# GIAC CERTIFIED FIREWALL ANALYST (GCFW)

# PRACTICAL ASSIGNMENT

Version 1.8 (Revised September 10, 2002)

---

Aloysius Johannes Kolibonso

January 1, 2003

# TABLE OF CONTENTS

# Abstract

This Practical Assignment is created as part of the requirements to pass GIAC Certified Firewall Analyst certification. This assignment comprises of four parts. The first part defines GIAC Enterprises business requirements and the network security architecture proposed. The second part describes security policies for each security components and provides a short tutorial on configuring one of the components. The third part describes the audit activities and results. The last part of the assignment is an exercise on actual threats to network design.

# 1. Assignment 1 – Security Architecture

## 1.1 Company Background

GIAC Enterprises is an e-business, which deals in the online sale of fortune cookie sayings. Their e-commerce business operations involve:

- Customers (Companies or individuals that purchase bulk online fortunes)
- Suppliers (Companies that supply GIAC Enterprises with their fortune cookie sayings)
- Partners (International companies that translate and resell fortunes): GIAC currently has only one Partner Company.
- GIAC Enterprises employees located on GIAC Enterprise's internal network
- GIAC Enterprises mobile sales force and teleworkers

## 1.2 Business Requirements

This section describes the requirements needed for GIAC to operate properly. This includes defining the relationships between GIAC and the other entities it interacts with.

### 1.2.1 Customers

Customers purchase bulk online fortunes via the Internet using a web browser that supports 128-bit SSL encryption. GIAC web server will be accessible from the Internet using HTTP and HTTPS. Customers shall be able to perform the following things on the GIAC website:

- Browse for general information and the login page (HTTP)
- Register online as a new customers (HTTPS)
- Login using a registered account to make purchase, update customer information, and download fortune cookies (HTTPS)

### 1.2.2 Suppliers

Suppliers access GIAC web server using a web browser that supports 128-bit SSL. The web server is accessible from the Internet using HTTP (for general information and login page) and HTTPS (from submitting login information until logged out). Once logged in to the web site, the supplier shall be able to submit invoices, view invoices and view his transaction history. In addition to that Suppliers will also need to be able to upload fortune cookies files to GIAC site. Since plain FTP is considered insecure, files uploading capability will be enabled by using FTP-over-SSH protocol. The supplier will need to have an SSH client or a secure FTP client (i.e. SecureFX from Van Dyke Technologies, Inc.) that supports FTP over SSH2.

### 1.2.3 Partners

GIAC has established a business-to-business (B2B) integration with its first overseas Partner, IndoFortunes Inc., a company based in Jakarta, Indonesia. The integration solution is developed using Microsoft BizTalk Server. Transactions between GIAC and IndoFortunes will be performed by exchanging XML documents over the Internet using HTTPS protocol. Business processes will be automated using BizTalk with ability to execute rollback and/or compensating transaction, full state management, workflow, and rules engine. This integration model has been selected as the standard integration architecture for GIAC future partners.

GIAC realizes that integration with external entities also brings more risk to the organization. To ensure that network communication really comes from a trusted Partner network, and to secure the information exchanged between the two companies, GIAC requires the Partner to implement a Gateway-to-Gateway VPN to GIAC Firewall. This type of VPN is best suited for company partnerships where there are known static IP addresses for both entities.

### 1.2.4 Internal Employees

GIAC internal employees shall be permitted to access the Internet via HTTP, HTTPS, and FTP through the firewall's application proxies. Internal employees shall be able to send and receive email through the internal mail server (MS Exchange 2000 Server). This internal mail server will then forward mail to and receive mail from the external mail server located on DMZ1. This is to prevent direct connections from the internal network to the Internet. Both mail servers will have virus-scanning software running on them.

Some internal employees will have access to the servers on the DMZ1 and DMZ2 for systems administration. For remote administration purposes, Windows 2000 Servers will have their Terminal Services enabled in Remote Admin Mode. However, Terminal Services access to DMZ servers shall be restricted to only allow incoming connection requests from the designated Management Workstations.

### 1.2.5 Mobiles Sales Force and Teleworkers

All GIAC Mobile Sales Force and Teleworkers shall be able to access GIAC Enterprises network using dial-in connection provided by Remote Access Server (RAS). All RAS users connect from their laptops operating system's RAS client in combination with RSA SecurID token to provide two-factor authentication. ACE/Server located on the internal network provides RAS authentication service. This will require RADIUS communications from the RAS Server to ACE/Server (udp port 1645 and udp port 1646).

RAS users shall be able to access a Terminal Server located in the internal network to run applications that they have privilege to. They will also be able to access the internal mail server. Each mobile user's laptops is protected by Norton Anti Virus software (http://www.symantec.com/) and ISS Black Ice Personal Firewall (http://www.iss.net/) to protect them from attacks when they are connected to the Internet or other networks.

