.168.0.0   0.0.255.255     any log
```

Block packets with source IP address of a private network address.

```
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
```

Block packets with source IP address of default DHCP failed address.

```
access-list 101 deny ip      169.254.0.0   0.0.255.255     any log
```

Block packets with source IP address of a multicast and reserved address.

```
access-list 101 deny ip      223.0.0.0     32.255.255.255        any log
```

Block packets with source IP address of a loopback address.

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

Block packets with source IP address of GIAC External network.

```
access-list 101 deny ip      xxx.yyy.zzz.0 0.0.0.255             any log
```

Block packets with source IP address of all unallocated legal IP addresses.

```
access-list 101 deny ip      0.0.0.0       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      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     1.255.255.255    any log
access-list 101 deny ip    58.0.0.0     1.255.255.255    any log
access-list 101 deny ip    70.0.0.0     9.255.255.255    any log
access-list 101 deny ip    83.0.0.0     6.255.255.255    any log
access-list 101 deny ip    90.0.0.0     9.255.255.255    any log
access-list 101 deny ip    100.0.0.0    9.255.255.255    any log
access-list 101 deny ip    110.0.0.0    9.255.255.255    any log
access-list 101 deny ip    120.0.0.0    6.255.255.255    any log
access-list 101 deny ip    173.0.0.0    6.255.255.255    any log
access-list 101 deny ip    180.0.0.0    7.255.255.255    any log
access-list 101 deny ip    189.0.0.0    1.255.255.255    any log
access-list 101 deny ip    197.0.0.0    0.255.255.255    any log
```

To prevent Smurf Attack from attackers who will send a lot of ICMP echo packets to GIAC's External network and broadcast address.

```
access-list 101 deny ip    any host     xxx.yyy.zzz.255      log
access-list 101 deny ip    any host     xxx.yyy.zzz.0        log
```

Block inbound ICMP traffic with echo packets to prevent attacker from creating a map on GIAC subnets and nodes behind the border router. The attacker can initiate a denial of service attack by sending a large amount of echo packets to the border router or internal nodes.

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

To prevent the attacker from making some changes to the routing table in a host with ICMP redirect packets.

```
access-list 101 deny icmp    any    any    redirect      log
```

To prevent the attacker from sending in a mask-request for internal IP address mask as a response.

```
access-list 101 deny icmp    any    any    mask-request  log
```

Permit only GIAC External network to receive icmp reply.

```
access-list 101 permit icmp    any    xxx.yyy.zzz.0    0.0.0.255    log
```

Block risky protocols – tcpmux

```
access-list 101 deny   tcp any any eq 1 log
access-list 101 deny   udp any any eq 1 log
```

Block risky protocols – echo

```
access-list 101 deny   tcp any any eq 7 log
access-list 101 deny   udp any any eq 7 log
```

Block risky protocols – discard

```
access-list 101 deny   tcp any any eq 9 log
access-list 101 deny   udp any any eq 9 log
```

Block risky protocols – systat
access-list 101 deny tcp any any eq 11 log

Block risky protocols – daytime
access-list 101 deny tcp any any eq 13 log
access-list 101 deny udp any any eq 13 log

Block risky protocols - netstat
access-list 101 deny tcp any any eq 15 log

Block risky protocols - chargen
access-list 101 deny tcp any any eq 19 log
access-list 101 deny udp any any eq 19 log

Block risky protocols – ftp, ftp-data
access-list 101 deny tcp any any range 20 21 log

Block risky protocols - time
access-list 101 deny tcp any any eq 37 log
access-list 101 deny udp any any eq 37 log

Block risky protocols - whois
access-list 101 deny tcp any any eq 43 log

Block risky protocols - bootp
access-list 101 deny udp any any eq 67 log

Block risky protocols - tftp
access-list 101 deny udp any any eq 69 log

Block risky protocols - finger
access-list 101 deny tcp any any eq 79 log

Block risky protocols – supdup
access-list 101 deny tcp any any eq 93 log

Block risky protocols – sunrpc
access-list 101 deny tcp any any eq 111 log
access-list 101 deny udp any any eq 111 log

Block risky protocols – loc-srv
access-list 101 deny tcp any any eq 135 log
access-list 101 deny udp any any eq 135 log

Block risky protocols – netbios-ns (137), netbios-dgm (138), netbios-ssn (139)
access-list 101 deny tcp any any range 137 139 log

access-list 101 deny udp any any range 137 139 log

Block risky protocols - xdmcp
access-list 101 deny udp any any eq 177 log

Block risky protocols – netbios (ds)
access-list 101 deny tcp any any eq 445 log

Block risky protocols – rexec
access-list 101 deny tcp any any eq 512 log

Block risky protocols – rlogin
access-list 101 deny tcp any any eq 513 log

Block risky protocols – who
access-list 101 deny udp any any eq 513 log

Block risky protocols – rsh, rcp, rdist, rdump
access-list 101 deny tcp any any eq 514 log

Block risky protocols – lpr
access-list 101 deny tcp any any eq 515 log

Block risky protocols – talk
access-list 101 deny udp any any eq 517 log

Block risky protocols – ntalk
access-list 101 deny udp any any eq 518 log

Block risky protocols – uucp
access-list 101 deny tcp any any eq 540 log

Block risky protocols – new who
access-list 101 deny tcp any any eq 550 log
access-list 101 deny udp any any eq 550 log

Block risky protocols – Microsoft UpnP SSDP
access-list 101 deny tcp any any eq 1900 log
access-list 101 deny udp any any eq 1900 log
access-list 101 deny tcp any any eq 5000 log
access-list 101 deny udp any any eq 5000 log

Block risky protocols – nfs
access-list 101 deny udp any any eq 2049 log

Block risky protocols – X Window System

access-list 101 deny tcp any any range 6000 6063 log

Block risky protocols – IRC
access-list 101 deny tcp any any eq 6667 log

Block risky protocols – NetBus
access-list 101 deny tcp any any range 12345 12346 log

Block risky protocols – Back Orifice
access-list 101 deny tcp any any eq 31337 log
access-list 101 deny udp any any eq 31337 log

Block risky protocols – snmp snmptrap
access-list 101 deny tcp any any range 161 162 log
access-list 101 deny udp any any range 161 162 log

Block risky protocols – syslog
access-list 101 deny udp any any eq 514 log

The following access lists will address GIAC business needs and users access requirements as identified in Assignment 1.

Only allows TCP traffic connections that have been established from GIAC External network.
access-list 101 permit tcp any xxx.yyy.zzz.0 0.0.0.255 established

Allow DNS access to GIAC External DNS server and with no log.
access-list 101 permit udp any xxx.yyy.zzz.1 eq 53

Allow smtp access to GIAC Mail relay server and with no log.
access-list 101 permit tcp any xxx.yyy.zzz.2 eq 25

Allow http access to GIAC Public web server and with no log.
access-list 101 permit tcp any xxx.yyy.zzz.3 eq 80

Allow https access to GIAC Public web server and with no log.
access-list 101 permit tcp any xxx.yyy.zzz.3 eq 443

Allow http access to GIAC Private web server and with no log (for partners, suppliers and mobile employees).
access-list 101 permit tcp ppp.ppp.ppp.0 0.0.0.255 xxx.yyy.zzz.4 eq 80
access-list 101 permit tcp sss.sss.sss.0 0.0.0.15 xxx.yyy.zzz.4 eq 80

Allow https access to GIAC Private web server and with no log (for partners, suppliers and mobile employees).

access-list 101 permit tcp ppp.ppp.ppp.0 0.0.0.255 xxx.yyy.zzz.4 eq 443
access-list 101 permit tcp sss.sss.sss.0 0.0.0.15 xxx.yyy.zzz.4 eq 443

Allow SSH access to GIAC SSH server and with no log (for partners, suppliers and mobile employees).

access-list 101 permit tcp ppp.ppp.ppp.0 0.0.0.255 xxx.yyy.zzz.5 eq 22
access-list 101 permit tcp sss.sss.sss.0 0.0.0.15 xxx.yyy.zzz.5 eq 22

Allow webmail access to GIAC Internal mail server and with no log (for suppliers and mobile employees).

access-list 101 permit tcp sss.sss.sss..0 0.0.0.15 xxx.yyy.zzz.2 eq 80

Allow VPN tunnel to be established with partners, suppliers and mobile employee via GIAC firewall and with log.

access-list 101 permit ip ppp.ppp.ppp.0 0.0.0.255 host xxx.yyy.zzz.254 log
access-list 101 permit ip sss.sss.sss.0 0 0.0.0.15 host xxx.yyy.zzz.254 log

Final rule to deny and to log packets that are not allow.

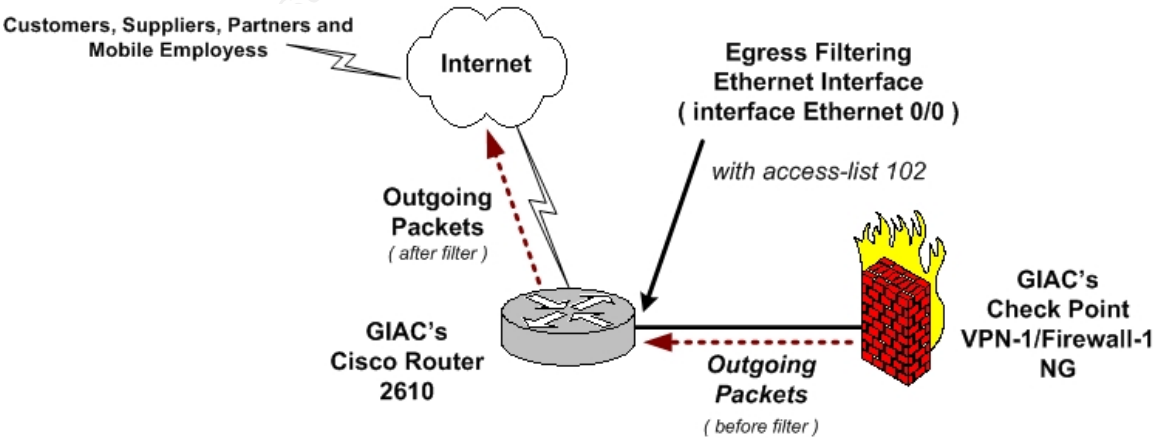
access-list 101 deny ip any any log

To enable the access-list 101 on the serial interface of the router.

interface Serial 0/0
ip address bbb.bbb.bbb.1 255.255.255.252
ip access-group 101 in

Egress Filtering Configuration

Extended access list 102 will be applied at the border router Ethernet interface (Ethernet 0/0) to filter outgoing traffic to the Internet.



Block packets with source IP address of GIAC Internal and Service network address.

```
access-list 102 deny ip    192.168.0.0   0.0.255.255   any log
```

Block packets with source IP address of a private network address.

```
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
```

Block packets with source IP address of default DHCP failed address.

```
access-list 102 deny ip    169.254.0.0   0.0.255.255   any log
```

Block packets with source IP address of a multicast and reserved address.

```
access-list 102 deny ip    223.0.0.0     32.255.255.255      any log
```

Block packets with source IP address of a loopback address.

```
access-list 102 deny ip    127.0.0.0     0.255.255.255       any log
```

Block packets with source IP address of all unallocated legal IP addresses.

```
access-list 102 deny ip    0.0.0.0       0.255.255.255       any log
access-list 102 deny ip    1.0.0.0       0.255.255.255       any log
access-list 102 deny ip    2.0.0.0       0.255.255.255       any log
access-list 102 deny ip    5.0.0.0       0.255.255.255       any log
access-list 102 deny ip    7.0.0.0       0.255.255.255       any log
access-list 102 deny ip    23.0.0.0      0.255.255.255       any log
access-list 102 deny ip    27.0.0.0      0.255.255.255       any log
access-list 102 deny ip    31.0.0.0      0.255.255.255       any log
access-list 102 deny ip    36.0.0.0      1.255.255.255       any log
access-list 102 deny ip    39.0.0.0      0.255.255.255       any log
access-list 102 deny ip    41.0.0.0      1.255.255.255       any log
access-list 102 deny ip    58.0.0.0      1.255.255.255       any log
access-list 102 deny ip    70.0.0.0      9.255.255.255       any log
access-list 102 deny ip    83.0.0.0      6.255.255.255       any log
access-list 102 deny ip    90.0.0.0      9.255.255.255       any log
access-list 102 deny ip    100.0.0.0     9.255.255.255       any log
access-list 102 deny ip    110.0.0.0     9.255.255.255       any log
access-list 102 deny ip    120.0.0.0     6.255.255.255       any log
access-list 102 deny ip    173.0.0.0     6.255.255.255       any log
access-list 102 deny ip    180.0.0.0     7.255.255.255       any log
access-list 102 deny ip    189.0.0.0     1.255.255.255       any log
access-list 102 deny ip    197.0.0.0     0.255.255.255       any log
```

This is to prevent Land Attack on the border router. Land attack can cause denial of service or to degrade a router's performance. An attacker can send a packet with same IP for the source and destination addresses.

```
access-list 102 deny ip    host xxx.yyy.zzz.253    host xxx.yyy.zzz.253    log
```

Permit outbound ICMP traffic with echo packets so that GIAC's administrator will be able to ping external hosts and request for information, mask and timestamp. Parameter problem and source quench can improve connectivity by informing the opposite nodes to slow down the delivery rate as the receiving node is facing problem coping with the traffic. Packet too big is for path MTU discovery.

```
access-list 102 permit icmp   xxx.yyy.zzz.0   0.0.0.255  any echo
access-list 102 permit icmp   xxx.yyy.zzz.0   0.0.0.255  any parameter-problem
access-list 102 permit icmp   xxx.yyy.zzz.0   0.0.0.255  any packet-too-big
access-list 102 permit icmp   xxx.yyy.zzz.0   0.0.0.255  any source-quench
access-list 102 permit icmp   xxx.yyy.zzz.0   0.0.0.255  any information-request
access-list 102 permit icmp   xxx.yyy.zzz.0   0.0.0.255  any mask-request
access-list 102 permit icmp   xxx.yyy.zzz.0   0.0.0.255  any timestamp-request
```

Block risky protocols – tcpmux

```
access-list 102 deny   tcp any any eq 1 log
access-list 102 deny   udp any any eq 1 log
```

Block risky protocols – echo

```
access-list 102 deny   tcp any any eq 7 log
access-list 102 deny   udp any any eq 7 log
```

Block risky protocols – discard

```
access-list 102 deny   tcp any any eq 9 log
access-list 102 deny   udp any any eq 9 log
```

Block risky protocols – systat

```
access-list 102 deny   tcp any any eq 11 log
```

Block risky protocols – daytime

```
access-list 102 deny   tcp any any eq 13 log
access-list 102 deny   udp any any eq 13 log
```

Block risky protocols - netstat

```
access-list 102 deny   tcp any any eq 15 log
```

Block risky protocols - chargen

```
access-list 102 deny   tcp any any eq 19 log
access-list 102 deny   udp any any eq 19 log
```

Block risky protocols – ftp, ftp-data

```
access-list 102 deny   tcp any any range 20 21 log
```

Block risky protocols - time

```
access-list 102 deny   tcp any any eq 37 log
```

access-list 102 deny udp any any eq 37 log

Block risky protocols - whois
access-list 102 deny tcp any any eq 43 log

Block risky protocols - bootp
access-list 102 deny udp any any eq 67 log

Block risky protocols - tftp
access-list 102 deny udp any any eq 69 log

Block risky protocols – supdup
access-list 102 deny tcp any any eq 93 log

Block risky protocols – sunrpc
access-list 102 deny tcp any any eq 111 log
access-list 102 deny udp any any eq 111 log

Block risky protocols – loc-srv
access-list 102 deny tcp any any eq 135 log
access-list 102 deny udp any any eq 135 log

Block risky protocols – netbios-ns (137), netbios-dgm (138), netbios-ssn (139)
access-list 102 deny tcp any any range 137 139 log
access-list 102 deny udp any any range 137 139 log

Block risky protocols - xdmcp
access-list 102 deny udp any any eq 177 log

Block risky protocols – netbios (ds)
access-list 102 deny tcp any any eq 445 log

Block risky protocols – rexec
access-list 102 deny tcp any any eq 512 log

Block risky protocols – lpr
access-list 102 deny tcp any any eq 515 log

Block risky protocols – talk
access-list 102 deny udp any any eq 517 log

Block risky protocols – ntalk
access-list 102 deny udp any any eq 518 log

Block risky protocols – uucp
access-list 102 deny tcp any any eq 540 log

Block risky protocols – Microsoft UpnP SSDP
access-list 102 deny tcp any any eq 1900 log
access-list 102 deny udp any any eq 1900 log
access-list 102 deny tcp any any eq 5000 log
access-list 102 deny udp any any eq 5000 log

Block risky protocols – nfs
access-list 102 deny udp any any eq 2049 log

Block risky protocols – X Window System
access-list 102 deny tcp any any range 6000 6063 log

Block risky protocols – IRC
access-list 102 deny tcp any any eq 6667 log

Block risky protocols – NetBus
access-list 102 deny tcp any any range 12345 12346 log

Block risky protocols – Back Orifice
access-list 102 deny tcp any any eq 31337 log
access-list 102 deny udp any any eq 31337 log

Block risky protocols – snmp snmptrap
access-list 102 deny tcp any any range 161 162 log
access-list 102 deny udp any any range 161 162 log

Block outgoing ICMP host unreachable to an external hosts, which could be attackers. This prevents the attacker from knowing that the host is not available.
access-list 102 deny icmp any any host-unreachable

Block outgoing ICMP echo- replies (type 0) to an external hosts which could be attackers. This prevent the attacker from knowing that the host is available.
access-list 102 deny icmp any any echo-reply

Block outgoing ICMP time-exceeded (type 11) for a packet which its Time To Live that has expired. If the attacker receive the ICMP time-exceeded, he or she can get more information about GIAC's network infrastructure.
access-list 102 deny icmp any any time-exceeded

Permit all outgoing traffic that originate from GIAC External network.
access-list 102 permit ip xxx.yyy.zzz.0 0.0.0.255 any

Final rule to deny and to log packets that are not allow.

access-list 102 deny ip any any log

To enable the access-list 102 on the Ethernet interface of the router.

interface Ethernet 0/0
ip address xxx.yyy.zzz.253 255.255.255.0
ip access-group 102 in

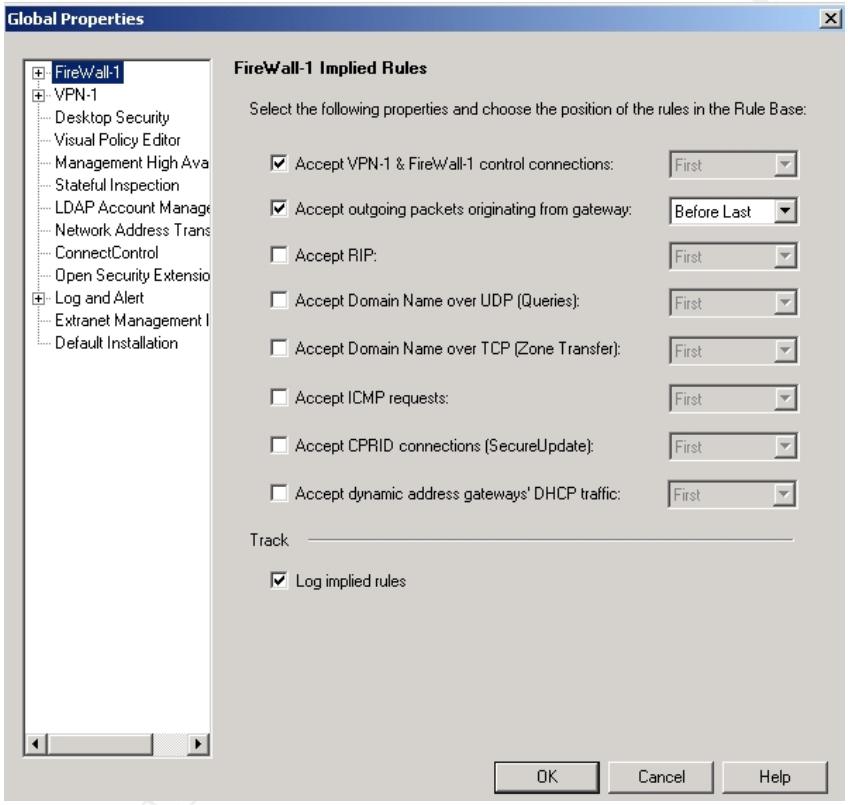
Order of The ACL

The order of the access control lists in the border router plays a very important role. Packets are match against the access control list in a top down manner. With the same set of control lists but in a different order can change the logic of packet inspection. It is primarily important to ensure that the order of our access control list are correct in order to achieve the correct filtering and to improve the border router's performance.

Firewall Rules

There are a few good points that we should follow in order to build a better set of rule base in the firewall. Below are some of the tips that I have learned from Lance Spitzner's white paper "Building Your Firewall Rule base". The white paper can be obtained at http://www.spitzner.net/rules.html

1. Default Properties
   There are a few services that are open by default in Check Point Firewall-1. We should turn off these open ports.



We should uncheck several implied rules that is enabled by default such as :-

- accept domain name over UDP (queries)
- accept domain name over TCP (zone transfer)
- accept ICMP requests
- accept CPRID connections (SecureUpdate)
- accept dynamic address gateways' DHCP traffic

If we need these services, we should add it into our rule base as enabling these options here will not log any of these activities.
(SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.2, pg 168-169)

2. Ban List

We should not allow any Internet advertisers or known attacker sites from entering and leaving GIAC network. We should drop this connection at the very beginning to avoid any security flaws and to improve firewall performance.

Rule 1 - will drop and log any incoming traffic from sites listed in our ban list.

Rule 2 - will drop and log any outgoing traffic to the sites listed in our ban list.

1	Ban-List	* Any	* Any	drop	Log	* Policy Targets	* Any	Ban Ho
2	* Any	Ban-List	* Any	drop	Log	* Policy Targets	* Any	Firewa

3. Lockdown Rule

A lockdown rule helps to block any access destine to the firewall.

Rule 3 - is a lockdown rule that helps to protect the firewall from any unauthorized access or attack.

3	* Any	GIAC-FW	* Any	drop	Log	* Policy Targets	* Any	Stealth Rule

4. Drop All

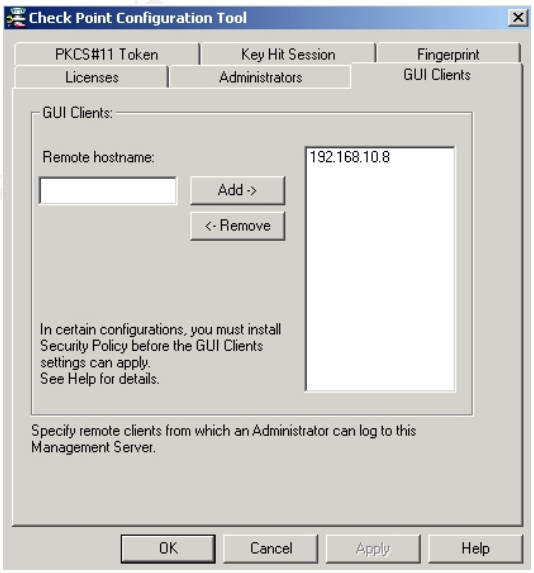
All packets that do not match any rules will be dropped by Check Point Firewall-1 but not log (by default). Therefore we should set to log it.

Rule 21 - is the last rule in the rule base that will drop and log all packets that do not match any rules.

21	* Any	* Any	* Any	drop	Log	* Policy Targets	* Any	Cleanu

5. Administrator's Access

We should define in our firewall to allow only the network administrator to access and manage the firewall via remote GUI client. The network administrator's desktop internal IP address is 192.168.10.8.



6. Performance Issue
   To improve the firewall performance, all common rules should be positioned at the beginning of the rule base. We will explain our rule base order at the end of this assignment 3.

Rule #1, 2 and 3 have been explained earlier.

External DNS
Purpose : To allow incoming domain name queries on GIAC's fully qualified domain name (FQDN) that resides in GIAC's External DNS server

Source	Destination	Service	Action	Track
Any (inclusive of Internal DNS server)	External DNS	domain-udp 53	accept	Log

Customers
Purpose : To allow customers or public to access the Public Web Server

Source	Destination	Service	Action	Track
Any	Public WebServer	http tcp 80 https tcp 443	accept	Log

Mail Relay
Purpose : To enable the Mail Relay server to receive incoming mail
To enable the Internal mail server to send outgoing email (to the Internet) via Mail Relay server

Source	Destination	Service	Action	Track
Any (inclusive of Internal Mail Server)	Mail Relay	smtp tcp 25	accept	Log

External DNS
Purpose : To enable the external DNS server to do external domain name queries

Source	Destination	Service	Action	Track
External DNS	Any	domain-udp 53 domain-tcp 53	accept	None

Mail Relay

Purpose : To enable Mail relay to forward incoming email to Internal mail server
To enable Mail relay to send internal users' email out to the Internet

Source	Destination	Service	Action	Track
Mail Relay	Any (inclusive of Internal Mail Server)	smtp tcp 25	accept	Log

Internal DNS

Purpose : To enable the internal DNS server to query the External DNS server for domain name resolution

Source	Destination	Service	Action	Track
Internal DNS	External DNS	domain-tcp 53	accept	Log

Rule #10, 11 and 12 will be explained later as VPN Rule Base

Network-Admin

Purpose : To allow the network administrator (at Internal network) to manage the border router by doing telnet sessions
To allow the network administrator (at Internal network) to manage the Service Network IDS via https

Source	Destination	Service	Action	Track
Network-Admin	Border Router Service Network	telnet tcp 23 https tcp 443	accept	Log

	IDS			

System-Admin

Purpose : To allow the system administrator (at Internal network) to manage all systems on Service Network

Source	Destination	Service	Action	Track
System - Admin	Service Network Systems	ssh tcp 22	accept	Log

Internal Network

Purpose : To enable internal staff on the internal network to do Internet browsing

Source	Destination	Service	Action	Track
Internal Network	Any	http tcp 80 https tcp 443	accept	None

GIAC-System

Purpose : To allow GIAC-System (comprise of service network servers and border router) to send its log file to the syslog server that resides at the Internal Network

Source	Destination	Service	Action	Track
GIAC-System	Syslog Server	syslog udp 514	accept	Log

Internal-Network

Purpose : To enable all internal nodes on Internal network to synchronous network time from the NTP server that resides on the Service network

Source	Destination	Service	Action	Track
Internal Network	NTP Server	ntp udp 123	accept	Log

Backup Database

Purpose : To perform periodic data backup from Database server at Service Network to Backup Database server at Internal Network

Source	Destination	Service	Action	Track
Backup Database	Database	tcp 1521	accept	Log

Administration

Purpose : To allow administrators and servers to send ICMP requests to external hosts

Source	Destination	Service	Action	Track
Network Admin System Admin Service-Net-System Internal-Net System	Any	ICMP Request	accept	Log

Administration

Purpose : To allow administrators and servers to receive ICMP replies from external hosts

Source	Destination	Service	Action	Track
Any	Network Admin System Admin Service-Net-System Internal-Net System	ICMP Replies	accept	Log

Rule #21 has been explained earlier.

VPN Rule Base

On GIAC's VPN Gateway

Incoming Traffic

The VPN settings use for suppliers and mobile sales & teleworkers are as below :-

Encryption schemes – IKE
Key exchange encryption – 3DES
Data integrity – MD5
Authentication method – VPN-1 & Firewall-1 password

Suppliers and Mobile Sales & Teleworkers

Purpose : To allow dialup suppliers and mobile employees

- to browse the Private Web Server
- to upload data to the GIAC SSH server
- to access webmail via Mail Relay (proxy)

Source	Destination	Service	Action	Track
SC-Group@Any	Private Web Server GIAC SSH Server Mail Relay	http tcp 80 https tcp 443 ssh tcp 22 webmail tcp 80	Client encrypt	Log

Partner

The VPN settings with our partners are as listed below :-

Encryption schemes – IKE
Key exchange encryption – 3DES
Data integrity – MD5
Authentication method – Pre-shared secrets

Purpose : To allow partners

- to browse the Private Web Server
- to upload and download data to the GIAC SSH server
- to send email to GIAC Enterprises

Source	Destination	Service	Action	Track
Partner Network	Private Web Server	http tcp 80 https tcp 443	encrypt	Log

	GIAC-SSH-Server Mail Relay	ssh tcp 22 smtp tcp 25		

Outgoing Traffic

Sales Admin

Purpose : To allow the sales administrator to upload invoices and other marketing data to the Partner's SSH server