### 1.2.6 Other Operational Network Traffic

The following network traffic shall also be allowed for normal operation of GIAC infrastructure:

- ssh access to Border Router from designated Management Workstations for administration purposes.
- syslog from all devices to Log Server. Third-party software will be utilized on Windows 2000 Servers to capture Event Logs.
- ntp from all internal devices to NTP Server (running on the same machine as the Log Server).
- radius authentication and accounting from RAS Server to RSA ACE/Server.
- https from designated Management Workstations to Firewall for firewall administration from the Management Workstations.
- ms-sql from Web Server to Database Server (MS SQL Server 2000).
- ms-sql from BizTalk Server to Database Server(MS SQL Server 2000).
- Windows Terminal Service from RAS users to Terminal Server.
- Windows Terminal Service from designated Management Workstations to all Windows 2000 Server.
- ssh from designated Management Workstations to Mail Relay server.
- smtp from the Internet to Mail Relay, and vice versa.
- smtp from Internal Mail Server to Mail Relay, and vice versa.
- ms-exchange from RAS clients to Internal Mail Server (requires a registry edit make sure the Exchange Server uses fixed port numbers. By default, Exchange Server picks a random port number that the client uses in order to communicate with the Exchange Server. The port numbers to be used by GIAC are 6001 and 6002).
- DNS query from Internal Network and DMZs to Firewall (split DNS servers shall be running on the Firewall providing Internal DNS and Forwarder DNS).
- DNS query from Firewall (which runs Forwarder DNS) to ISP's DNS Server (which hosts GIAC External DNS).

## 1.3 Network Security Architecture

GIAC's network is as illustrated in Figure 1. The network comprises of 1 (one) external network (the Internet) and 4 (four) internal networks:

- Remote Access network
- DMZ 1: service network for access from the Internet (Customers & Suppliers)
- DMZ 2: service network for Partners via VPN
- Internal Network

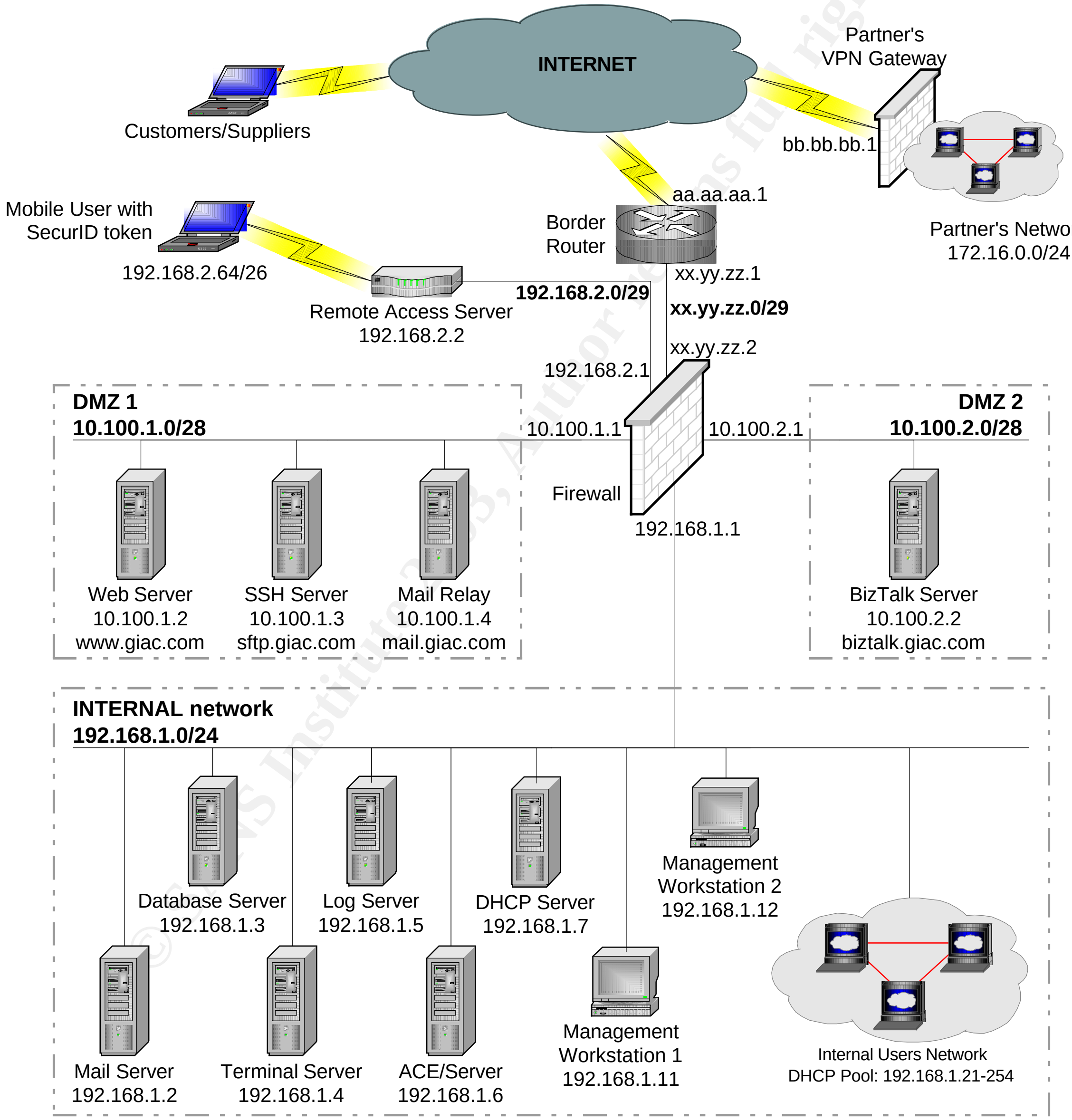


*Figure 1. GIAC Network Architecture*

The following table describes GIAC's IP addressing scheme:

| Network Segment | Network Address | Subnet Mask |
|---|---|---|
| External Network | xx.yy.zz.0 | 255.255.255.248 |
| Remote Access Network | 192.168.2.0 | 255.255.255.248 |
| DMZ 1 | 10.100.1.0 | 255.255.255.240 |
| DMZ 2 | 10.100.2.0 | 255.255.255.240 |
| Internal Network | 192.168.1.0 | 255.255.255.0 |

All internal networks utilize non-routable IP addresses (RFC 1918). The Firewall shall use Dynamic NAT (Network Address Translation) for all internal addresses, except for Log Server. All servers that need to be accessed from External Network will be using Cyberguard's proxies, except for Log Server that will have a virtual IP addresses configured on the Firewall for it: xx.yy.zz.9.

## 1.4 Architecture Components

This section will describe each component of GIAC Network Architecture.

### 1.4.1 Border Router

The border router is a Cisco Router 3620 with IOS version 12.2. It is selected because it is a relatively inexpensive router with rich features and should be able to accommodate future bandwidth growth. The router has an Ethernet interface on the internal side and a T1 interface on the external side for WAN connection to the ISP. The Ethernet interface address is set to xx.yy.zz.1 and the WAN interface is set to aa.aa.aa.1. It also has its SSH feature enabled for administration from designated Management Workstations.

### 1.4.2 Firewall/VPN Appliance

The firewall is Cyberguard Firewall/VPN Appliance FS500 release 5.0 Unixware PSU 2 with 6 (six) 10/100 Ethernet interfaces. It is a proxy-based firewall appliance with integrated VPN capabilities. It has earned Common Criteria Evaluation Assurance Level 4 (EAL4), ICSA, and other certification standards. It boasts capable to handle up to 550 thousand simultaneous connections, with 250 Mbps performance. Cyberguard FS500 features multilevel security hardened operating system, integrated IPSec VPN, secure remote management via SSL (Tarantella), stateful time-based packet filtering, application proxies (SmartProxies) for common protocols (e.g. FTP, HTTP, SSL, SMTP), dynamic and static NAT, Split DNS, routing, and optional high availability software for future needs.

A complete data sheet of this firewall appliance model is available at http://www.cyberguard.com/PDF/datasheet_FS_5_1.pdf

Cyberguard Firewall Manual (Release 5.0) can be downloaded from ftp://ftp.cybg.com/Unix/5.0/Doc/

### 1.4.3 Remote Access Server

GIAC's Remote Access Server is Cisco AS3600 with IOS version 12.2. It has 32 ports dial access and supports Radius for authentication with RSA ACE/Server (two-factor authentication with SecurID token).

### 1.4.4 Web Server

GIAC's Web Server is a Windows 2000 Server Service Pack 3 running Internet Information Server 5.0 with all Windows 2000 Hotfix (Pre-SP4) installed. The web server has been hardened with IISLockDown tool with the following purposes:

- to remove script mappings
- to remove sample web files
- to remove the Scripts virtual directory
- to remove MSADC directory
- to disable WebDAV (Web Distributed Authoring and Versioning)
- to set file permissions to prevent the IIS anonymous user from executing system utilities (such as cmd.exe, tftp.exe)
- to set file permissions to prevent the IIS anonymous user from writing to content directories

GIAC web server also utilizes URLscan, an ISAPI filter that analyzes and screen HTTP request to reduce exposure to potential attacks. It allows configuration of IIS to reject requests based on the following criteria:

- The request method (verb)
- The file extension of the resource requested
- Suspicious URL encoding
- Presence of non ASCII characters in the URL
- Presence of particular character sequences in the URL
- Presence of particular headers in the request

IISLockDown and URLscan are available from Microsoft's website http://www.microsoft.com/security.