Source	Destination	Service	Action	Track
Sales Admin	Partner SSH Server	ssh tcp 22	encrypt	Log

VPN Client's Desktop Rule at Policy Server

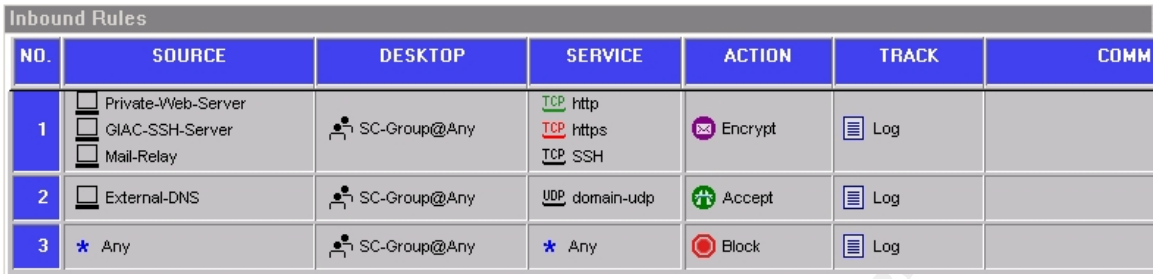
Incoming Traffic

Purpose : To allow the Private Web Server, GIAC SSH server, GIAC External DNS and Mail Relay to response to remote client's request for

- http, https
- ssh
- domain-udp (without VPN encryption, normal traffic)
- webmail access

Source	Destination	Service	Action	Track
Private Web Server GIAC SSH Server Mail Relay	SC-Group@Any	http tcp 80 https tcp 443 ssh tcp 22 webmail tcp 80	encrypt	Log
External DNS	SC-Group@Any	domain-udp 53	accept	Log

Any	SC-Group@Any	Any	Block	Log



Rule #1 allow that the remote client to receive responses from the private web server, GIAC SSH server and the Mail Relay via the client-to-gateway VPN tunnel
Rule #2 allow the remote client to receive responses from the External DNS without having to encrypt the domain-udp traffic.
Rule #3 is the protection rule for the remote VPN client. This prevent hackers or crackers from connecting to remote VPN client's desktop.

Outgoing Traffic

Purpose : To allow dialup suppliers and mobile employees

- to browse the Private Web Server
- to upload their data to the GIAC SSH server
- to access webmail via Mail Relay (proxy)
- to resolve hostname using GIAC External DNS server (without VPN encryption, normal traffic)

Desktop	Destination	Service	Action	Track
SC-Group@Any	Private Web Server GIAC SSH Server Mail Relay	http tcp 80 https tcp 443 ssh tcp 22 webmail tcp 80	encrypt	Log
SC-Group@Any	External DNS	domain-udp 53	accept	Log
SC-Group@Any	Any	Any	Block	Log

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK
4	SC-Group@Any	Private-Web-Server GIAC-SSH-Server Mail-Relay	TCP http TCP https TCP SSH	Encrypt	Log
5	SC-Group@Any	External-DNS	UDP domain-udp	Accept	Log
6	SC-Group@Any	* Any	* Any	Block	Log

Rule #4 ensure that the remote VPN client are allow to access the private web server, GIAC SSH server and the Mail Relay with a client-to-gateway VPN tunnel.
Rule #5 specifies that the remote client can access the External DNS but without having to encrypt the domain-udp traffic.
Rule #6 is the restrict rule that disallow the remote VPN client to access other destinations that are not define within the local encryption domain. This is for security purposes.

Order of The Firewall Rule Base

It is very important to spend some time evaluating the order of the rule base in the firewall. Rules are process in an orderly manner. Firewall will inspect a packet against the very first rule, second rule and so on till it found a rule that satisfies the condition or it will drop the packet if no match is found. It is not the best match rule that will be applied but is the first matched rule. Placing the same set of rule but in different order will produce different security results and performance.

Placing the rule base in a right order not only helps to improve the firewall performance but it certainly helps to prevent wrong configurations.

Below is the complete set of our rule base.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	
1	Ban-List	* Any	* Any	drop	Log	* Policy Targets	* Any	Ban Ho
2	* Any	Ban-List	* Any	drop	Log	* Policy Targets	* Any	Firewa
3	* Any	GIAC-FW	* Any	drop	Log	* Policy Targets	* Any	Stealth
4	* Any	External-DNS	UDP domain-udp	accept	Log	* Policy Targets	* Any	Any -->
5	* Any	Public-Web-Server	TCP http TCP https	accept	Log	* Policy Targets	* Any	Public
6	* Any	Mail-Relay	TCP smtp	accept	Log	* Policy Targets	* Any	Mail Re
7	External-DNS	* Any	UDP domain-udp TCP domain-tcp	accept	Log	* Policy Targets	* Any	DNS -->
8	Mail-Relay	* Any	TCP smtp	accept	Log	* Policy Targets	* Any	Mail Re
9	Internal-DNS	External-DNS	TCP domain-tcp	accept	Log	* Policy Targets	* Any	Int DNS
10	SC-Group@Any	Private-Web-Server GIAC-SSH-Server Mail-Relay	TCP http TCP https TCP SSH	Client Encrypt	Log	* Policy Targets	* Any	Secure
11	Partner-Network	Private-Web-Server GIAC-SSH-Server Mail-Relay	TCP http TCP https TCP SSH TCP smtp	Encrypt	Log	* Policy Targets	* Any	Partner
12	Sales-Admin	Partner-SSH-Server	TCP SSH	Encrypt	Log	* Policy Targets	* Any	Sales A
13	Network-Admin	Border-Router Service-Net-IDS	TCP telnet TCP https	accept	Log	* Policy Targets	* Any	Networ
14	System-Admin	Service-Net-System	TCP SSH	accept	Log	* Policy Targets	* Any	System
15	Internal-Network	* Any	TCP http TCP https	accept	Log	* Policy Targets	* Any	Interna
16	GIAC-System	SyslogServer	UDP syslog	accept	Log	* Policy Targets	* Any	Syslog
17	Internal-Network	NTP-Server	UDP ntp-udp	accept	Log	* Policy Targets	* Any	NTP Ru
18	Backup-Database	Database-Server	TCP sqlnet2-1521	accept	Log	* Policy Targets	* Any	Backup
19	Network-Admin System-Admin Service-Net-System Internal-Net-System	* Any	icmp-requests	accept	Log	* Policy Targets	* Any	
20	* Any	Network-Admin System-Admin Service-Net-System Internal-Net-System	ICMP dest-unreach ICMP echo-reply ICMP info-reply ICMP mask-reply ICMP time-exceeded ICMP timestamp-reply	accept	Log	* Policy Targets	* Any	
21	* Any	* Any	* Any	drop	Log	* Policy Targets	* Any	Cleanu

Rule #1 and #2 are rules created to block known attacker sites and advertiser from entering and leaving GIAC's network. There is no valid reason why we should allow these packets to be processed against any other rules for matches. Just drop it from the beginning. We should do similarly for the lockdown rule (rule #3). Placing the lockdown rule will deter access and attack to the firewall. This can safeguard the firewall from being compromise.

The next consideration is to place the most frequent hit rules and specific rules before any other general rules. This will speed up the network access and we can impose strict inspection on every packet. Rule # 4 to rule # 9 are the frequent hit rules as it serve e-business requirements. The next placement is the VPN rules (rule #10 till rule #12) for our remote suppliers, mobile employees and partners. We noticed that these groups of people have made their access quite often. Therefore, rule #10 to rule #12 should be placed before the internal access rules (rule #13 to rule # 20).

Rules #13 till rule #20 are basically the internal administration rule. The number of hits for these rules is low so therefore it should be placed below. The very last rule (rule #21) is to drop and log all packets that do not match any of the rule bases.

Please take note that it is practically important to periodically review and adjust the order of the rule base. When new rules are added or existing rules are removed, it can radically affect the firewall's performance and behavior as the logic and order of the rule base has changed.

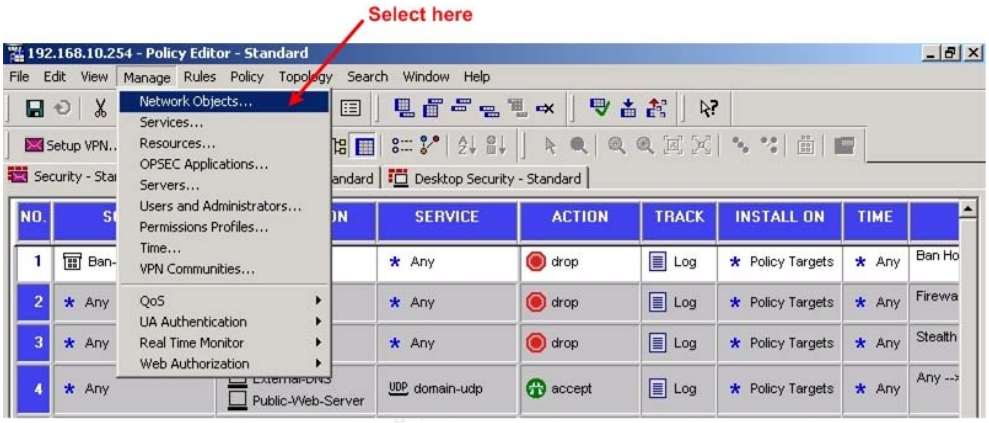
Tutorial for VPN Policy Implementation

References were made from the Student Edition book of Check Point VPN-1/Firewall-1 Management I & II NG before compiling this tutorial. The sequence of steps and some tips were excerpted from the book.
** Please take note that the numbers with circles on the snapshots are added to enhance the explanation of each steps labeled as a, b, c, etc.

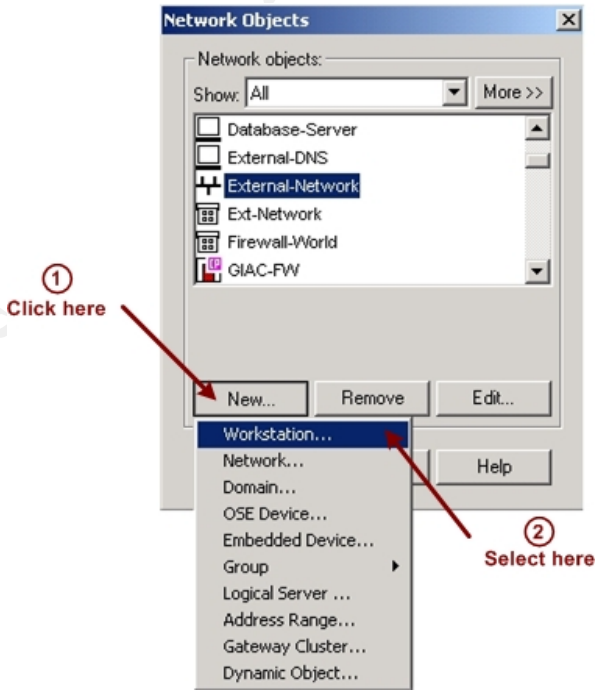
Create network objects

This section will explain ways to create network objects (host or gateway)

a. From the Policy Editor, click on the Manage menu and select the Network Objects option from the list.



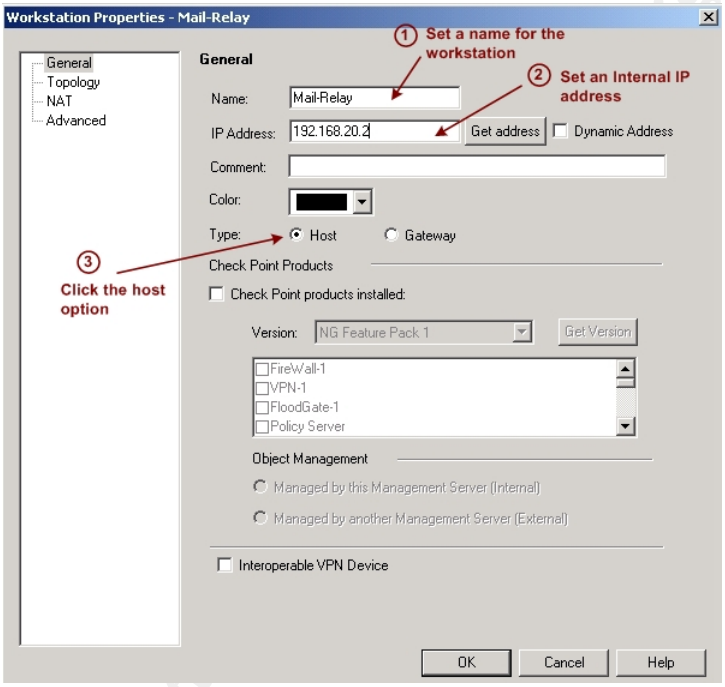
b. The network object screen will appear as below. Click on the New button and select workstation option.



**Note: Step c and d describe ways to create a host object
Step c1 and d1 describe ways to create a gateway object

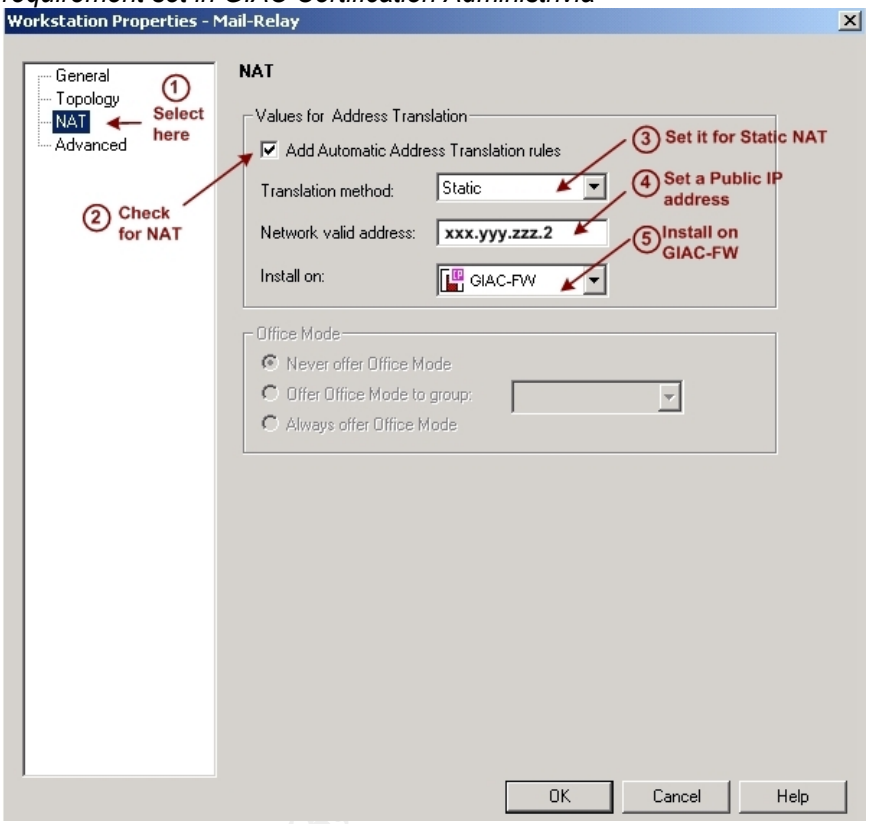
Host object

c. The workstation properties screen will appear as below. Key in a name for the host object, set an internal IP address and click type as host (example shown below is for the Mail Relay server).
Tips : Please make sure that the host object is set as host NOT gateway.



d. At the left pane, select the NAT option. Check on the “Add Automatic Address Translation rules” to enable NAT for this workstation. Set it as Static NAT (one public IP for one workstation), set a Public IP address (to translate internal IP of 192.168.20.2 → Public IP of xxx.yyy.zzz.2) and install on the GIAC-FW.

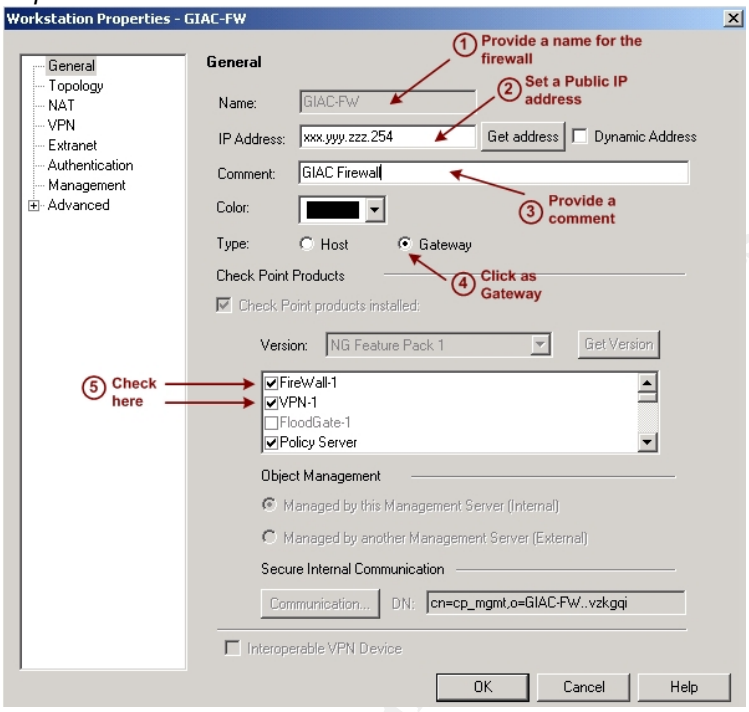
The external network IP address for this snapshot has been sanitized to fulfill the requirement set in GIAC Certification Administrivia



Gateway Object

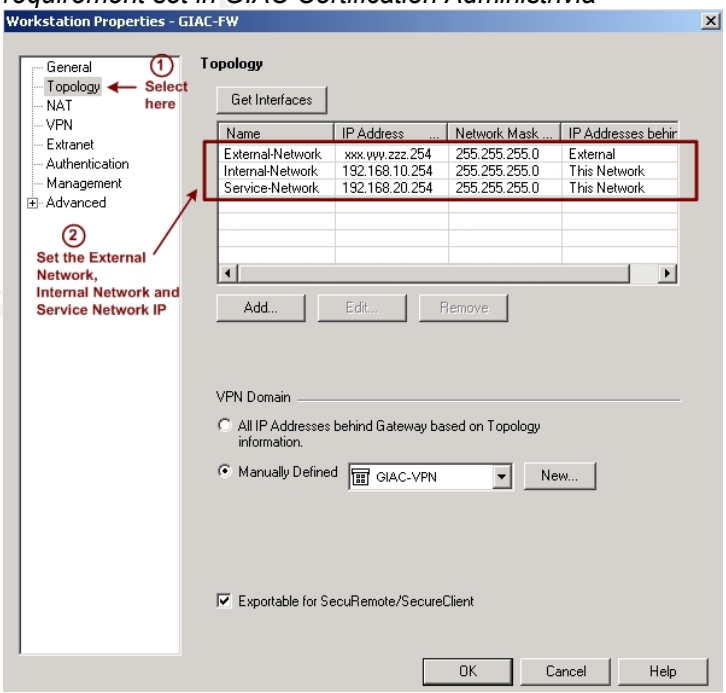
c1. The workstation properties shall appear as below. Key in a name for the gateway object, set a Public IP address, give a comment and click type as gateway (example shown below is for GIAC Firewall). Check the install option for Firewall-1 and VPN-1 (for integrated Firewall-1 & VPN-1 function). The Policy Server option will be discussed later (Configuring Policy Server section).
Tips : Please make sure that the firewall object is set as a gateway NOT host. The VPN-1 option must be checked as we are integrating the VPN gateway with the firewall.

The external network IP address for this snapshot has been sanitized to fulfill the requirement set in GIAC Certification Administrivia



d1. At the left pane, select the topology option. Set the External network, Internal network and Service network IP address and network mask for the firewall.

The external network IP address for this snapshot has been sanitized to fulfill the requirement set in GIAC Certification Administrivia



Gateway–to-Gateway VPN
(using IKE Encryption Method)

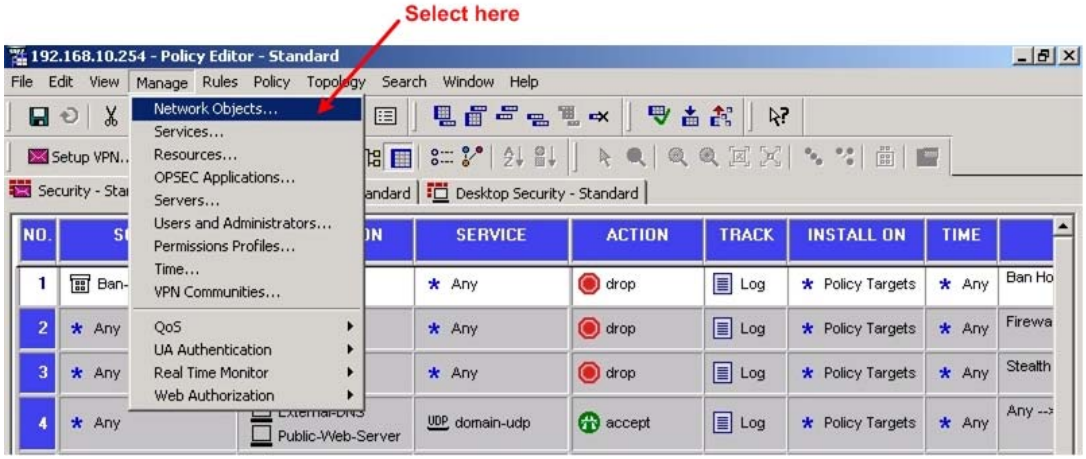
This section will explain ways to implement gateway-to-gateway VPN between GIAC's office and partners' office.

Before we could proceed with the configuration, it is very important for us to exchange information with our partners on the encryption schemes, data integrity and authentication methods. Configurations at both ends must be the same in order to establish the VPN connection. For our case, our partners and us had agreed to enable the configurations below in our firewalls.

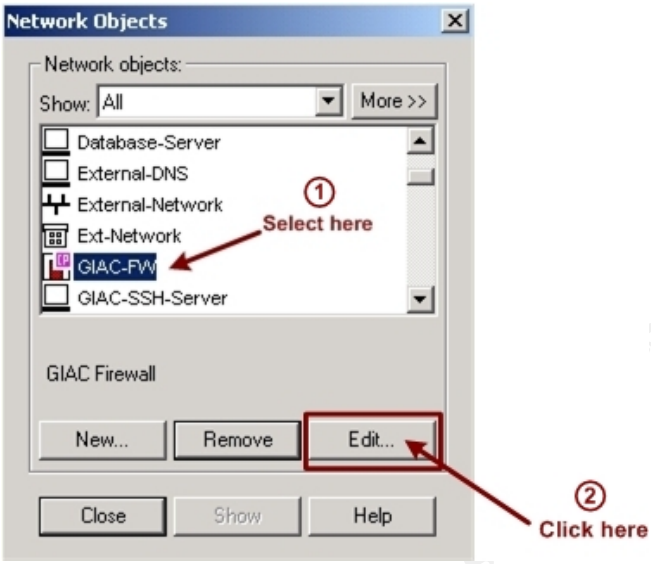
Encryption schemes	– IKE
Key exchange encryption	– 3DES
Data integrity	– MD5
Authentication method	– Pre-shared secrets

1. First, we need to configure the encryption domain for GIAC-Firewall
   This is important as we need to define objects or networks to be protected within the VPN tunnel.

   a. From the Policy Editor, click on the Manage menu and select the Network Objects option from the list.

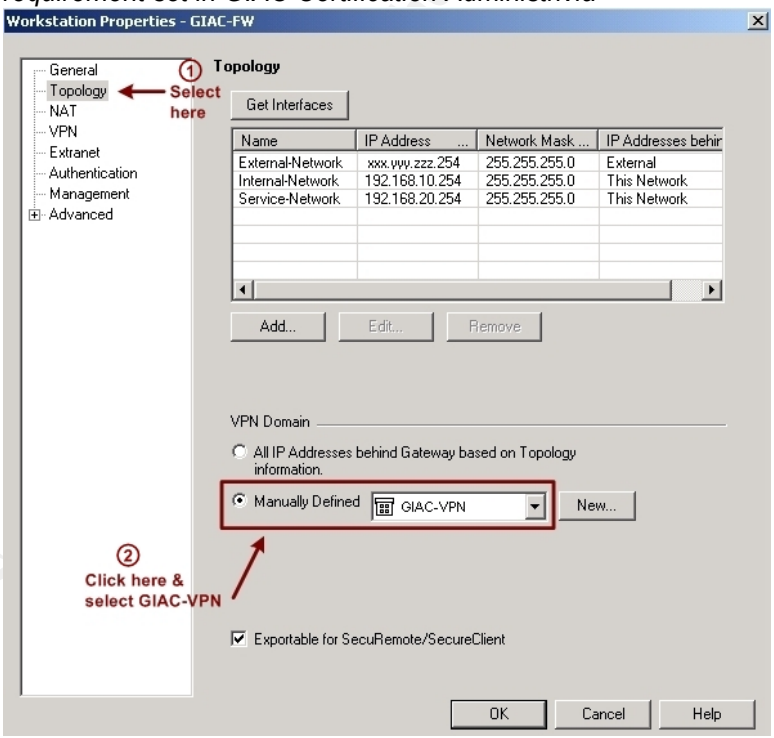


   b. The Network Objects screen will appear as below. Select GIAC-FW and click on the Edit button.



c. The GIAC-FW workstation properties will be displayed as below. At the left pane, select the topology option.

The external network IP address for this snapshot has been sanitized to fulfill the requirement set in GIAC Certification Administrivia

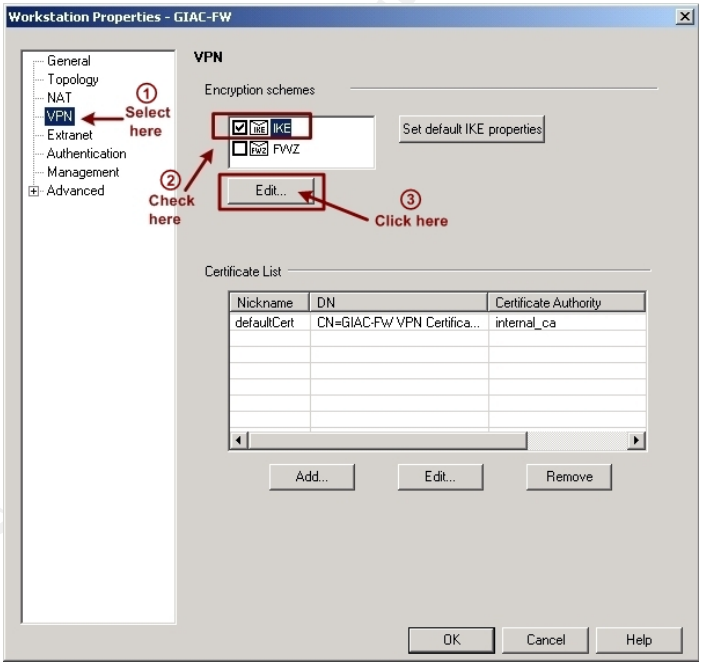


d. At the VPN Domain section, make sure that you click on the "Manually Defined" option.
Tips :Do not click on the option for "All IP Addresses behind Gateway based on Topology information" as partners could only access the servers on the Service Network via private IP. This

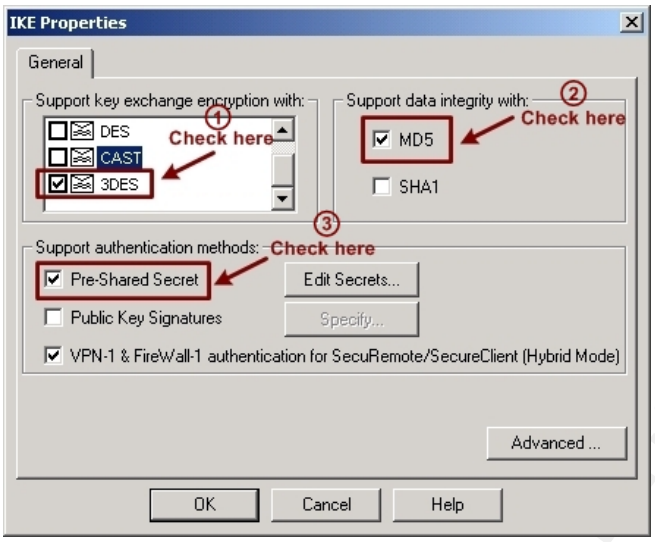
would not worked as private IP addresses are not routable through the Internet and we have filtered private IP addresses at our border router access control list.
To avoid this, we need to choose the “Manually Defined” option to ensure that internal servers are accessible by partners via Public IP. Please take note that whatever objects we set for “Manually Defined” option will fall within the VPN domain. Any objects that are defined can be accessible in a gateway-to-gateway VPN session or a client-to-gateway VPN session and this can be control at the firewall rule base.
For our case, we had selected the Mail-Relay, GIAC SSH server, Private web server and sales administrator desktop as the objects for the VPN domain and we have grouped it as “GIAC-VPN”.

2. The next step is to configure GIAC-Firewall (VPN gateway) to use IKE Encryption

   a. At the left pane, select the VPN option. Check on the IKE option as the Encryption Schemes.
   Tips : IKE is preferred as it is the industry standard protocol for VPN key management while FWZ is Check Point proprietary encryption scheme.



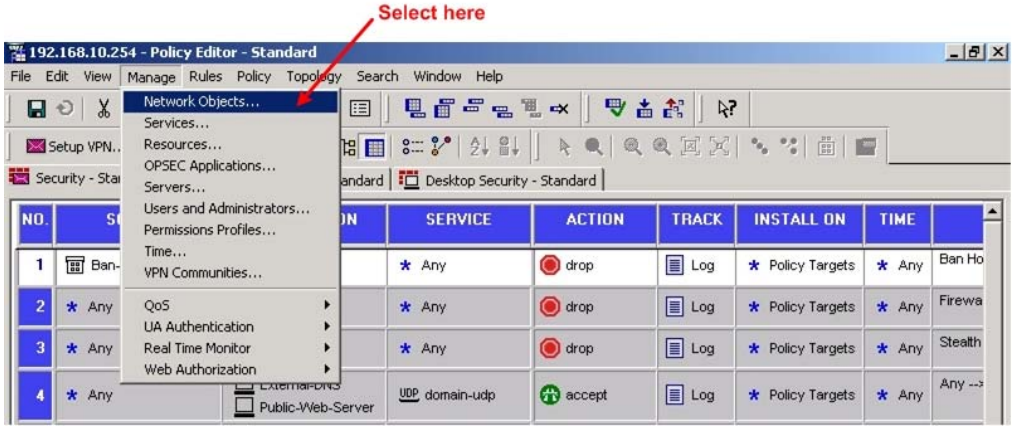
   b. Edit the IKE Properties settings by clicking on the Edit button. The IKE Properties screen shall be displayed as below.



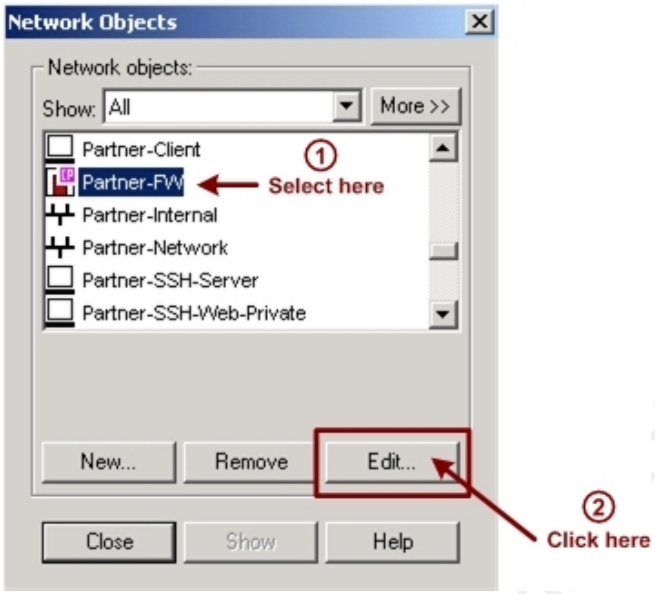
c. Make sure that 3DES option is checked as the key exchange encryption and MD5 is checked for data integrity. As for the "Support authentication methods" section, check on the Pre-Shared Secret option
Tips : Please take note that the options that we set above must follow the settings that we had agreed with our partners

3. The third step is to configure the Encryption Domain for our Partners' gateway.

a. From the Policy Editor, click on the Manage menu and select the Network Objects option from the list.

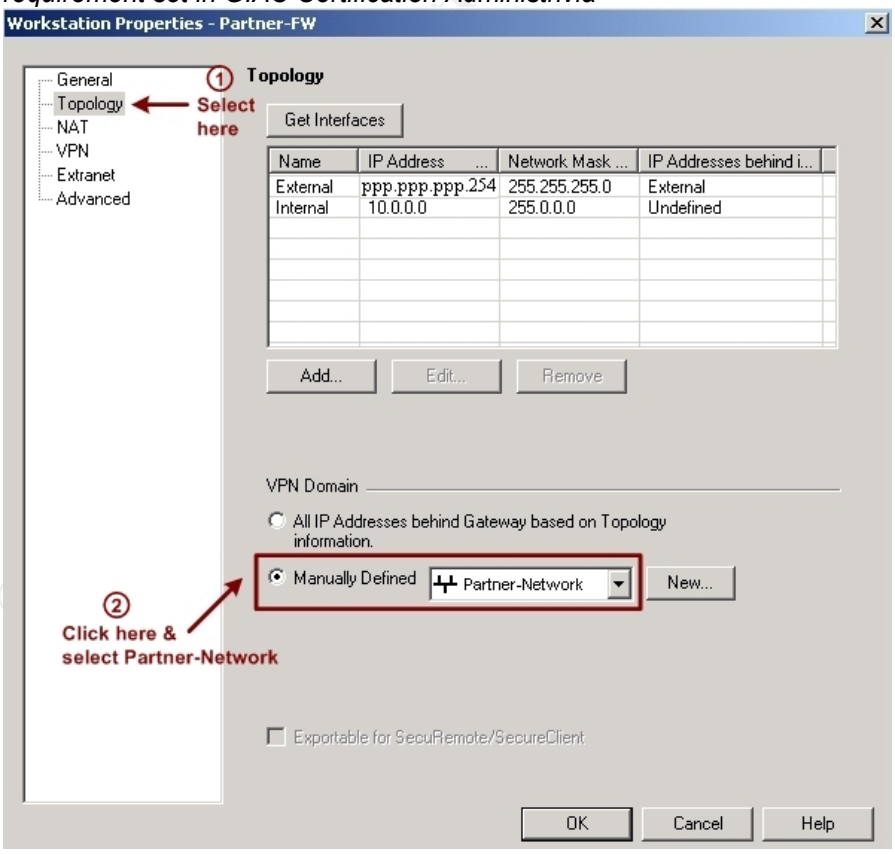


b. The Nework Objects screen will appear as below. Select Partner-FW and click on the Edit button



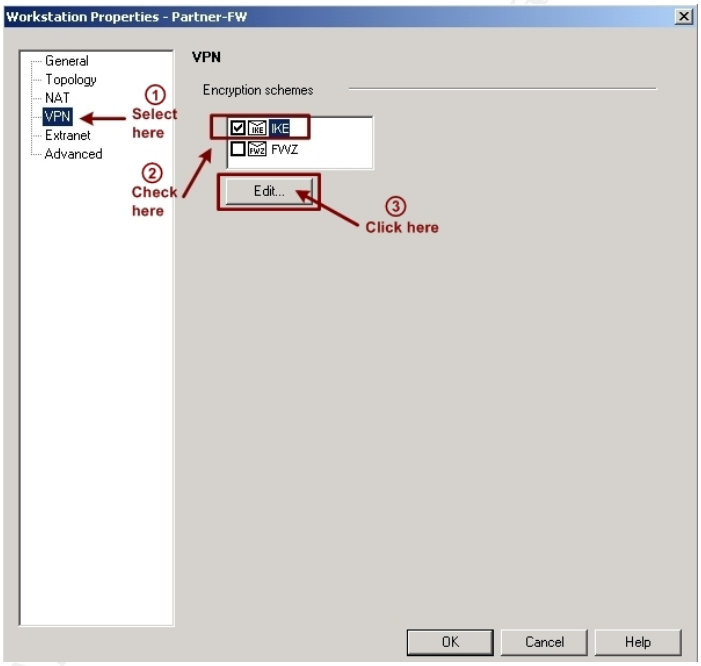
c. The Partner-FW workstation properties will be displayed as below. At the left pane, select the topology option.

The external network IP address for this snapshot has been sanitized to fulfill the requirement set in GIAC Certification Administrivia

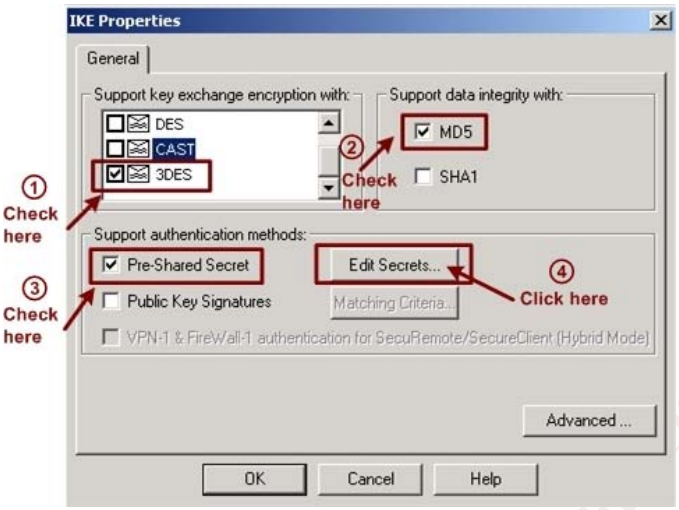


d. At the VPN Domain section, make sure that you click on the "Manually Defined" option
Tips : Do not click on the option for "All IP Addresses behind Gateway based on Topology information", as servers at partners' network can only be accessible via its Private IP. This would not work as private IP are not routable through the Internet and we have filtered private IP addresses at our border router access control list.
To avoid this, we need to choose the "Manually Defined" option to ensure that partners' servers or network are contactable via Public IP. For our case, we had selected the partner network as the object for the VPN domain.

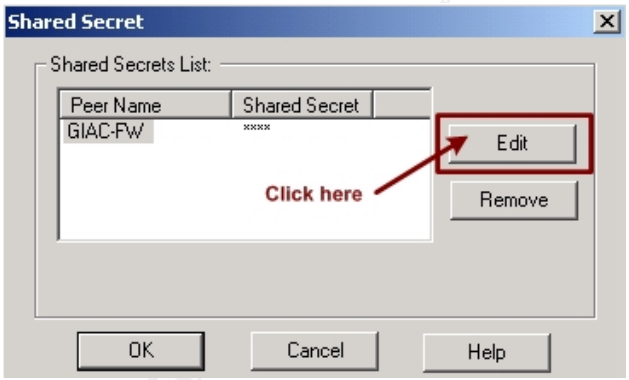
4. The fourth step is to configure Partner-FW (VPN gateway) to use IKE encryption.
   a. At the left pane, select the VPN option. Check on the IKE option as the Encryption Schemes.



   b. Edit the IKE Properties settings by clicking the Edit button. The IKE Properties screen shall be displayed as below.



c. Select 3DES as the key exchange encryption and MD5 for data integrity.
d. The next step is to check on the Pre-Shared secret and click on the Edit Secrets button



e. The shared secret screen shall appear as above. Click on the Edit button. Key in the shared secret password and confirm your password by clicking the Set button.

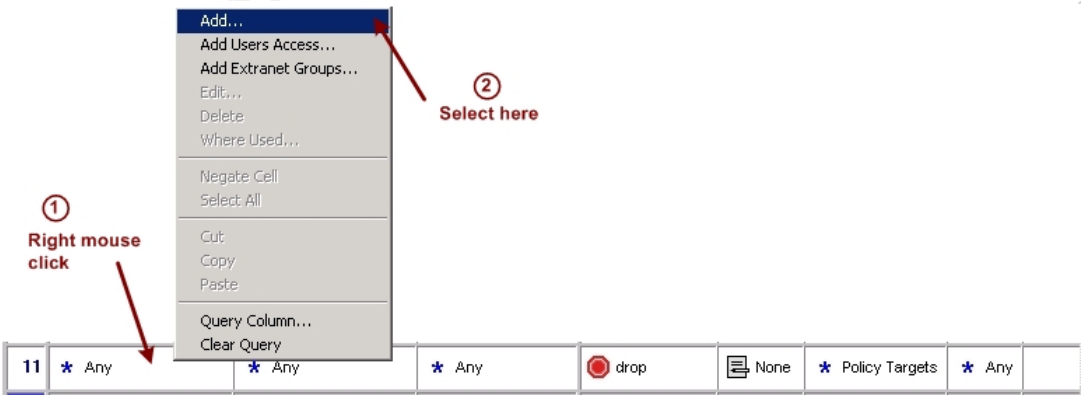
5. The fifth step is to create a gateway-to-gateway IKE VPN rule with the following requirements : -

Rule #	Source	Destination	Service	Action	Track	Install On
11	Partner-Network	Private-Web-Server GIAC-SSH-Server Mail Relay	http, https, ssh and smtp	Encrypt	Log	Policy Target
12	Sales-Admin	Partner-SSH-Server	ssh	Encrypt	Log	Policy Target

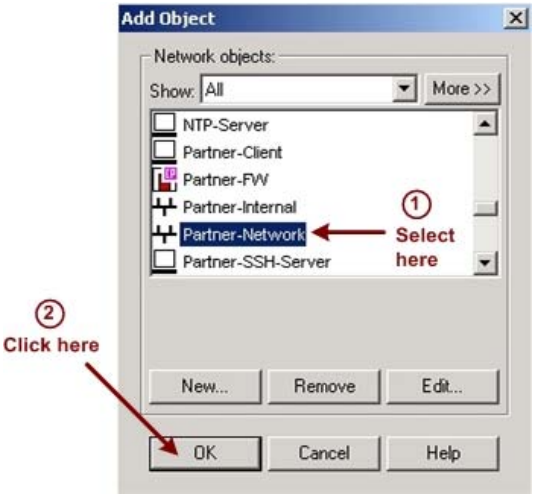
Ways to add rule

a. To create rule #11, highlight on rule #10. Then click on the Rules menu and Add Rule with option to place rule #11 below rule #10.

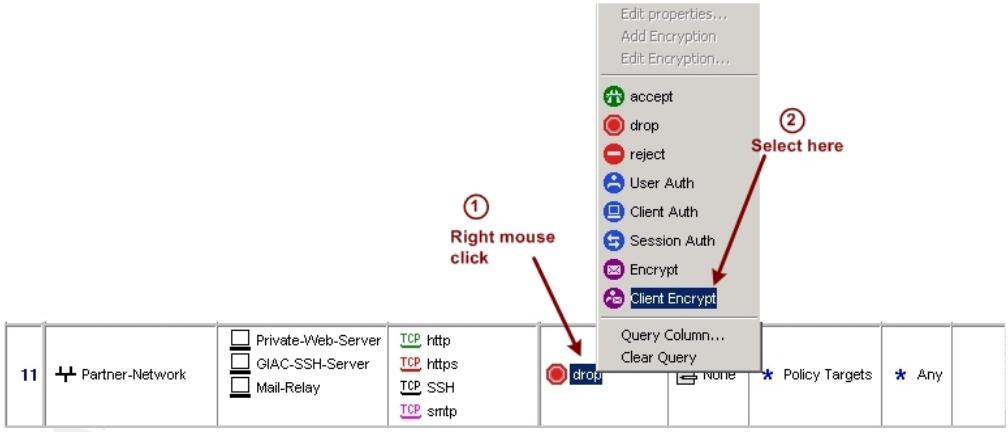
b. A new rule, rule #11 will be added to the rulebase.
c. Point at the Source column (1st column) and do a right mouse click and select the Add option.



d. The Add Object menu will appear as below. Select Partner Network as the source object and click the OK button.



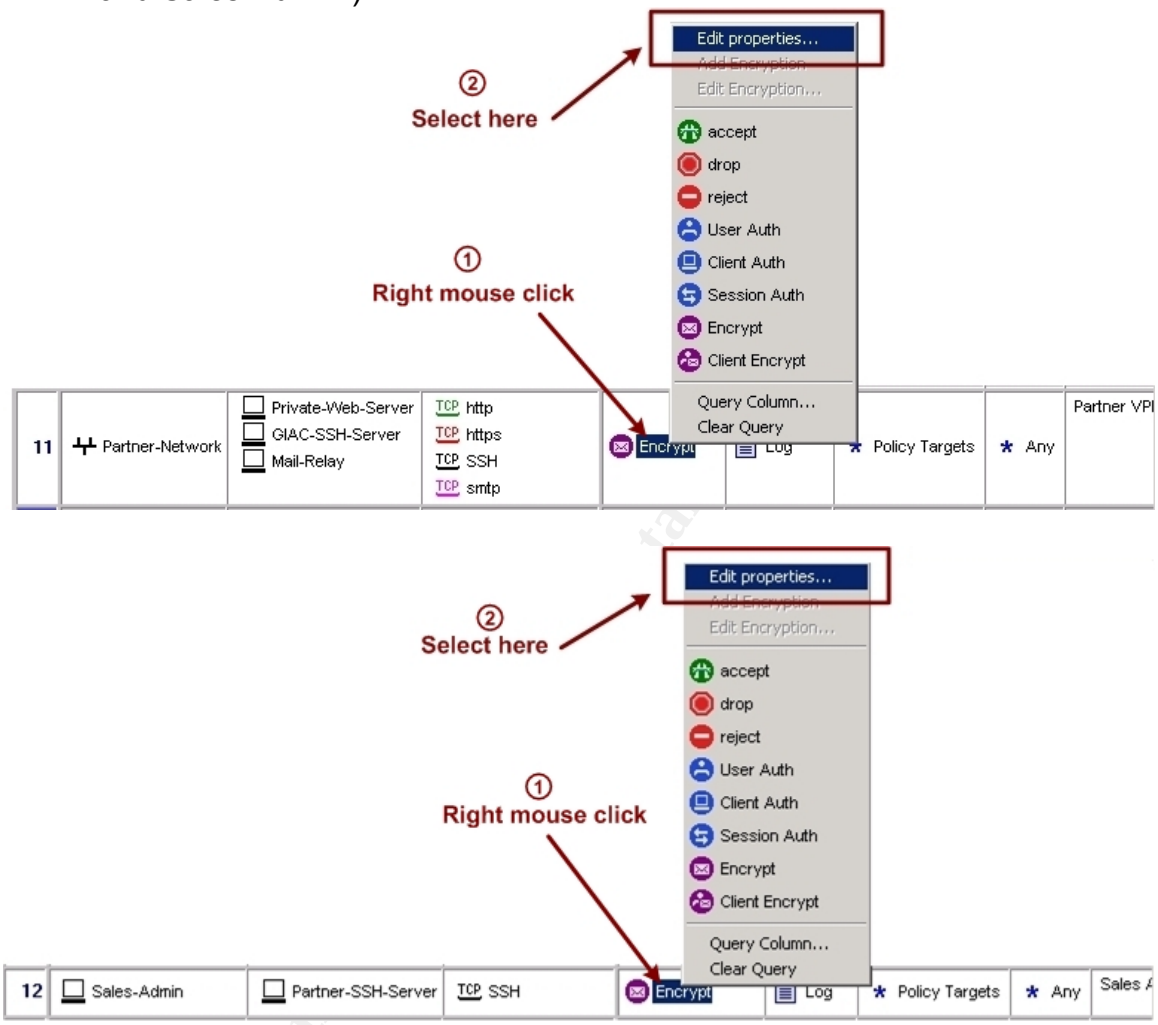
e. Repeat the similar steps like c and d for the Destination (2nd column), Service (3rd column), Action (4th column), Track (5th column) and Install On (6th column) with a right mouse click and select the appropriate action in accordance to the requirements listed above. Below is an example of the repeating procedure for Action column.
Tips : By default, a new rule is not set to log. Therefore, make sure that you choose to log it. By default the Install On (6th column) is set to Policy Target.



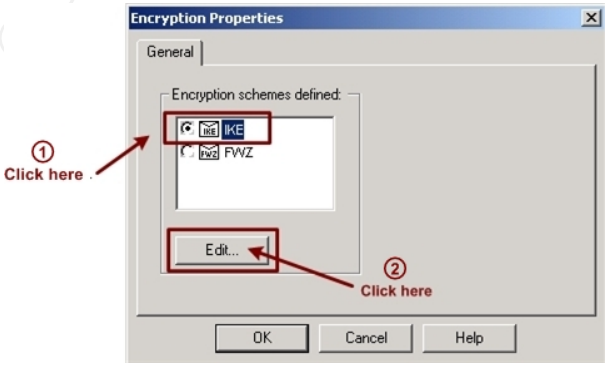
f. Repeat similar steps like a, b, c, d and e when adding Rule # 12
Tips : Please make sure that the correct objects are set for source and destination and select the right service and action for Rule #12.

Rule # 11 and # 12 are now added to the rule base.

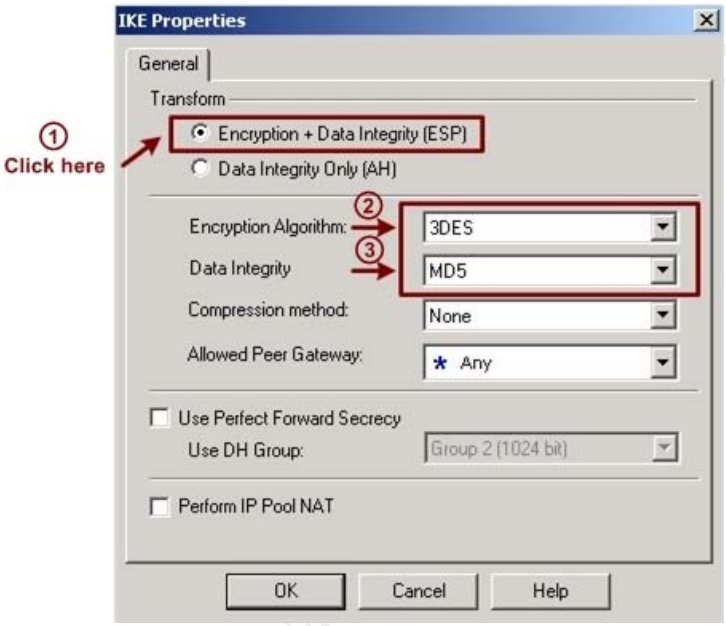
a. From the Action column, right mouse click button on the Encrypt icon and select the Edit properties option. (Do for both Partner-Network and Sales-Admin)



b. The Encryption Properties screen will appear as below. Click IKE as the Encryption schemes.
Tips : IKE is preferred as it is the industry standard for encryption scheme while FWZ is Check Point proprietary encryption method.



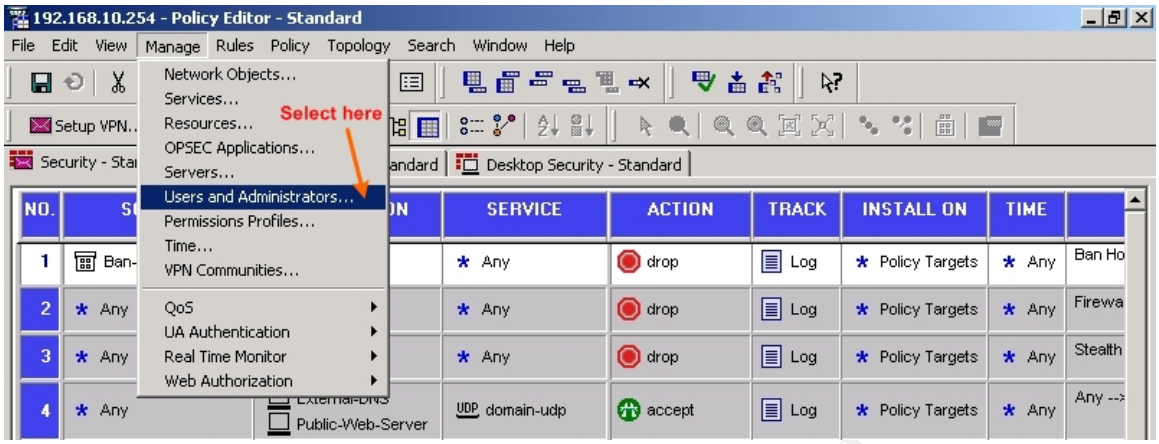
c. Click on the Edit button. The IKE Properties screen shall be displayed as below. Click on the option for Encryption + Data Integrity (ESP) and 3DES as the encryption algorithm and MD5 for the data integrity. This shall be applied to all allowed peer gateway
Tips : Do not select the option for "Data Integrity Only (AH)" as AH is incompatible and breaks with many NAT implementations. Select ESP as it can function with most NAT implementations.
(SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.4, pg 101-107)



Client–to-Gateway VPN
(using IKE Encryption Method)

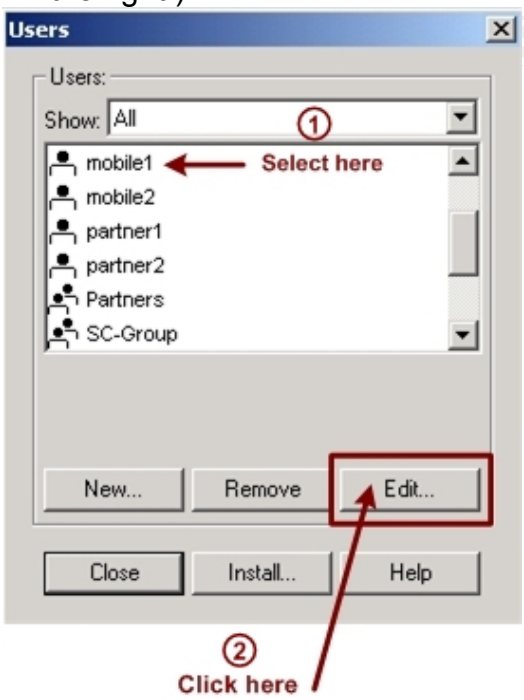
This section will explain ways to implement client-to-gateway VPN connection with suppliers and mobile employees. Similarly, all traffic between the remote VPN client and GIAC-FW (VPN Gateway) will be encrypted using IKE encryption scheme.

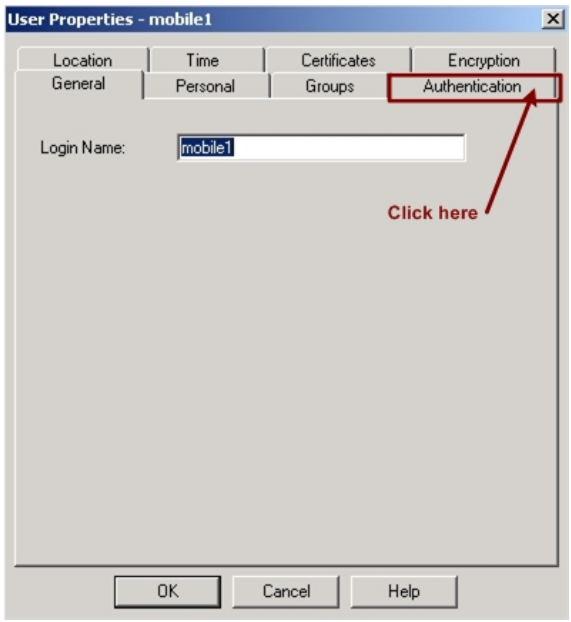
1. First, we need to configure the user properties.
   a. From the Policy Editor, click on the Manage menu and select the Users and Administrators option from the list.



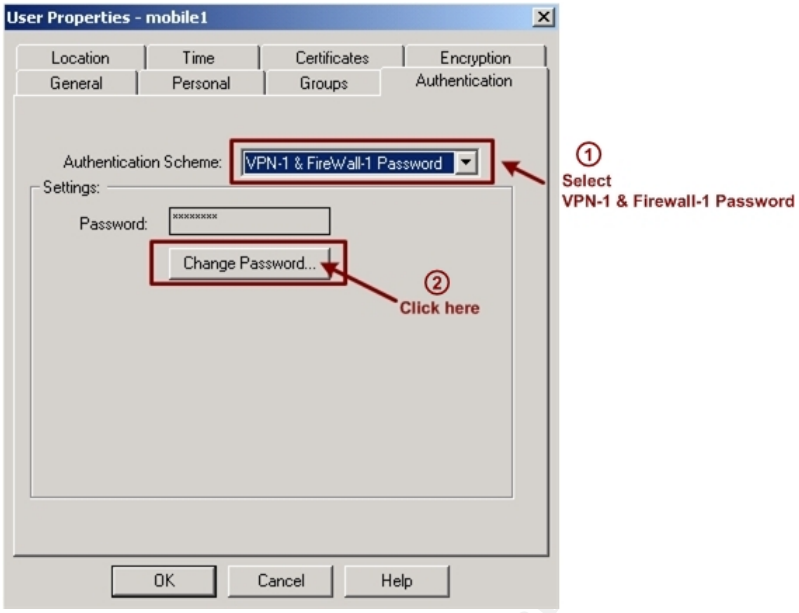
b. From the list of users, select mobile1 and click on the Edit button (as shown on the left).
Note : In our configuration, we have created mobile1 and mobile2 as mobile employees' account and supplier1 and supplier2 as our suppliers' account.

c. The User Properties for mobile1 shall appear as below (as shown on the right).



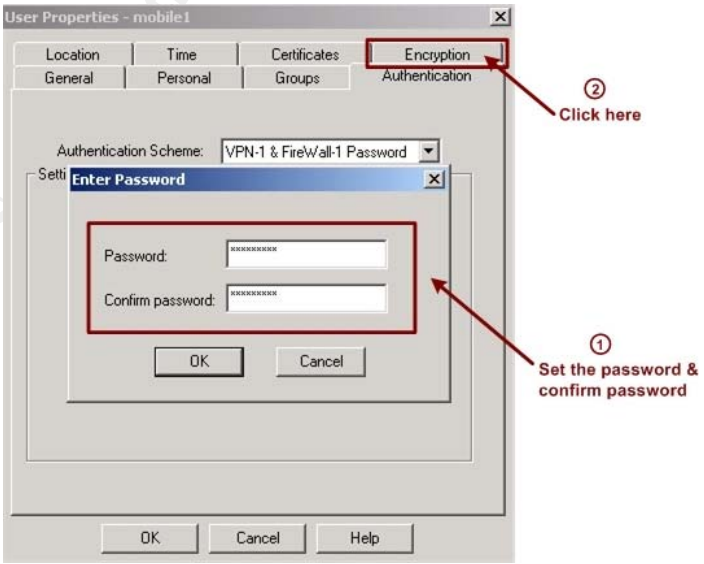


d. Click on the Authentication tab and make sure that the VPN-1 & Firewall-1 password is selected for user mobile1 as the authentication method.

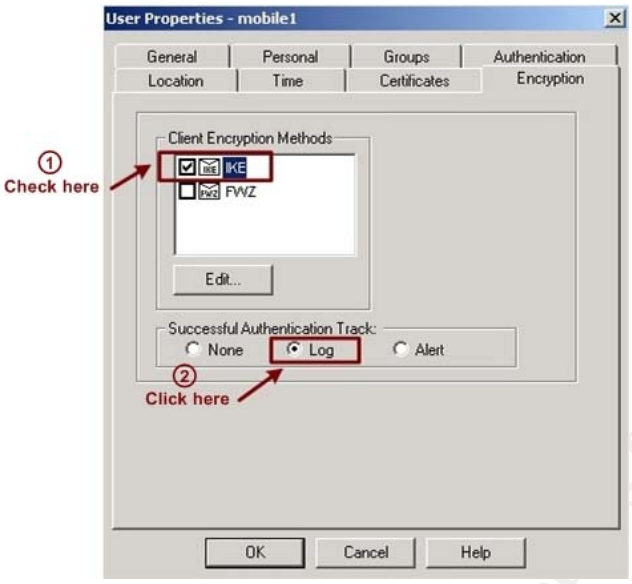


Though the VPN gateway can support several other stronger authentication schemes (such as SecureID, Radius, TACACS, AXENT Pathways Defender) but due to budget constraint we had to limit ourselves to use the VPN-1 & Firewall-1 Password.
Tips : The authentication scheme selected for remote VPN users must also be enabled at the Authentication tab of GIAC-FW Workstation Properties. The step to configure this will be discussed later (Configuring Policy Server section).

e. From the settings section, click on the change password button. Type in the new password and confirm the password. The next step is to click on the Encryption tab to configure the Encryption settings.

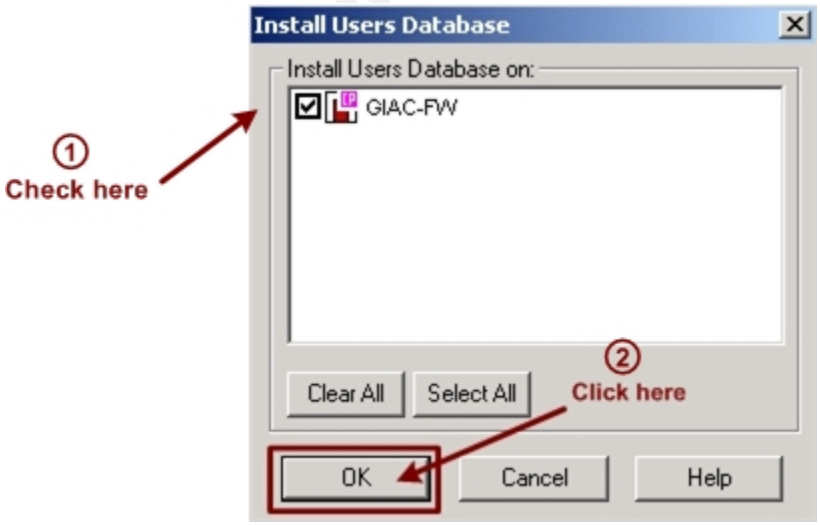


f. At the Client Encryption Methods section, check on the IKE option.

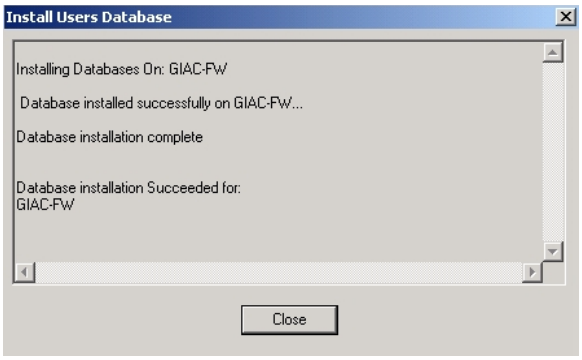


g. From the Successful Authentication Track, you should choose to log mobile1 user's activities at the firewall. This is for auditing purposes. **Tips** : We need to repeat step 1 for all suppliers and mobile employees accounts that we have created.

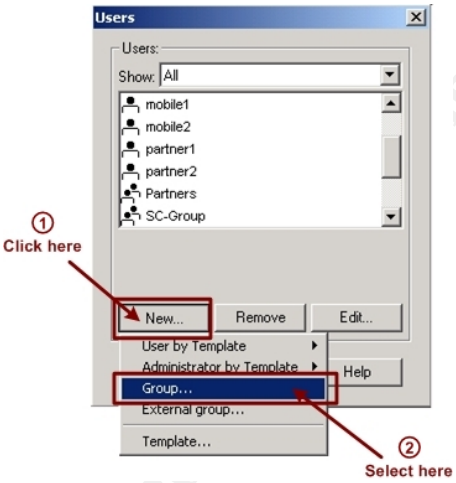
2. As soon as we have completed step 1, we need to activate the configuration that we had set for the users by doing a user database installation.

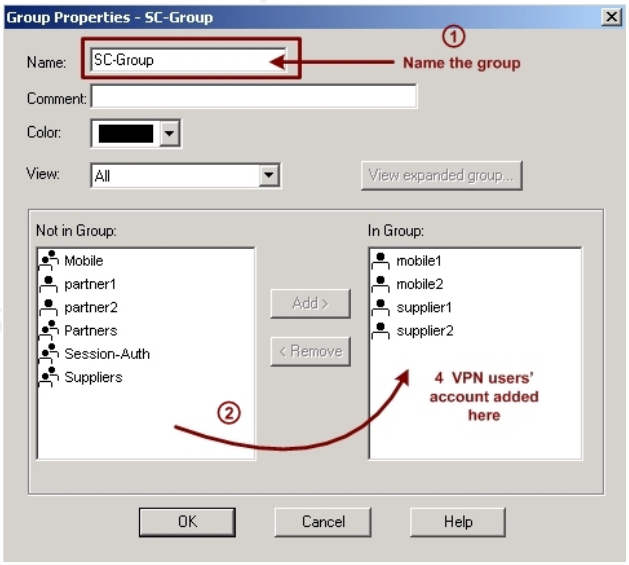


To install the user database, check on the GIAC-FW object and click on the OK button and you will prompted with a screen as shown below.



3. The next task is to create a group for these client-to-gateway VPN users. From the user screen, click on New then on Group.





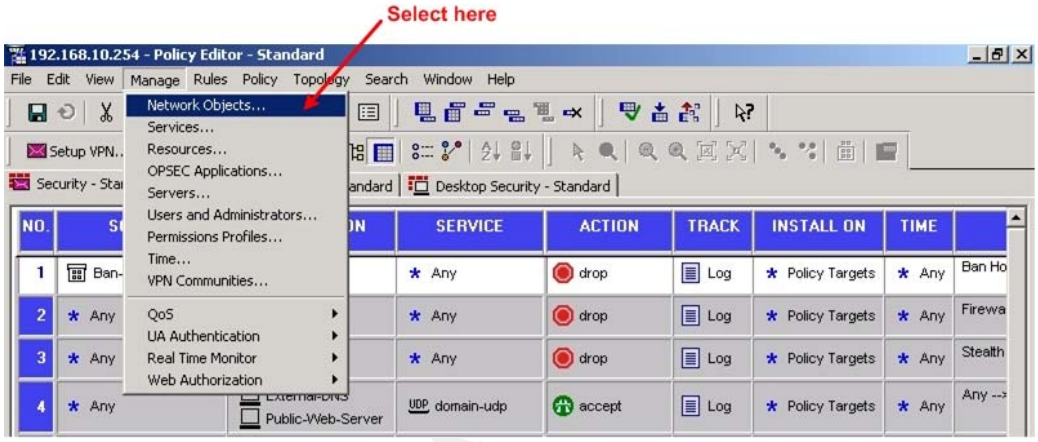
Provide a meaningful name for this group. In our setting, we called it as SC-Group and we had added mobile1, mobile2, supplier1 and supplier2 accounts into this group.

Configuring the Policy Server

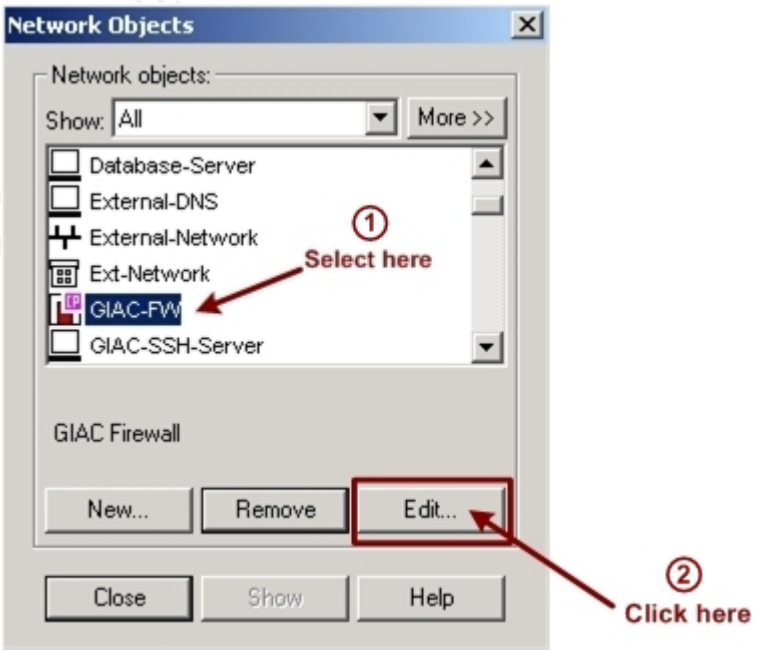
This section will explain ways to configure the GIAC-FW as the Policy Server. The Policy Server contains security policy that will be uploaded into the remote VPN client's desktop whenever they are successfully connected to GIAC's network.

1. First we need to configure the workstation properties of the GIAC-FW.

   a. From the Policy Editor, click on the Manage menu and select the Network Objects option from the list.

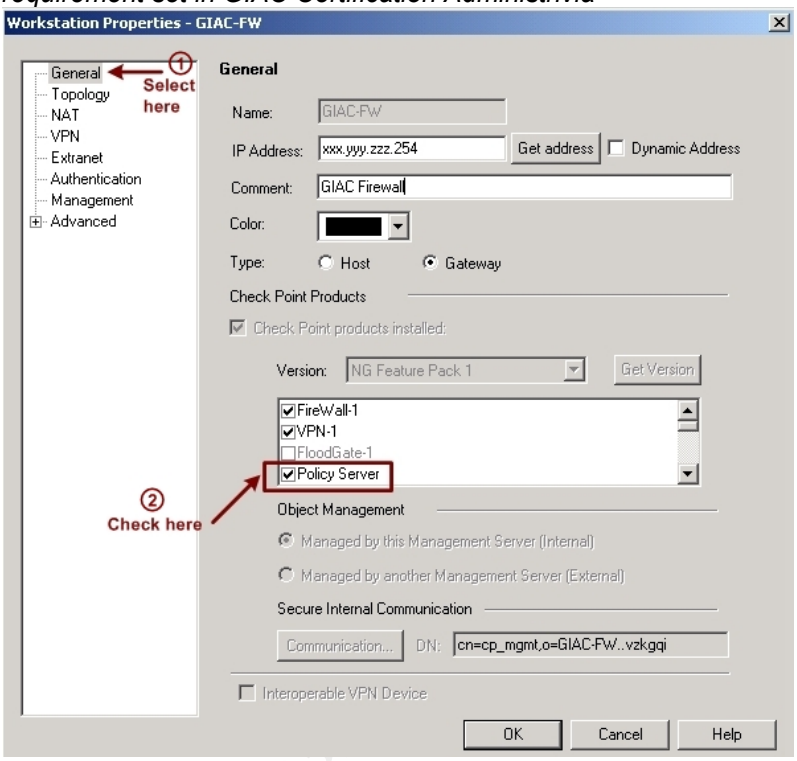


   b. The Network Objects screen will appear as below. Select GIAC-FW and click on the Edit button.



c. The GIAC-FW workstation properties will be displayed as below. At the left pane, select the General option.

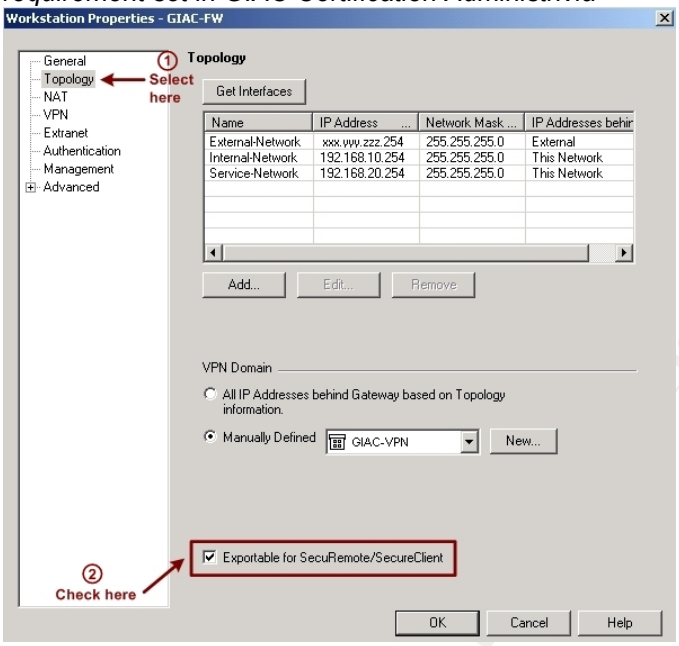
The external network IP address for this snapshot has been sanitized to fulfill the requirement set in GIAC Certification Administrivia



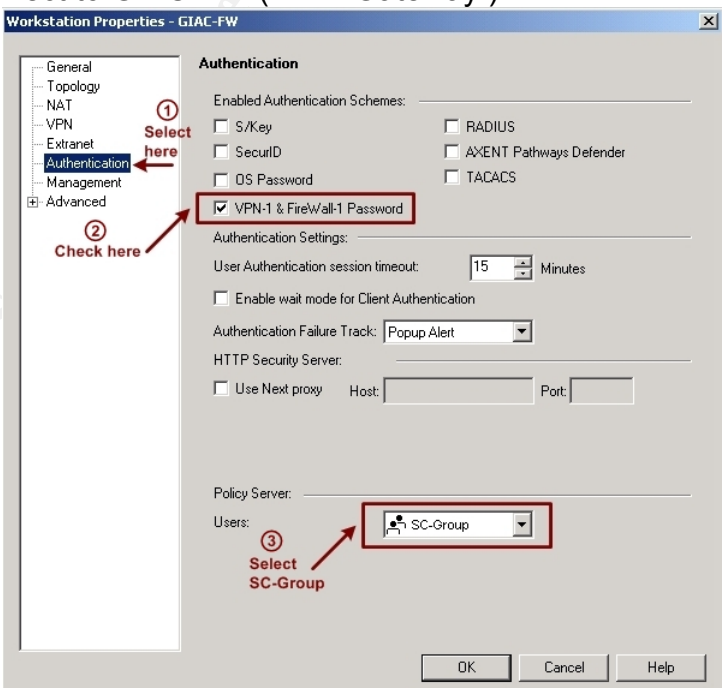
d. Make verification that the Policy Server option is checked

e. The next step is to select the Topology option from the left pane and make sure that the option for “Exportable for SecureRemote” is checked.
Tips : By checking this option, the Policy server’s encryption domain topology is available to all remote VPN clients. The remote client’s desktop can then download the desktop security policy set by GIAC’s administrator.

The external network IP address for this snapshot has been sanitized to fulfill the requirement set in GIAC Certification Administrivia

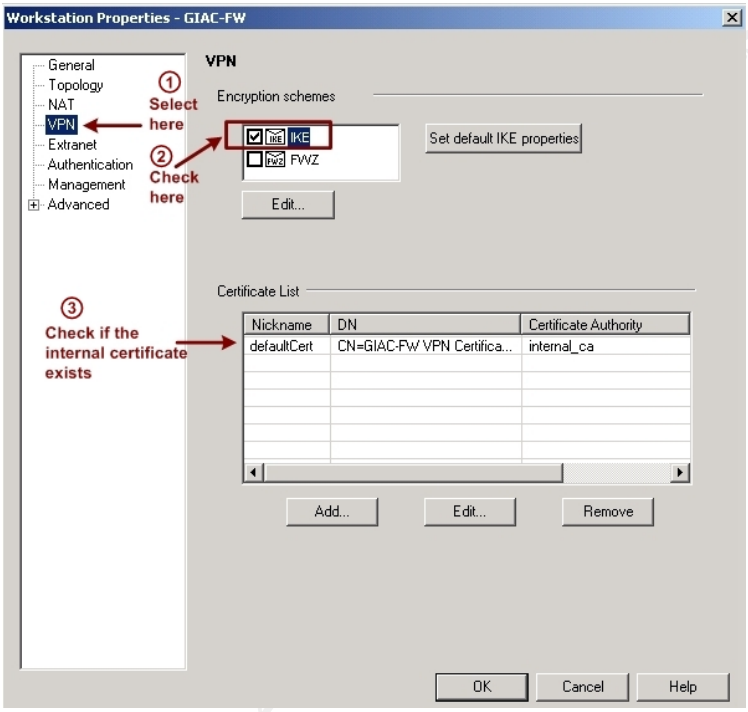


f. From the left pane, select the Authentication option. We need to verify that the VPN-1 & Firewall-1 Password option is checked for the Enabled Authentication scheme section.