This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

This Web Server will be accessed via Cyberguard's SmartProxy.

### 1.4.5 SSH Server

GIAC's SSH Server is Van Dyke Software's VShell Server v2.1.1 running on Windows 2000 Server Service Pack 3 with all Windows 2000 Hotfix (Pre-SP4) installed. This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

This Web Server will be accessed via Cyberguard's PortGuard.

### 1.4.6 Mail Relay

This mail server acts as a gateway for all inbound and outbound e-mails. It runs Sendmail 8.12.6 on Linux Redhat 7.2 machine. This server does not contain real data. It also runs OpenSSH 3.5 for administration from designated Management Workstations.

This Web Server will be accessed via Cyberguard's SmartProxy.

### 1.4.7 BizTalk Server

This server acts as integration server with GIAC's Partner, IndoFortunes Inc. It is a Windows 2000 Server Service Pack 3 running Microsoft BizTalk Server 2000 SP1 with all Windows 2000 Hotfix (Pre-SP4) installed. It also runs Internet Information Server 5.0 and hardened with IISLockDown and URLscan tools (see 1.4.4). This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

This Web Server will be accessed via Cyberguard's SmartProxy.

### 1.4.8 Internal Mail Server

GIAC's mail server is a Windows 2000 Server SP3 running Microsoft Exchange 2000 SP3 with all Windows 2000 Hotfix (Pre-SP4)installed. A registry edit has been done to set the server to use fixed communications ports, tcp/6001 and tcp/6002. A virus scanning software is installed on this Exchange Server. This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

### 1.4.9 Database Server

GIAC's database server is a Windows 2000 Server SP3 running Microsoft SQL 2000 Server SP2 with all Windows 2000 Hotfix (Pre-SP4) installed. MS SQL Server network protocol is set to default port 1433. This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

### 1.4.10 Terminal Server

GIAC's Terminal Server is a Windows 2000 Server SP3 with all Windows 2000 Hotfix (Pre-SP4) installed. It runs Terminal Service in Application Server mode. RAS users shall be able to connect to this Terminal Server to run some internal applications.

### 1.4.11 Log Server

GIAC's Log Server is a Windows 2000 Server SP3 with all Windows 2000 Hotfix (Pre-SP4) installed. It runs Kiwi Enterprises' Syslog Daemon v7.0.2 (http://www.kiwisyslog.com/) and Tardis 2000 (http://www.kaska.demon.co.uk/) to provide NTP service for time synchronization. This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

### 1.4.12 RSA ACE/Server

GIAC's RSA ACE/Server is a Windows 2000 Server SP3 with all Windows 2000 Hotfix (Pre-SP4) installed. It runs RSA Security's ACE/Server v5.0 (http://www.rsasecurity.com/products/securid/datasheets/dsace50.html). This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

### 1.4.13 DHCP Server

GIAC's DHCP Server is a Windows 2000 Server SP3 with all Windows 2000 Hotfix (Pre-SP4) installed. It has DHCP service enabled with address pool from 192.168.1.21 to 192.168.1.254. It provides DHCP service for internal employees' workstations. This server also runs Terminal Service in Remote Administration mode for administration from designated Management Workstations.

### 1.4.14 Management Workstations

GIAC's Management Workstations are Windows 2000 Professional SP3 with all Windows 2000 Hotfix (Pre-SP4) installed. Required administration tools are installed on this workstations. Only the system administrators are allowed to logon on these machines. Both Management Workstations are assigned static IP addresses (192.168.1.11 and 192.168.1.12). This will allow creating security rules per IP address basis for some administration/management traffic.

# 2. Assignment 2 – Security Policy and Tutorial

## 2.1 Border Router Policy

The border router is a Cisco Router 3620 with IOS version 12.2. The router has an Ethernet interface on the internal side and a frame relay T1 interface on the external side for WAN connection to the ISP. The Ethernet interface address is set to xx.yy.zz.1 and the WAN interface is set to aa.aa.aa.1. It also has its SSH feature enabled for administration from designated Management Workstations.

Logging is sent to the Log Server (syslog) located internal network at address 192.168.1.5. The firewall will be configured a virtual IP address of xx.yy.zz.9 for the Log Server so the router can send its logging. NTP Server is also located on this Log Server.