Tips : This is very important as all remote VPN clients authentication scheme are set with VPN-1 & Firewall-1 Password. If the user authentication scheme define in the user account is RADIUS, then you should check the RADIUS option or else the user would not be able to connect to GIAC-FW (VPN Gateway).



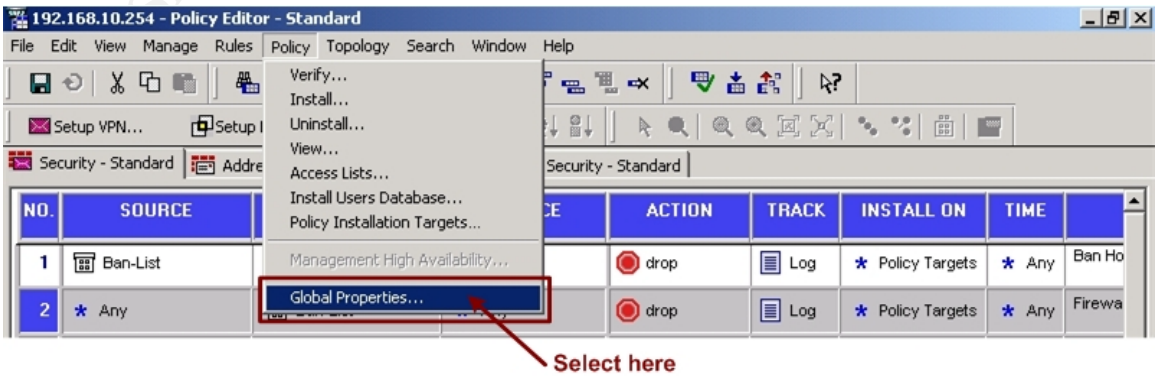
g. At the Policy Server section, click on the Users drop-down menu and select the group (SC-Group) that we have created earlier.
Tips : If we missed this step, the remote VPN client would not be able to make contact with the Policy Server.

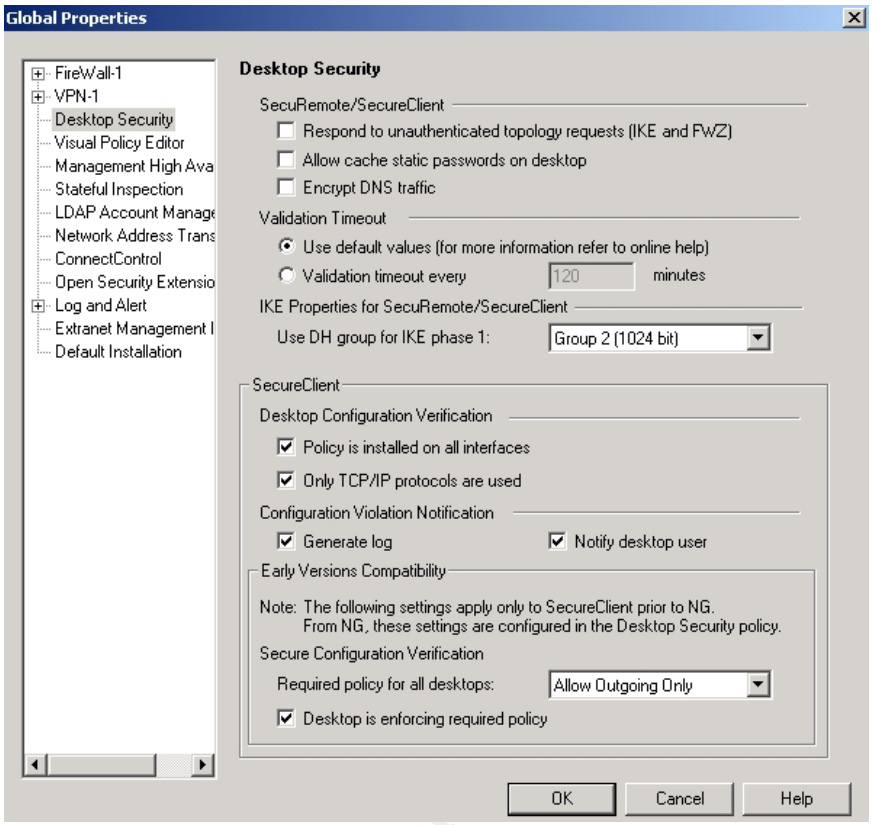
h. After defining the users group, we need to make some verification on the VPN configuration. At the left pane, select the VPN option.



i. Please make sure that the Encryption scheme selected is IKE (as we have defined IKE as the encryption method for all remote users) and the Internal Certificate does exists in the Certificate List section.

2. The second step is to check the settings in Desktop Security Properties.
   a. From the Policy Editor, click on the Policy menu and select the Global Properties option from the list.





b. At the left pane, select the Desktop Security option. Make sure that the settings for Desktop Security properties appear as above.

   (Explanations below were excerpted from CheckPoint VPN-1/Firewall-1 NG Help file for Global Properties window – Desktop Security)
   The "use default values" is for validation timeout allow IKE passwords to expire in 4 hours.
   The "Policy is installed on all interfaces" enable the Policy Server to check that the desktop policy is present on all physical interfaces of every desktops.
   The "Allow Outgoing Only" means to allow only SecureClient to initiate the connections.

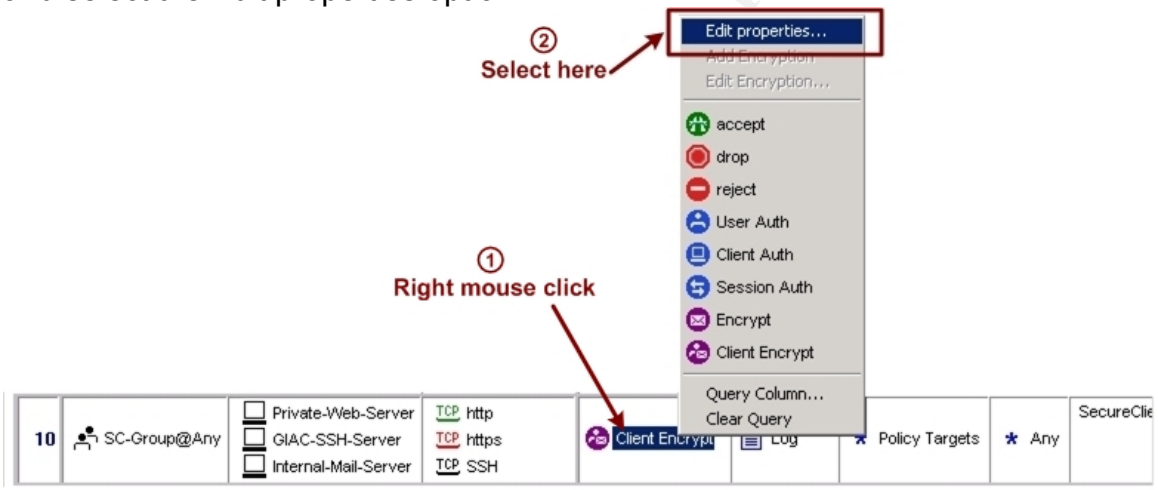
   Tips : Please take note that under the SecureClient section, make sure that the remote VPN clients' PCs or notebooks are not loaded with non-TCP/IP protocol. If yes, then you may need to uncheck the "Only TCP/IP protocol are used" option or else the client would face some connectivity problems. For our case, our remote VPN clients desktops are loaded only with TCP/IP protocol.

3. The third step is to create a client-to-gateway IKE VPN rule with the following requirements :-

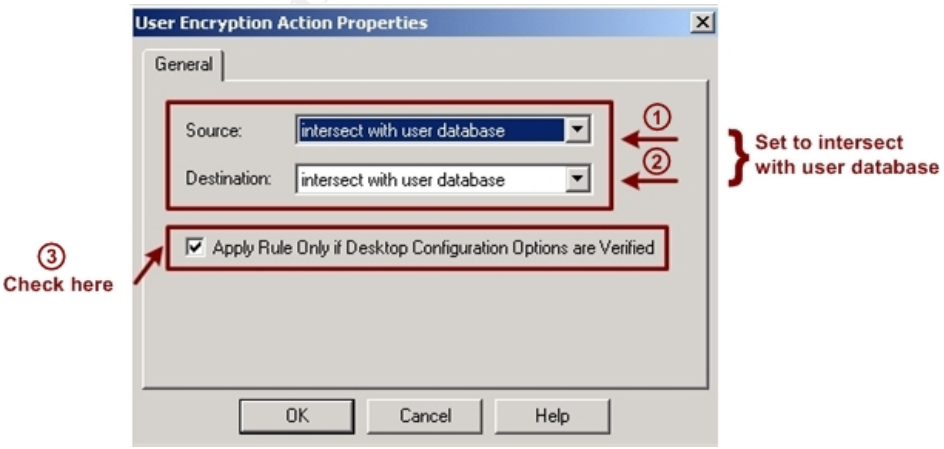
Rule #	Source	Destination	Service	Action	Track	Install On
10	SC-Group@Any	Private-Web-Server GIAC-SSH-Server Mail Relay	http, https and ssh	Client Encrypt	Log	Policy Target

Please refer to page 57 – 58 for guides to add rule.

From the Action column, right mouse click button on the Client Encrypt icon and select the Edit properties option.



The User Encryption Action screen will appear as below.



Make sure that you choose to set “intersect with user database” for the source and destination.

(Explanation below was excerpted from CheckPoint VPN-1/Firewall-1 NG Help file for User Encryption Action Properties)
This is to apply the intersection of the access privileges specified in the rule set above and in the user properties window.

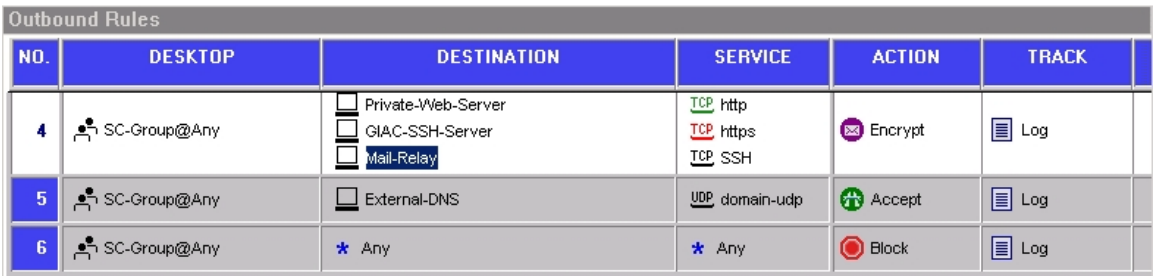
Verify that the “Apply Rule Only if Desktop Configuration Options are Verified” option is checked.
Tips : This is important as we want to enforce all security rule base loaded on the remote VPN client’s personal firewall.

4. The fourth step is to create the VPN desktop rule for remote client’s desktop firewall.

    a. From the Policy Editor, click on the Desktop Security tab.

    b. We need to create some outbound rules with the following requirements :-

Rule #	Desktop	Destination	Service	Action	Track
4	SC-Group@Any	Private-Web-Server GIAC-SSH-Server Mail Relay	http, https and ssh	Encrypt	Log
5	SC-Group@Any	External DNS	domain-udp	Accept	Log
6	SC-Group@Any	Any	Any	Block	Log



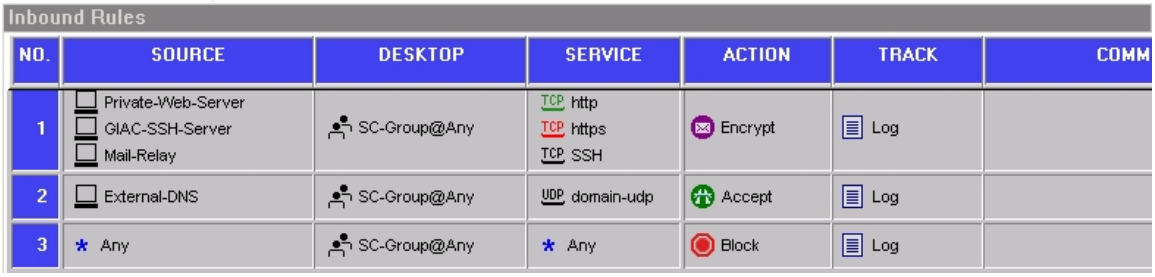
Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK
4	SC-Group@Any	Private-Web-Server GIAC-SSH-Server Mail-Relay	TCP http TCP https TCP SSH	Encrypt	Log
5	SC-Group@Any	External-DNS	UDP domain-udp	Accept	Log
6	SC-Group@Any	* Any	* Any	Block	Log

Rule #4 ensure that the remote VPN client are allow to access the private web server, GIAC SSH server and the Mail Relay with a client-to-gateway VPN tunnel.
Rule #5 specifies that the remote client can access the External DNS but without having to encrypt the domain-udp traffic.
Rule #6 is the restrict rule that disallow the remote VPN client to access other destinations that are not define within the local encryption domain. This is for security purposes.

c. We need to create some inbound rules with the following requirements :-

Rule #	Source	Destination	Service	Action	Track
1	Private-Web-Server GIAC-SSH-Server Mail Relay	SC-Group@Any	http, https and ssh	Encrypt	Log
2	External DNS	SC-Group@Any	domain-udp	Accept	Log
3	Any	SC-Group@Any	Any	Block	Log



Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMM
1	Private-Web-Server GIAC-SSH-Server Mail-Relay	SC-Group@Any	TCP http TCP https TCP SSH	Encrypt	Log	
2	External-DNS	SC-Group@Any	UDP domain-udp	Accept	Log	
3	* Any	SC-Group@Any	* Any	Block	Log	

Rule #1 allow that the remote client to receive responses from the private web server, GIAC SSH server and the Mail Relay via the client-to-gateway VPN tunnel
Rule #2 allow the remote client to receive responses from the External DNS without having to encrypt the domain-udp traffic.
Rule #3 is the protection rule for the remote VPN client. This prevent hackers or crackers from connecting to remote VPN client's desktop.

Assignment 3 : Verify the Firewall Policy

Implementing security policy on the firewall is not the only task that we should do in order to secure our network. We need to audit or make verification on the security rules that we have set. Human are prone to errors. Therefore it is essential for us to do the extra mile in making sure that the security rules in our firewall are correctly specified. Foremost, it must meet the business needs and access requirements defined in Assignment 1 and 2.

Plan the audit

Technical approach

Our main goal is to verify the firewall policy. We are NOT ask to perform a vulnerability assessment or to audit other network devices. The focus in this audit process is to ensure that the primary firewall is implementing GIAC Enterprises' security policy.

We will apply the audit procedures suggested by Lance Spitzner in his white paper "Auditing Your Firewall Setup". This white paper is available at http://www.spitzner.net/audit.html.

For The Rule base

We will be performing several port scans with several laptops equipped with a port scanning tool (NmapWin v1.3.1). These laptops are the audit systems. The scanning will be carried out from one network to every other network. This helps us to be certain if the firewall is only accepting traffic that is allow in the rule base.

First, we will place the audit systems at the External Network (Internet) and initiate several ports scans to all servers that reside on the Service Network. The port scan will also include scanning the firewall external interface.

Performing port scan from the External Network alone is not adequate for a comprehensive rule base audit. We need to simulate scenario if one of our servers on the Service Network is compromised. Therefore, it will be a good idea to substitute the servers on the Service Network with the audit systems. When we substitute the servers with the audit systems, we need to plan for a right time to turn off the server and configure the internal IP of the server on the audit system. Thereafter, we can start to do our port scan from the audit systems to the targeted servers on the Internal Network.

We should also do the same audit test on the Internal Network. Please remember that we need to schedule an appropriate downtime before we could offline the server and switch the internal IP of the server to the audit system. By positioning the audit systems on the Internal Network, we could perform several port scans to the servers located on the Service Network.

For Authentication/Encryption Rule base

In our rule base, we have defined several VPN rules for connection with our partners, suppliers and mobile employees. To test the VPN rules, we will apply a different approach. We need to ensure that the remote client can only gain access when they are authenticated.

Firstly, we need to determine what happen if the remote client (suppliers and mobile employees) failed to login to GIAC VPN gateway? Are they able to join the VPN domain and gain access to the servers?

Secondly, we need to verify if the data transmitted between GIAC and the remote VPN clients and partners are encrypted over the wire. We can test this out by placing a packet sniffer tool eg. Ethereal on the wire and at the same time we can monitor the log at the firewall.

Consideration

The assessment should be carried out on a Sunday morning 00:01 AM. We had estimated that the assessment might take 20 hours to complete. The network connection will resume 1 hour after the assessment had stopped. This is because we need some time to relocate and turn on some of servers that we had taken offline and make a few systems and network check for further confirmation. The whole audit exercise will complete by 21:00 PM and we hope our connection will resume by 21:01 PM.

Prior to that we need to make an early announcement to our customers, suppliers, partners, mobile employees and internal employees that our network will be inaccessible on this particular timeframe. The announcement can be made via email or through our website. We should also inform our ISP with a formal letter that we would be conducting a thorough audit on our firewall rule base. We have selectively invited one of our partners to participate in our audit. This partner of ours was friendly enough to agree with the time schedule and had arranged the necessary facilities to perform the audit with us.

We should present our audit plan to our President, the network and system administrators and our friendly partner. Everyone should be aware of how the audit plan would work and agreeable with the plan. The audit plan should consist of steps to perform the audit, expected results and a contingency plan for disaster recovery. A formal approval from the President and our partner is a MUST before we could proceed doing it.

The system and network administrators will carry out the audit with close supervision by the IT Manager. The administrators had mutually agreed to use NmapWin v1.3.1 and Ethereal as the audit tools. These tools are free and downloadable from the Internet.

Estimated costs

Level Effort	Hours	
Planning	5 hours	None
System Backup	8 hours	$266
Tools		None
Port Scan	20 hours	$1600
System and Network Check	1 hour	$80
Vendor standby service		$260
Collecting reports and logs	3 hours	None
Report writing and recommendation	6 hours	None
Total		$2206

There are no costs incurred for planning, collections of reports and logs and report writing, as the administrators will be doing it during office hour. Cost will only incurred for system backup, port scan activities, system and network check, as we need to buy backup facilities and to pay allowances to all staffs who worked on non-business hour. We also need to pay our vendor for their standby service.

Risks and Consideration

There are risks that we need to consider before we could proceed with the audit plan. The risks include lost of system and valuable business data. To mitigate these risks, we need to perform system and data backup before the audit.
We may need to spend approximately 8 hours to restore all system and data files. Therefore, the latest time for the network and systems to resume may fall on Monday morning 05:00AM.
All vendors are notified about the audit and they had agreed to be on standby.
The other risk that we might face is the risk of being attack during the audit. We had advised our team members about the possibility and we shall make a close monitoring on any alerts or messages trigger by the Intrusion Detection System.

Conduct the audit

For The Rulebase :-

There are several type of port scan available in NmapWin tool. We are not able to initiate all type of scans as we have time limitation and each scan does take a while to complete. We have quite a number of servers and there are 65535 number of ports to scan for each type of scan. Thus, we had to limit ourselves to use the :-

- Connect Scan
  Is use to open a connection to every listening port on the servers. If the port is listening, then the connect scan will succeed else the port will be unreachable.
- Syn Stealth Scan
  Is a "half-open" scan as it does not open a full TCP connection. The SYN Stealth scan will send a SYN packet and wait for a reply. A SYN|ACK reply tells that the port is listening while a RST indicates that the port is not listening.
- ACK Scan
  Is use to map out the firewall rule base. The ACK scan can help to determine if the firewall is stateful. If a RST is received, the ports is considered as "unfiltered". If an ICMP unreachable messages is returned or no reply is received, the port shall be considered as "filtered"
- UDP Scan
  The UDP scan will send 0 byte udp packets to each port on a target system. If an ICMP port unreachable reply is received, the port will be considered close else the port is consider open.
  (Descriptions above were written with references obtained from NmapWin Help file - nmapwin.chm at scan folder page)

Assessment from the External Network

First we need to set the IP and gateway address on the audit system. We will use xxx.yyy.zzz.222 as the IP address with netmask of 255.255.255.0 and default gateway IP to xxx.yyy.zzz.253 (border router external interface IP).

The targeted servers for this round of port scan are :-

xxx.yyy.zzz.254	firewall external interface IP
xxx.yyy.zzz.1	External DNS
xxx.yyy.zzz.2	Mail Relay
xxx.yyy.zzz.3	Public Web Server
xxx.yyy.zzz.4	Private Web Server
xxx.yyy.zzz.5	GIAC SSH Server

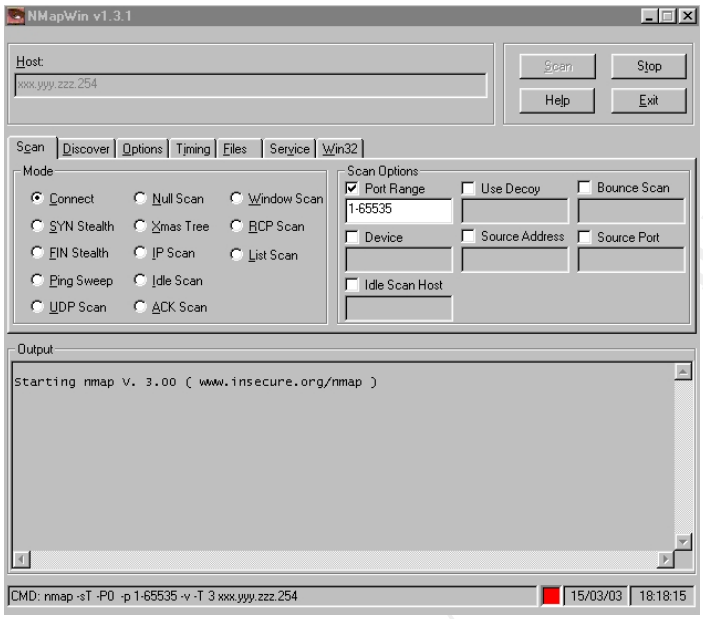
- We will perform ping test on every IP listed above.
  Ping xxx.yyy.zzz.000

(References obtained from NmapWin Help file - nmapwin.chm at nmap manual page)

- For all the commands below :
  -sT is for Connect Scan
  -sS is for SYN Stealth Scan
  -sA is for ACK Scan
  -sU is for UDP Scan
  -P0 is to turn off ping

-p 1-65535 range of port scan
-v for verbose output
-T 3 for Normal Throttle

- Connect Scan command :-
  nmap –sT –P0 –p 1-65535 –v –T 3 xxx.yyy.zzz.000



- Syn Stealth Scan command :-
  nmap –sS –P0 –p 1-65535 –v –T 3 xxx.yyy.zzz.000

- ACK Scan command :-
  nmap –sA –P0 –p 1-65535 –v –T 3 xxx.yyy.zzz.000

- UDP Scan command :-
  nmap –sU –P0 –p 1-65535 –v –T 3 xxx.yyy.zzz.000

Assessment from the Service Network

The targeted servers for this round of port scan are :-

192.168.10.254	Firewall Internal Network Interface
192.168.10.1	Internal DNS Server
192.168.10.2	Internal Mail Server
192.168.10.3	Backup Database Server
192.168.10.4	Syslog Server

- Connect Scan command :-
  nmap –sT –P0 –p 1-65535 –v –T 3 192.168.10.xxx

- Syn Stealth Scan command :-

nmap –sS –P0 –p 1-65535 –v –T 3 192.168.10.xxx

- ACK Scan command :-
  nmap –sA –P0 –p 1-65535 –v –T 3 192.168.10.xxx

- UDP Scan command :-
  nmap –sU –P0 –p 1-65535 –v –T 3 192.168.10.xxx

To substitute External DNS

Set the settings below on the audit system.
IP Address : 192.168.20.1
Netmask : 255.255.255.0
Gateway : 192.168.20.254

To substitute Mail Relay

Set the settings below on the audit system.
IP Address : 192.168.20.2
Netmask : 255.255.255.0
Gateway : 192.168.20.254

To substitute Public Web Server

Set the settings below on the audit system.
IP Address : 192.168.20.3
Netmask : 255.255.255.0
Gateway : 192.168.20.254

To substitute Private Web Server

Set the settings below on the audit system.
IP Address : 192.168.20.4
Netmask : 255.255.255.0
Gateway : 192.168.20.254

To substitute Database Server

Set the settings below on the audit system.
IP Address : 192.168.20.5
Netmask : 255.255.255.0
Gateway : 192.168.20.254

To substitute GIAC SSH Server

Set the settings below on the audit system.

IP Address : 192.168.20.6
Netmask : 255.255.255.0
Gateway : 192.168.20.254

To substitute NTP Server

Set the settings below on the audit system.
IP Address : 192.168.20.7
Netmask : 255.255.255.0
Gateway : 192.168.20.254

Assessment from the Internal Network

The targeted servers for this round of port scan are :-

192.168.20.254	Firewall Service Network Interface
192.168.20.1	External DNS
192.168.20.2	Mail Relay
192.168.20.3	Public Web Server
192.168.20.4	Private Web Server
192.168.20.5	Database Server
192.168.20.6	GIAC SSH Server
192.168.20.7	NTP Server

- Connect Scan command :-
  nmap –sT –P0 –p 1-65535 –v –T 3 192.168.20.xxx

- Syn Stealth Scan command :-
  nmap –sS –P0 –p 1-65535 –v –T 3 192.168.20.xxx

- ACK Scan command :-
  nmap –sA –P0 –p 1-65535 –v –T 3 192.168.20.xxx

- UDP Scan command :-
  nmap –sU –P0 –p 1-65535 –v –T 3 192.168.20.xxx

To substitute Internal DNS

Set the settings below on the audit system.
IP Address : 192.168.10.1
Netmask : 255.255.255.0
Gateway : 192.168.10.254

To substitute Internal Mail Server

Set the settings below on the audit system.
IP Address : 192.168.10.2

Netmask : 255.255.255.0
Gateway : 192.168.10.254

To substitute Backup Database

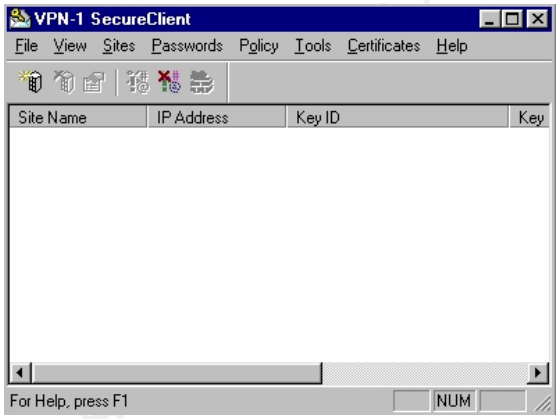
Set the settings below on the audit system.
IP Address : 192.168.10.3
Netmask : 255.255.255.0
Gateway : 192.168.10.254

To substitute Syslog Server

Set the settings below on the audit system.
IP Address : 192.168.10.4
Netmask : 255.255.255.0
Gateway : 192.168.10.254

For Authentication/Encryption Rule base :-

There are no commands to show for testing the authentication and encryption rule base.
To audit on the remote client authentication, we need to install the SecureClient software and set one of the dialup Public IP that GIAC had reserved with the ISP for example sss.sss.sss.1 and netmask 255.255.255.240 on the audit system.



We will coordinate via phone calls while conducting audit with our partner.

A packet sniffer tool such as Ethereal will help us to validate if the data transmitted across the VPN tunnel are encrypted over the wire.

Evaluate the audit

For The Rulebase :-

UDP Scan Result

From the various port scans that we have conducted, the output of the UDP scan has caught our attention and surprise. Although the UDP ports were disallowed in the rule base, but these UDP ports that were listed as open in the UDP scan. To analyze further, we referred to the log file in the firewall. We were relieved to discover that the security policy in the firewall managed to detect and drop the UDP scan. Below are some of the logs that we had viewed.

Log file extracted from GIAC-FW
The UDP scan for udp port 22 was dropped

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	User	Xlat
GIAC-FW	log	drop	22	Audit-System	GIAC-SSH-Server	udp	21	42630		

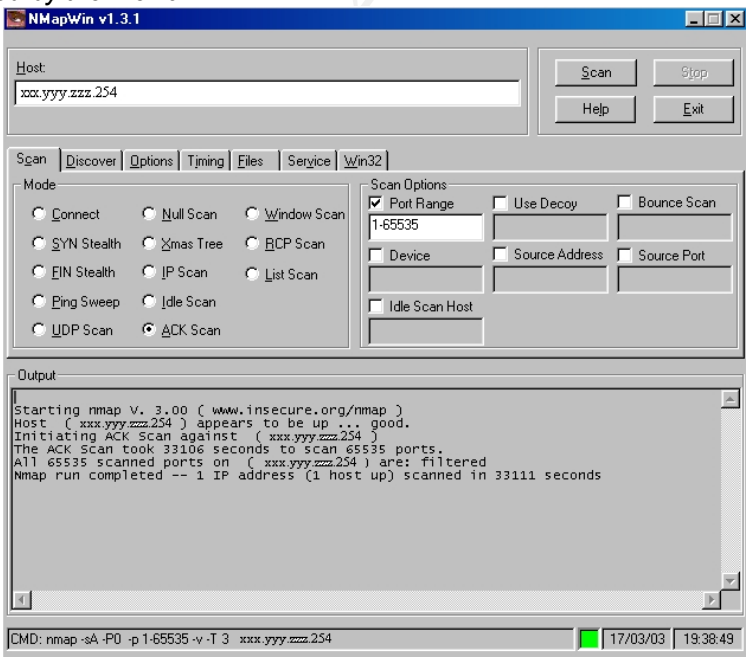
Log file extracted from GIAC-FW
The UDP scan for udp port 80 was dropped

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	User	Xlat
GIAC-FW	log	drop	80	Audit-System	Public-WebServe...	udp	21	58100		

Connect Scan and ACK Scan Result

The Connect scan and ACK scan had so far met our expectations. We are certain that the firewall is stateful in detecting the ACK scan and the Connect scan had confirmed that the security policy in our firewall are in good shape. Below is one of the snapshot taken from an ACK scan on the Firewall External Interface.

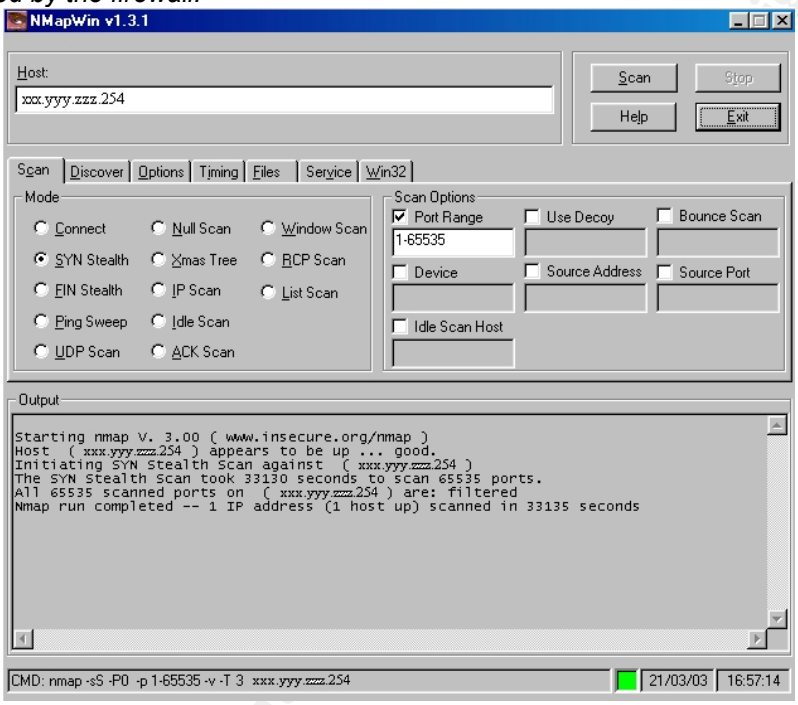
This figure is a snapshot of an ACK Scan on the Firewall External Interface. The Public IP address has been sanitized to fulfill the requirement set in GIAC Certification Administrivia There were 65535 ports scanned on the external interface of the firewall and all ports are found to be filtered by the firewall.



Ping Test Result
We are able to block all ping requests from the audit system at the External network.

SYN Stealth Scan Result
The SYN Stealth had similarly met the expected results. Below is one of the snapshot taken from a SYN Stealth scan on the Firewall External Interface.

This figure is a snapshot of an SYN Stealth Scan on the Firewall External Interface. The Public IP address has been sanitized to fulfill the requirement set in GIAC Certification Administrivia There were 65535 ports scanned on the external interface of the firewall and all ports are found to be filtered by the firewall.



For Authentication/Encryption Rule base :-

For Client to VPN Gateway (Mobile Employees and Suppliers)

Incorrect Password Test :-
We had conducted several session of VPN-1 & Firewall-1 Password authentication from the audit system. We had deliberately keyed in an incorrect password just to observe the behavior of the connection. We want to be certain that the remote client could not gain access to our corporate network when the authentication had failed.

Result :-

The firewall policy had rejected the user mobile1 request when an incorrect password was given. No further access can be attained when the authentication failed. The reject action is shown in the firewall's log.

Log file extracted from GIAC-FW
Mobile1 user's desktop was rejected and denied from access by the firewall.

Origin	Type	Action	Ser..	Source	Destin..	P..	R..	S_..	User	Info.
.. GIAC-FW	alert	reject		Audit-System	GIAC-FW		0		mobile1	reason Client Encryption: Access denied

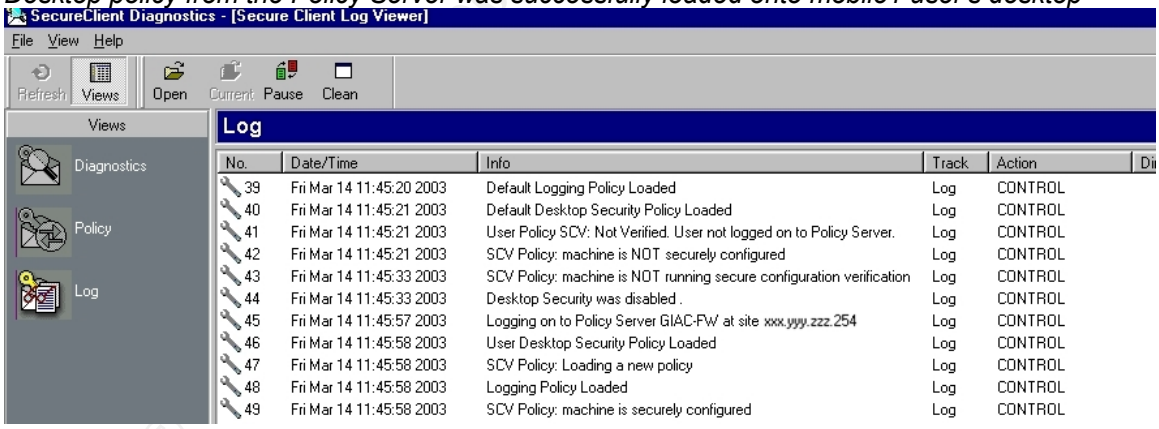
Correct Password Test :-
The second audit that we did was to input a correct password for user mobile1 (GIAC's mobile employee).

Result :-
User mobile 1 was successfully authenticated and this is shown in the log of both GIAC-FW and user mobile1 system.

Log file extracted from GIAC-FW
Successful Authentication with key installation at the mobile1 user's desktop

Origin	Type	Action	Servi..	Source	Destination	P..	..	S_P..	User	Info.
GIAC-FW	log	key install							mobile1	IKE: Main Mode comple
GIAC-FW	log	login		Audit-System	GIAC-FW		0		mobile1	success reason: User
GIAC-FW	log	key install		Audit-System	GIAC-FW				mobile1	IKE: Quick Mode compl

Log file extracted from the SecureClient Personal Firewall (at mobile1 user's desktop)