The border router is the first line of defense. GIAC used the NSA Router Security Configuration Guide as a guideline in configuring the border router.

### 2.1.1 General Configuration

Assign a hostname and username(s), enable password encryption and assign “enable” password, and set up a warning banner.

```
hostname charlie
username johan password AjaX1973
service password-encryption
enable secret RaHaSi4
banner motd *WARNING: UNAUTHORIZED ACCESS IS PROHIBITED*
```

Turn off all servers that are not required.

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip bootp server
no ip http server
no snmp-server
no service config
no boot network
no cdp run
```

Disable source routing and classless routing.

```
no ip source-route
no ip classless
```

Disable domain name lookup as it may pose some risk of spoofing and may hurt performance.

```
no ip domain-lookup
```

For all interfaces, disable directed broadcasts (may be used in DoS attack), disable proxy-arp, and prevent sending of IP unracheables, redirects, and mask replies (may be used in network mapping by attackers).

```
no ip directed-broadcast
no ip proxy-arp
no ip unreachable
no ip redirect
no ip mask-reply
```

Set border router to use NTP server

```
ntp source Ethernet0/0
service timestamps log datetime localtime
service timestamps debug datetime localtime
ntp server xx.yy.zz.9
```

Configure router to send logging messages to Log Server using syslog. Messages will be sent from the internal interface of the router using local7 facility.

```
logging on
logging console informational
no logging monitor
logging xx.yy.zz.9
logging trap debugging
logging facility local7
logging source interface Ethernet0/0
```

Enforce vty to require SSH.

```
Charlie(config)# line vty 0 4
Charlie(config-line)# login local
Charlie(config-line)# transport input ssh
```

### 2.1.2 Access Control Lists (ACLs)

GIAC's border router utilizes extended ACLs, which offers more filtering options. Filtering will be based on source IP address, destination IP address, source and destination ports, protocol, and ICMP message types. Filtering will be applied to inbound traffic on external interface, and to inbound traffic on the internal interface.

### 2.1.2.1 External Interface ACL

```
no access-list 101

! Block packets with internal addresses as source ip
access-list 101 deny ip xx.yy.zz.0 0.0.0.15 any log

! Block loopback and all reserved addresses
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

! Block multicast and broadcast
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
access-list 101 deny ip host 0.0.0.0 any log

! Block ICMP redirects
access-list 101 deny icmp any any redirect log

! Block Land attacks
access-list 101 deny ip host aa.aa.aa.1 host aa.aa.aa.1 log

! Block incoming syslog traffic
access-list 101 deny udp any any eq syslog log

! Block incoming snmp traffic
access-list 101 deny udp any any eq 161 log
access-list 101 deny udp any any eq 162 log
access-list 101 deny tcp any any eq 161 log
access-list 101 deny tcp any any eq 162 log

! Block NetBIOS traffic
access-list 101 deny tcp any any range 135 139 log

! Block TFTP traffic
access-list 101 deny udp any any eq 69 log

! Permit only traffic destined for firewall’s external interface
! and published virtual IP (Log Server)

access-list 101 permit ip any host xx.yy.zz.2
access-list 101 permit ip any host xx.yy.zz.9

! Deny everything else
access-list 101 deny ip any any log
```

To apply this access-list to inbound traffic on the external interface, type the following command in the interface configuration mode.

```
ip access-group 101 in
```

### 2.1.2.2 Internal Interface ACL

```
no access-list 102

! Block ICMP traffic that may be used for network mapping
access-list 102 deny icmp any any host-unreachable
access-list 102 deny icmp any any echo-reply
access-list 102 deny icmp any any time exceeded

! Permit traffic from firewall external interface and virtual IPs only
access-list 102 permit ip host xx.yy.zz.2 any
access-list 102 permit ip host xx.yy.zz.9 any

! Deny everything else
access-list 102 deny ip any any
```

To apply this access-list to inbound traffic on the internal interface, type the following command in the interface configuration mode.