Desktop policy from the Policy Server was successfully loaded onto mobile1 user's desktop



We also noticed that the desktop policy defined at the Policy Server GIAC-FW has been successfully loaded on the mobile1 user's desktop. This is shown in the SecureClient log as attached above.

Encryption Test :-
User mobile1 has been granted with all the access defined in the rule but we need to be certain that these access are encrypted. The data transmitted must be encrypted at user mobile1 system and decrypted as it reached to the VPN

gateway. We need to verify this and therefore we refer to the log generated in GIAC-FW and user mobile1's system.

Results :-
The log below shows that the data was encrypted and decrypted over the VPN tunnel.

Encrypted webmail access from user mobile1's system

100	Fri Mar 14 11:40:44 2003	rule:4 , scheme::IKE ...	Log	ENCRYPT	OutBound	80	TCP 1401

Decrypted webmail access at GIAC-FW

Origin	Type	Action	Servi..	Source	Destination	P..	..	S_P..	User	Info.
GIAC-FW	log	decrypt	http	Audit-System	Mail-Relay	tcp	10	1251	mobile1	

Encrypted http access from user mobile1's system

112	Fri Mar 14 11:42:09 2003	rule:4 , scheme::IKE ...	Log	ENCRYPT	OutBound	80	TCP 1410

Decrypted http access at GIAC-FW

Origin	Type	Action	Servi..	Source	Destination	P..	..	S_P..	User	Info.
GIAC-FW	log	decrypt	http	Audit-System	Private-Web-Server	tcp	10	1223	mobile1	

Encrypted SSH access from user mobile1's system

104	Fri Mar 14 11:41:11 2003	rule:4 , scheme::IKE ...	Log	ENCRYPT	OutBound	22	TCP 1404

Decrypted SSH access at GIAC-FW

Origin	Type	Action	Servi..	Source	Destination	P..	..	S_P..	User	Info.
GIAC-FW	log	decrypt	SSH	Audit-System	GIAC-SSH-Server	tcp	10	1234	mobile1	

To reconfirm on our findings, we had also placed Ethereal software on the network to sniff the packet. When we try to decode the packet, we found that the packets were actually encrypted.

<u>For Gateway-to-Gateway VPN (Partners)</u>

Results :-
These are the logs generated on the GIAC-FW when we perform the VPN audit with one of our partners.

Log file extracted from GIAC-FW
Successful authentication with pre-shared secret password and key installation at Partner-FW

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	User	Xlat
GIAC-FW	log	key install		GIAC-FW	Partner-FW					
GIAC-FW	log	key install		GIAC-FW	Partner-FW					
GIAC-FW	log	key install		Partner-FW	GIAC-FW					
GIAC-FW	log	decrypt	http	Partner-Client	Private-Web-Serv...	tcp	11	1104		

Decrypted SSH access at GIAC-FW

Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	User	Xlat
GIAC-FW	log	decrypt	SSH	Partner-Client	GIAC-SSH-Server	tcp	11	kpop		

Partner was able to access the permitted services had confirmed that the data were encrypted at their end.
When we sniffed the packets with Ethereal, we also discovered that the packets were encrypted over the wire.

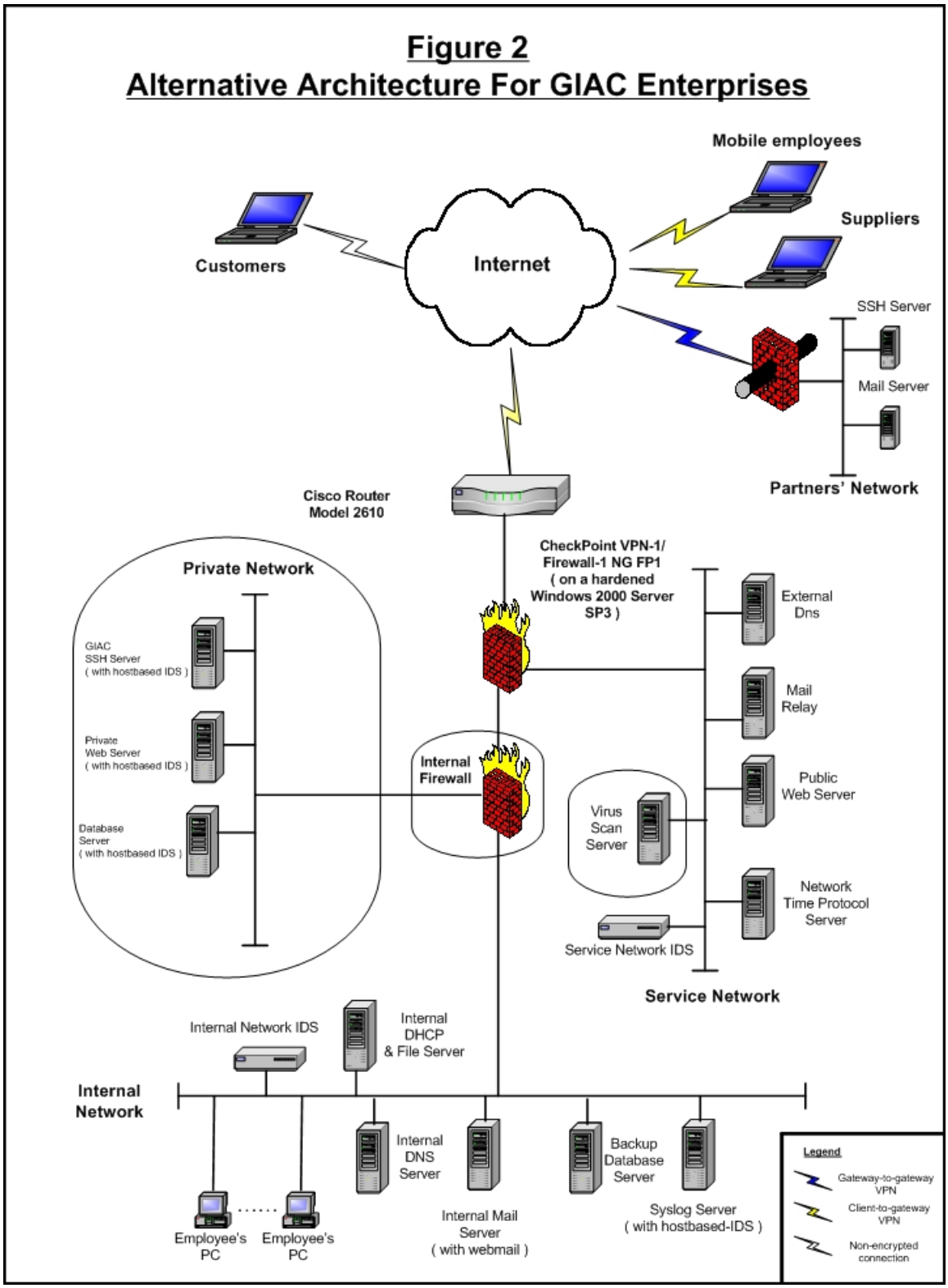
Based on the analysis shown above, we are certain that the primary firewall has correctly enforced and implemented GIAC Enterprises's security policy as describe in Assignments 1 and 2.

However, we felt that there are stillrooms for improvements with an alternate architecture.

Recommendation

We are aware that our President would like to start this e-business project with the very basic security components. With this reason, we had designed a very basic security architecture for a start. If the business grows positively, we shall then propose the design in Figure 2 as the alternate architecture for GIAC Enterprises.

Figure 2
Alternative Architecture For GIAC Enterprises



- It is vital to have an internal firewall to provide additional protection for servers on the Internal network and to segregate the GIAC SSH server, Private Web Server and the Database Server away from the Service

Network. In the event when the primary firewall is compromised, hackers or attackers can have direct access to these valuable servers. If we have another layer of protection, it would be harder for them to do so. They would need to spend more time and effort to defeat the second firewall. We should consider other type of firewall technologies when we make a purchase for a second firewall. It is truly a bad idea to place 2 set of firewall from the same vendor. The reason is very simple. Hackers or attackers will normally try their luck to use the same method to penetrate through the second firewall. If both of these firewalls are from the same vendor, the hackers or attackers will then be making their way in very easily.

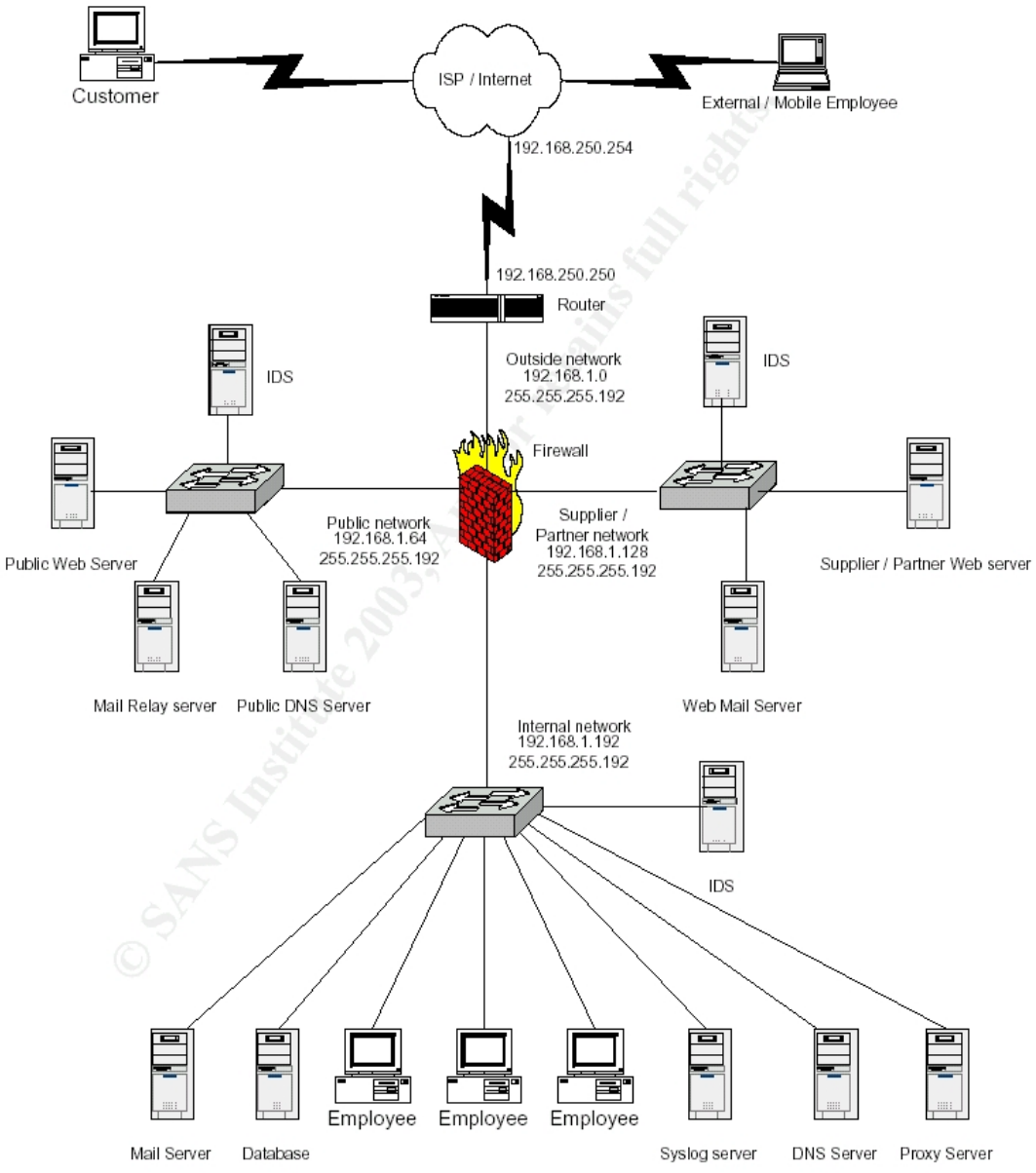
- The second consideration is to place a virus scan server. The virus scan server will work hand-in-hand with the firewall to scan all incoming and outgoing packet eg. smtp attachment with viruses. It helps to block malicious viruses from spreading to the Internal network and Service network
- Install host-based IDS on the critical servers, namely the Database server, Backup Database server, GIAC SSH server and the Syslog server. The ultimate purpose is to provide additional protection for the data and the operating system.
- Encourage other form of stronger authentication scheme for eg. SecureID for the mobile employees and suppliers.
- Do a periodic review on the firewall and server vulnerabilities. Practice constant patch and security updates and perform vulnerabilities assessment when time permit.

Assignment 4 – Design Under Attack

The practical paper that I have chosen for my attack is from Brian States. His paper can be found at http://www.sans.org/practical/GCFW/Brian_States_GCFW.pdf.
(Analyst number : 0368)

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.

Brian States has written a good practical paper and his paper is chosen because he had configured a Check Point VPN-1/Firewall-1 NG version with FP2 as the primary firewall on a Solaris 8 platform.

An Attack against the firewall itself

Research and describe a vulnerability

There is information on the Internet that described vulnerability found in Check Point VPN-1/Firewall-1 NG. The vulnerability is about employing "IKE Aggressive Mode" with share secret authentication for SecureRemote/ SecureClient is insecure as username can be sniffed and guessed.

The information is available at
http://www.securitytalks.com/forum/viewtopic.php?p=171&sid=f0f4457dcf0e79c6944faaced5f

Below are some of the details of the vulnerability that I have excerpted from http://www.securitytalks.com/forum/viewtopic.php?p=171&sid=f0f4457dcf0e79c6944faaced5f (author : Clement Dupuis)
Securitytalks.com forum gives the following description for Check Point VPN-1/Firewall-1 NG vulnerability :

> *Systems Affected :*
> *Systems running Check Point Firewall-1 version 4.0, 4.1, NG, NG FP1 and NG FP2 that use the IKE (Internet Key Exchange) [4] encryption scheme (known as ISAKMP/Oakley in v4.0) with shared secret authentication for remote user VPNs with SecuRemote/SecureClient. Note : in VPN-1/Firewall-1 NG Aggressive Mode is not enabled by default.*
>
> *Issues detail :*
> *Username Guessing*
> *The username guessing issue involves attempting to authenticate with the Firewall using IKE (Internet Key Exchange) [4] that is a standard protocol that forms part of the IPSec (IP Security) architecture [1]. If a remote user sends an appropriately constructed IKE packet to the Firewall containing the username to be tested, the Firewall will indicate whether the user is valid or not in, its reply packet. It is not necessary to send a password to obtain the reply from the Firewall.*
> *The correct approach would be to wait until both the username and password (shared secret) have been sent and then, if either is incorrect, to send a generic error message indicating that authentication had failed without detailing whether the username, password, or both were incorrect. In this way, an attacker is not able to determine if a given username is valid without also knowing the associated password. This technique is standard security practice in many other authentication mechanisms including UNIX login.*

Username sniffing
If a shared secret authentication is used with IKE aggressive mode, the identity is passed in the first packet that must be in the clear because the key exchange has not completed at this point so encryption cannot be used. SecuRemote uses the username for the identity in this first packet and therefore the username is passed in the clear. This ID sniffing issue is to some extent inherent in IKE aggressive mode because the ID must be passed in the clear. The problem here is that many users will not realize that potential issue and will therefore have a false sense of security. This username sniffing issue has the same potential weak password issue as the username guessing issue mentioned above, with the same possible result of full access to the company network via the VPN.

Vendor Response :
In the vulnerability claim document, two issues were presented :

a. *usernames are passed in cleartext using IKE Aggressive Mode*
b. *usernames are suscepticle to brute-force guessing when using IKE Aggressive Mode*

The first item is merely an accurate description of the IKE protocol. Check Point has no bug or vulnerability, but has correctly implemented the IKE standard for Aggressive Mode. The passing of usernames in cleartext is common to any vendors of IKE products who support Aggressive Mode. The claim of a vulnerability is incorrect.
The second item exists only in VPN-1/Firewall-1 v4.1 modules which are still configured to support SecuRemote/SecureClient connections using IKE Aggressive Mode, despite the availability of more secure options in the product. Note, again, that the guessable usernames in this scenario are, by design of the IKE protocol, sent in cleartext. By default, Aggressive Mode is not enabled in NG. In 4.1, the recommended configuration is to disable Aggressive Mode and use Hybrid Mode instead (which involves no change to the user experience).

Design an attack based on the vulnerability

We heard rumors that Brian State might have enabled aggressive mode and configured shared secret for a few of his SecureRemote users. We are not sure how valid is the rumors and we are indeed curious to check this out. Therefore we had planned to perform the username guessing attack to find out the truth.

To perform the username guessing we will use the fw1-ike-userguess program. The usage of fw1-ike-userguess program is shown in http://www.securitytalks.com/forum/viewtopic.php?p=171&sid=f0f4457dcf0e79c6944faaced5f.

We will run this command at our client.

$ fw1-ike-userguess --file=testusers.txt --sport=0 192.168.1.2
(192.168.1.2 is the external IP address of the targeted firewall)

We had gathered all the information that we need in order to increase the chances of success for the attack. We had also initiated the social engineering attempt by calling up the receptionist to enquire names of all GIAC mobile sales force. This helps us to create a list of potential names in our testuser.txt file.

To avoid detection, we managed to spoof an IP address from another network before we begin the attack.

Results of the attack