```
ip access-group 102 in
```

## 2.2 Firewall Policy

GIAC's Firewall will be configured in a way that everything that is not required for normal operation of the site will be denied.

The following table lists Firewall interfaces configuration.

| Interface | IP address | Subnet Mask | Comments |
|---|---|---|---|
| Dec0 | xx.yy.zz.2 | 255.255.255.248 | External interface connected to Border Router |
| Dec1 | 10.100.1.1 | 255.255.255.240 | Internal interface connected to DMZ1 |
| Dec2 | 10.100.2.1 | 255.255.255.240 | Internal interface connected to DMZ2 |
| Dec3 | 192.168.2.1 | 255.255.255.248 | Internal interface connected to Remote Access network |
| Dec4 | 192.168.1.1 | 255.255.255.0 | Internal interface connected to Internal network |

Dynamic NAT rule is applied to the External network interface. Pass Address feature is turned off.

| Dynamic NAT for Interface | IP address | Subnet mask |
|---|---|---|
| External | xx.yy.zz.2 | 255.255.255.248 |

Static NAT is configured to enable access to Log Server.

| Static NAT for Server | Global Address (virtual IP address) | Internal Address (real IP address) |
|---|---|---|
| Log Server | xx.yy.zz.9 | 192.168.1.5 |

The following table summarizes all access requirements of GIAC Firewall.

| Service/Protocol | Source | Destination |
|---|---|---|
| http (tcp/80) | Internet | Web Server 10.100.1.2 |
| | Partner's Network bb.bb.bb.1 | BizTalk Server 10.100.2.2 |
| | Internal Network | Internet |
| | Internal Network | Web Server 10.100.1.2 |
| https (tcp/443) | Internet | Web Server 10.100.1.2 |
| | Partner's Network bb.bb.bb.1 | BizTalk Server 10.100.2.2 |
| | Internal Network | Internet |
| | Internal Network | Web Server 10.100.1.2 |
| ftp (tcp/21) | Internal Network | Internet |
| ssh (tcp/22) | Internet | SSH Server 10.100.1.3 |

| | | |
|---|---|---|
| | Internal Network | SSH Server<br>10.100.1.3 |
| | MgmtWkstn1<br>192.168.1.11 | Border Router<br>xx.yy.zz.1 |
| | MgmtWkstn2<br>192.168.1.12 | Border Router<br>xx.yy.zz.1 |
| | MgmtWkstn1<br>192.168.1.11 | Mail Relay<br>10.100.1.4 |
| | MgmtWkstn2<br>192.168.1.12 | Mail Relay<br>10.100.1.4 |
| smtp (tcp/25) | Internet | Mail Relay<br>10.100.1.4 |
| | Mail Relay<br>10.100.1.4 | Internet |
| | Internal Mail Server<br>192.168.1.2 | Mail Relay<br>10.100.1.4 |
| MS SQL (tcp/1433) | Web Server<br>10.100.1.2 | Database<br>192.168.1.3 |
| | BizTalk Server<br>10.100.2.2 | Database<br>192.168.1.3 |
| Terminal Services (tcp/3389) | MgmtWkstn1<br>192.168.1.11 | DMZ1 |
| | MgmtWkstn2<br>192.168.1.12 | DMZ1 |
| | MgmtWkstn1<br>192.168.1.11 | DMZ2 |
| | MgmtWkstn2<br>192.168.1.12 | DMZ2 |
| | RAS Users | Terminal Server<br>192.168.1.4 |
| MS Exchange<br>(tcp/6001, tcp/6002) | RAS Users | Internal Mail Server<br>192.168.1.2 |
| Ntp (udp/123) | Border Router<br>xx.yy.zz.1 | Log Server<br>192.168.1.5 |
| | RAS<br>192.168.2.2 | Log Server<br>192.168.1.5 |
| | DMZ1 | Log Server<br>192.168.1.5 |
| | DMZ2 | Log Server<br>192.168.1.5 |
| Syslog (udp/514) | Border Router<br>xx.yy.zz.1 | Log Server<br>192.168.1.5 |
| | RAS<br>192.168.2.2 | Log Server<br>192.168.1.5 |
| | DMZ1 | Log Server<br>192.168.1.5 |
| | DMZ2 | Log Server<br>192.168.1.5 |
| | Firewall | Log Server<br>192.168.1.5 |
| Radius-auth (udp/1645) | RAS<br>192.168.2.2 | ACE/Server<br>192.168.1.6 |
| Radius-acctg (udp/1646) | RAS<br>192.168.2.2 | ACE/Server<br>192.168.1.6 |