```
$ fw1-ike-userguess --file=testusers.txt --sport=0 192.168.1.2
testuser        Notification code 14
testing123      Notification code 14
guest           Notification code 14
brian           Notification code 14
amy             Notification code 14
robert          Notification code 14
$ exit
```

The attack has failed, as we could not find any users that have valid IKE configurations with shared secret authentication. Our attack was difficult as the firewall only responds with notification code 14. With this respond, we knew that the user is invalid. We could not determine why the user is invalid, as the firewall did not provide further information. In accordance to RFC 2408 section 3.14.1, the notification code 14 is defined as “NO-PROPOSAL-CHOSEN”.

The attack had run for about 10 minutes but we only received Notification code 14 as the results. We are certain that Brian State knew about this vulnerability and did not enabled the IKE Aggressive mode in his firewall and did not configured any of his SecureRemote/SecureClient users to use the shared secret authentication scheme.

(The document about countermeasures is available at http://www.securitytalks.com/forum/viewtopic.php?p=171&sid=f0f4457dcf0e79c6944faaced5f)

Countermeasures for the above attack :-
Below are some countermeasures that will help to mitigate the attack :-

- Use certificates for VPN authentication and avoid using usernames and passwords. This helps to overcome username guessing and sniffing problems.

- Implement Hybrid Mode authentication that have strong authentication scheme like RADIUS. This also helps to overcome username guessing and username sniffing problem.

A denial of service attack.

50 compromised cable modem/DSL
Our next action plan is to initiate the denial of service attack. The main purpose for this attack is to flood GIAC public web server with a very large amount of network traffic. This can prevent GIAC's customer from reaching the web server and may eventually force GIAC to bring down the web server temporarily.
To achieve such attack we must first find multiple compromised systems, which we could install the DDoS tools and use them as our weapon to attack. We had run a few scans and finally we managed to find a set of 50-compromised cable modem/DSL systems.

(The document about TFN2K is available at
http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt ,
http://www.ciac.org/ciac/documents/CIAC-2319_Distributed_Denial_of_Service.pdf)

We need to load a program called Tribal Flood Network 2000 (TFN2K) onto these newly compromised systems. Once the program has been successfully loaded, the 50 compromised cable modem/DSL systems will then be broken down as handlers and agents respectively.

The protocol use for communication between us (the attacker) and the handlers can be carried out via TCP, UDP or ICMP. The handlers will then later coordinate with the agents to trigger the attack.

The method of the attack is to do a SYN flood on the public web server's tcp port 80.

The command to use is as below :-
./ tfn –f tfn-client –i www.giac.com -p 80 –c 5

It would be hard for GIAC to trace this attack as
- IP addresses are spoofed to facilitate this attack
- Encryption is use for the communication between the handler and agents
- This DDoS tool has stealth capabilities built within

(The documents about countermeasures are available at
http://www.cert.org/incident_notes/IN-99-07.html
http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt

http://www.ciac.org/ciac/documents/CIAC-2319_Distributed_Denial_of_Service.pdf)

Describe the Countermeasures

Below are some countermeasures that will help to mitigate the attack :-

- Enable SYN defender feature in the Check Point VPN-1/Firewall-1 NG
- Reduce TCP session time out limits from default 60 minutes (3600 secs) to about 20 minutes (1200 secs). This helps to efficiently remove old entries created by DDoS attack before exhausting state tables entries at the firewall. We must be careful in selecting the time out limits as it may affect FTP command sessions (in Brian States's design it should not be a problem as there are no access requirement for FTP services).
  (SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.2, page 92)
- Firewall has limited size state table. Increase the maximum sessions from default 5,000 connection to about 50,000. This helps to create more entries in an internal connection table as attacker can easily filled up the state tables with many non-legitimate entries during the DDoS attack. Once the state table is filled up, no more new entries can be created and thus can affect the firewall.
  (SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.2, page 93)
- Have IDS install on the network to monitor for denial of service attack. The IDS system should have the latest attack patterns or signatures.
- Disallow spoofed source addresses as the source IP packet. This can be control at the border router Access Control List for the ingress and egress filtering.
- Unnecessary ICMP, TCP and UDP traffic should be blocked.
- All operating systems and applications software must be frequently updated with the most current security patches and hot fixes.
- All services that are not required on the servers or network devices should be turned off
- Encourage users to use strong password and do a periodic change on their password
- System administrator should practice to use tools that are available to detect possible handlers and agents in their system. The tools are available from National Infrastructure Protection Center (NIPC) at http://www.fbi.gov/nipc/trinoo.htm.
- Perform regular systems and network security audit and check all logs promptly

Compromise An Internal System

Select a Target

Our next target to attack shall be the Public Web Server. There are a few reasons why we had chosen this system as our attack.

Reasons :-

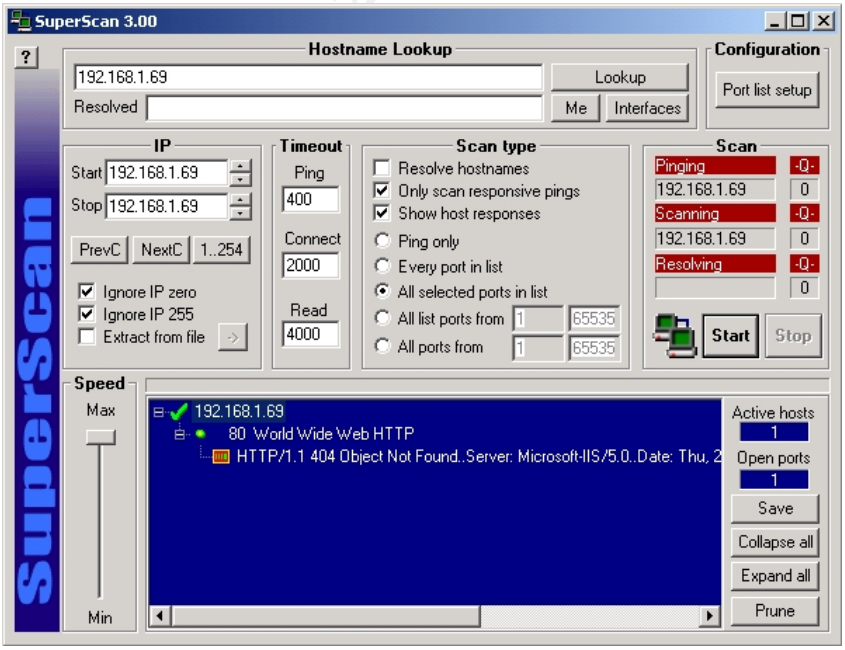
- There are many websites on the Internet that are using Microsoft IIS Server as their web server. IIS web server is very common and many organizations had deployed their website using IIS web server as it comes by default with the Windows operating system.
- Http port 80 is commonly open in any organization's firewall. We as an attacker can take this advantage to craft a packet and sent that packet to the web server via the open port and slowly perform the attack.
  (http://www.pinpt.com/solutions/whitepapers/wp_intrusion.html)
- It is very easy for us to determine the hostname and IP address of a publicly accessible web server as these information can be obtained by querying GIAC external DNS server. It unlike servers that reside in the internal network where we need to do some advance tracing or mapping with an exposed SNMP protocol.

Process to Compromise

To begin with the attack, we need to determine the web server hostname or IP address by doing a simple query to the GIAC external DNS server . The known public IP address for the webserver is 192.168.1.69 (as specified in Brian States's practical paper) and hostname is www.giac.com.

Our very next step is to find out what kind of web server is GIAC using. A scan tool called SuperScan 3.0 can help us to expose the server type.

Below is a scan result that we had detected with SuperScan 3.0.



We were truly glad that our guesses are right. The web server use is indeed a Microsoft IIS Web server and we are now able to proceed with our attack.

We found a white paper that explains the ".+HTR" vulnerability in IIS Web Server. The white paper is available at
http://www.pinpt.com/solutions/whitepapers/wp_intrusion.html

An attack can be carried out by sending in a normal http request with an append of a "+" and ".HTR" to request for a filename. This can cause the ISM.DLL to be called by IIS in order to get the target file open. Part of the target file's source code will be displayed to us if the target file opened by ISM.DLL is not an .HTR file. We only need to send a simple URL (as shown below) with our browser and a source code will be displayed if the attack is successful.

Attack via http request :-
http://www.giac.com/global.asa+.htr

The "global.asa" file name cannot be changed and it is use to define event scripts and objects.

Our attempt has failed, as we did not get to see the source code in the returned page. We believed that GIAC must have carried out some countermeasures by patching the IIS server with the latest patches, hot fixes and had disabled some extensions in the IIS web server.

References

Assignment 1

SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.3
SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.4
SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.5

"Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs". 2003. URL:http://www.checkpoint.com/products/downloads/why_choose_integration.pdf (12 May 2003)

Check Point Software Technologies Ltd. "Remote Access VPN Solution" Document P/N 500187. June 2000

"Network Intrusion Detection System, The Accurate, Tunable Intrusion SecureNet Series". November 2002.
URL : http://www.intrusion.com/products/downloads/NidsPO_1102.pdf (21 June 2003)

"Check Point VPN-1/Firewall-1". TCP and UDP Ports used by Next Generation. 26 February 2003. URL : http://www.fw-1.de/aerasec/ng/ports-ng.html. (17 March 2003)

IP Addressing Scheme

Yakov Rekhter, Robert G Moskowitz, Daniel Karrenberg, Geert Jan de Groot, Eliot Lear. "Address Allocation for Private Internets". February 1996.
URL : http://www.isi.edu/in-notes/rfc1918.txt (2 March 2003)

Assignment 2

Cisco Router Access Control List

Yakov Rekhter, Robert G Moskowitz, Daniel Karrenberg, Geert Jan de Groot, Eliot Lear. "Address Allocation for Private Internets". February 1996.
URL : http://www.isi.edu/in-notes/rfc1918.txt (2 March 2003)

"NSA/SNAC Router Security Configuration Guide – Executive Summary Card" Version 1.1. URL:http://www.nsa.gov/snac/cisco/guides/cis-1.pdf (2 March 2003)

Vanessa Antoine, Raymond Bongiorni, Anthony Borza, Patricia Bosmajian, Daniel Duesterhaus, Michael Dransfield, Brian Eppinger, Kevin Gallicchio, James Houser, Andrew Kim, Phyllis Lee, Tom Miller, David Opitz, Florence Richburg, Michael Wiacek, Mark Wilson, Neal Ziring. "Router Security Configuration Guide" Version 1.1. 27 Sept. 2002. URL : http://www.nsa.gov/snac/cisco/guides/cis-2.pdf (2 March 2003)

Frank Keeney. "Cisco Access List". URL : http://pasadena.net/cisco/secure.html (2 March 2003)

Chris Brenton. “What is Egress Filtering and How Can I Implement It ?” Egress Filtering v0.2. 29 February 2000.
URL : http://www.sans.org/infosecFAQ/firewall/egress.htm (2 March 2003)

“Internet Protocol V4 Address Space”. 4 April 2003.
URL : http://www.iana.org/assignments/ipv4-address-space. (3 June 2003)

SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.2
SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.3

Building Firewall Rule base

Lance Spitzner. “Building Your Firewall Rulebase”. 26 January 2000
URL : http://www.spitzner.net/rules.html. (8 January 2003)

SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.2

Hardening Windows 2000 Server
SANS Institute, “ Securing Windows 2000 Step by Step Version 1.5“ Malaysia Edition, July 1, 2001

Tutorial

Student Edition Book - Check Point VPN-1/Firewall-1 Management I & II NG

SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.4

Check Point VPN-1/Firewall-1 NG Help File

Assignment 3
Firewall Rule Base Audit

Lance Spitzner. “Auditing Your Firewall Setup”. 12 December 2000
URL : http://www.spitzner.net/audit.html. (8 January 2003)

“Check Point VPN-1/Firewall-1”. TCP and UDP Ports used by Next Generation. 26 February 2003. URL : http://www.fw-1.de/aerasec/ng/ports-ng.html. (17 March 2003)

NmapWin Help File – nmapwin.chm

Assignment 4
Design Under Attack

http://www.sans.org/practical/GCFW/Brian_States_GCFW.pdf

Attack Against The Firewall
Clement Dupuis. "Checkpoint FW-1 VPN Security Flaw". 3 September 2002. URL:http://www.securitytalks.com/forum/viewtopic.php?p=171&sid=f0f4457dcf0e79c6944faaced5f. (17 March 2003)

Distributed Denial Of Service Attack
SANS Institute Track 2 – Firewalls, Perimeter Protection and VPNs, Book 2.2

Jason Barlow and Woody Thrower. "TFN2K – An Analysis". Version 1.3. 7 March 2000. URL : http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt. (18 March 2003)

Paul J. Criscuolo. "Distributed Denial of Service". Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319. 14 February 2000. URL : http://www.ciac.org/ciac/documents/CIAC-2319_Distributed_Denial_of_Service.pdf. (18 March 2003)

http://www.fbi.gov/nipc/trinoo.htm

Rik Farrow. " Distributed Denial of Service Attacks". 3 January 2000. URL : www.networkmagazine.com/article/NMG20000512S0041 (17 March 2003)

"Distributed Denial of Service Tools". 15 January 2001. URL : www.cert.org/incidents_notes/IN-99-07.html (17 March 2003)

Compromise An Internal System
Yona Hollander, PhD. "The Future of Web Server Security – Why your Web site is still vulnerable to attack". URL : http://www.pinpt.com/solutions/whitepapers/wp_intrusion.html. (17 March 2003)

Shawn V. Hernan. "Vulnerability Note VU#363715". 10 April 2002. URL : http://www.kb.cert.org/vuls/id/363715 (17 March 2003)

Shawn V. Hernan. "CERT® Advisory CA-2002-09 Multiple Vulnerabilities in Microsoft IIS". 11 April 2002. URL : http://www.cert.org/advisories/CA-2002-09.html (17 March 2003)

Scanning Tools and Sniffer
www.nmap.org
http://www.networkingfiles.com/PingFinger/downloads/superscandownload.htm
www.ethereal.com

Additional References (Practical Papers with Honors)
http://www.sans.org/practical/Emily_Gladstone_GCFW.zip
http://www.sans.org/practical/Peter_Vestergaard_GCFW.zip