The following table lists all the required proxies that need to be configured on GIAC Firewall:

| **Proxy** | **Port** | **Source** | **Destination** | **Remarks** |
|---|---|---|---|---|
| HTTP | 80 | ALL_EXTERNAL | FIREWALL | SmartProxy Servers are: www and biztalk |
| | | dec4_NETWORK | ALL_EXTERNAL | From Internal network to Internet |
| | | dec4_NETWORK | 10.100.1.2 | From Internal network to Web Server |
| SSL | 443 | ALL_EXTERNAL | FIREWALL | SmartProxy Servers are: www and biztalk |
| | | dec4_NETWORK | ALL_EXTERNAL | From Internal network to Internet |
| | | dec4_NETWORK | 10.100.1.2 | From Internal network to Web Server |
| FTP | 21 | dec4_NETWORK | ALL_EXTERNAL | From Internal network to Internet |
| SMTP | 25 | ALL_EXTERNAL | FIREWALL | SmartProxy Server is mail (Mail Relay) |
| | | 10.100.1.4 | ALL_EXTERNAL | From Mail relay to Internet |
| | | 192.168.1.2 | 10.100.1.4 | From Internal Mail Server to Mail Relay |
| Port Guard | 22 (SSH) | ALL_EXTERNAL | FIREWALL | SmartProxy Server is sftp (SSH Server) |
| | | dec4_NETWORK | 10.100.1.3 | From Internal network to SSH Server |
| | | 192.168.1.11 | xx.yy.zz.1 | From Management Workstation 1 to Router |
| | | 192.168.1.12 | xx.yy.zz.1 | From Management Workstation 2 to Router |
| | | 192.168.1.11 | 10.100.1.4 | From Management Workstation 1 to Mail Relay |
| | | 192.168.1.12 | 10.100.1.4 | From Management Workstation 2 to Mail Relay |

The following table lists all the required Packet-Filtering rules that need to be configured on GIAC Firewall:

| Service | Port | Source | Destination | Remarks |
|---|---|---|---|---|
| MS SQL Server | tcp/1433 | 10.100.1.2 | 192.168.1.3 | From Web Server to Database Server |
| | | 10.100.2.2 | 192.168.1.3 | From BizTalk to Database Server |
| MS Exchange Server | tcp/6001, tcp/6002 | 192.168.2.64/26 | 192.168.1.2 | From RAS users to Internal Mail Server |
| MS Terminal Service | tcp/3389 | 192.168.1.11 | dec1_NETWORK | From Management Workstation 1 to DMZ1 |

| | | | | |
|---|---|---|---|---|
| | | 192.168.1.11 | dec2_NETWORK | From Management Workstation 2 to DMZ1 |
| | | 192.168.1.12 | dec1_NETWORK | From Management Workstation 2 to DMZ1 |
| | | 192.168.1.12 | dec2_NETWORK | From Management Workstation 2 to DMZ2 |
| | | 192.168.2.64/26 | 192.168.1.4 | From RAS users to Terminal Server |
| NTP | udp/123 | xx.yy.zz.1 | 192.168.1.5 | From Border Router to Log Server |
| | | dec1_NETWORK | 192.168.1.5 | From DMZ1 to Log Server |
| | | dec2_NETWORK | 192.168.1.5 | From DMZ2 to Log Server |
| syslog | udp/514 | xx.yy.zz.1 | 192.168.1.5 | From Border Router to Log Server |
| | | dec1_NETWORK | 192.168.1.5 | From DMZ1 to Log Server |
| | | dec2_NETWORK | 192.168.1.5 | From DMZ2 to Log Server |
| | | FIREWALL | 192.168.1.5 | From Firewall to Log Server |
| Radius-auth | udp/1645 | 192.168.2.2 | 192.168.1.6 | From RAS to ACE/Server |
| Radius-acctg | udp/1646 | 192.168.2.2 | 192.168.1.6 | From RAS to ACE/Server |

Split DNS is implemented on GIAC Firewall. The Public Name Server is a forwarder that forwards all DNS request to a GIAC's ISP DNS Servers (which are authoritatives for GIAC's domain, giac.com). The Private Name Server hosts GIAC's internally used domain giacent.com.

The following is an excerpt from the Firewall Packet Filter Rules Configuration File (netguard.conf).

```
##############################################################################
#
#       Internet Protocol Packet Filter Rules Configuration File
#
##############################################################################
#
##############################################################################
#
# Select any alternative from each column.
#
# Action service/protocol Frm host/subnetmask To host/subnetmask  Options
# ====== ===============  =================== ==================  ===========
#
# PERMIT service/protocol INTERNAL_NETWORK    INTERNAL_NETWORK    ENABLE_REPLY
# DENY   service          EXTERNAL_NETWORK    EXTERNAL_NETWORK    DONT_AUDIT
# PROXY  ALL              LOCAL_HOST          LOCAL_HOST          TIME_OUT=nnn
#        ALL/protocol     EVERYONE            EVERYONE            NO_IF_CHECK
#                         if_NETWORK          if_NETWORK          TCPSYNFLD
#                         nnn.nnn.nnn.nnn     nnn.nnn.nnn.nnn     TCPSYNFLD_TIMEOUT=nnn
#                         nnn.nnn.nnn.nnn/subnet nnn.nnn.nnn.nnn/subnet
#
##############################################################################
##############################################################################
```

```
#
#
# EXAMPLES
#
# Allow ping / echo packets
#
#permit echo/icmp      EVERYONE       EVERYONE       ENABLE_REPLY
#permit echo/udp       EVERYONE       EVERYONE       ENABLE_REPLY
#
#
include /etc/security/firewall/ng_inet/netguard.include
########################################################################
# The following line is used to locate the end of the header comments.
# DO NOT DELETE OR MODIFY THIS LINE.
# Place site-specific rules here, above the rules that are generated
# automatically by the firewall administrative interface.
########################################################################

# Allow all machines on the internal network to connect to Web Server
# using http and https
permit  http/tcp      internal_NETWORK      10.100.1.2
permit  https/tcp     internal_NETWORK      10.100.1.2

# Allow internal mail server to connect to Mail Relay
# using smtp
permit  smtp/tcp      192.168.1.2    10.100.1.4

# Allow all machines on the internal network to connect to SSH Server
# using SSH
permit  22/tcp        internal_NETWORK      10.100.1.3

# Allow Management Workstations to connect to Border Router and Mail Relay
# using SSH
proxy   22/tcp        192.168.1.11          xx.yy.zz.1
proxy   22/tcp        192.168.1.12          xx.yy.zz.1
permit  22/tcp        192.168.1.11          10.100.1.4
permit  22/tcp        192.168.1.12          10.100.1.4

# Allow Management Workstations to connect to Firewall
# using SSL (Tarantella)
permit  https/tcp     192.168.1.11          192.168.1.1
permit  https/tcp     192.168.1.12          192.168.1.1

# Allow Web Server and BizTalk Server to connect to Database Server
# using MS-SQL-Server service
permit  1433/tcp      10.100.1.2            192.168.1.3
permit  1433/tcp      10.100.2.2            192.168.1.3

# Allow Management Workstations to connect to DMZ1 and DMZ2
# using MS Terminal Service
permit  3389/tcp              192.168.1.11          dec1_NETWORK
permit  3389/tcp              192.168.1.12          dec1_NETWORK
permit  3389/tcp              192.168.1.11          dec2_NETWORK
permit  3389/tcp              192.168.1.12          dec2_NETWORK

# Allow RAS Users to connect to Terminal Server
# using MS Terminal Service
permit  3389/tcp              192.168.2.64/26       192.168.1.4

# Allow RAS Users to connect to Internal Mail Server
# using 6001/tcp and 6002/tcp
permit  6001/tcp              192.168.2.64/26       192.168.1.2
permit  6002/tcp              192.168.2.64/26       192.168.1.2

# Allow Border Router, RAS, DMZ1 machines, and DMZ2 machines to contact NTP Server
# using NTP queries

permit  123/udp       xx.yy.zz.1     xx.yy.zz.9     ENABLE_REPLY
permit  123/udp       192.168.2.2    192.168.1.5    ENABLE_REPLY
permit  123/udp       dec1_NETWORK   192.168.1.5    ENABLE_REPLY
permit  123/udp       dec2_NETWORK   192.168.1.5    ENABLE_REPLY
```

```
# Allow logging to be sent to Log Server from Border Router, RAS, DMZ1, DMZ2
# using syslog
permit  514/udp        xx.yy.zz.1     xx.yy.zz.9
permit  514/udp        192.168.2.2    192.168.1.5
permit  514/udp        dec1_NETWORK   192.168.1.5
permit  514/udp        dec2_NETWORK   192.168.1.5

# Allow radius authentication and accounting to be sent from RAS to ACE/Server
# usning radius-auth and radius-acctg
permit  1645/udp       192.168.2.2    192.168.1.6    ENABLE_REPLY
permit  1646/udp       192.168.2.2    192.168.1.6    ENABLE_REPLY

# Allow GIAC’s Partner to communicate to DMZ2 in both directions
# using http and https
# via Gateway-to-Gateway VPN between GIAC Firewall and Partner’s Firewall
permit  http/tcp       172.16.0.0/24  10.100.2.0/28   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto
permit  http/tcp       10.100.2.0/28  172.16.0.0/24   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto
permit  https/tcp      172.16.0.0/24  10.100.2.0/28   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto
permit  https/tcp      10.100.2.0/28  172.16.0.0/24   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto

#
# DO NOT DELETE OR MODIFY THE FOLLOWING LINE.
# DO NOT DELETE: The following rules are added during initial boot.
# These rules allow any internal machine to ping the internal interface
# of the firewall available from to its respective network.  They are only
# uncommented for network troubleshooting situations.
# permit       echo/icmp      ALL_INTERNAL   FIREWALL        ENABLE_REPLY
# permit       echo/icmp      FIREWALL       ALL_INTERNAL    ENABLE_REPLY
# DO NOT DELETE: The above rules are added during initial boot.

# Automatically-generated rules added here.

# SMTP proxy rules (added automatically)
# Proxy parameters (smtp): inToFirewall outThruFirewall
# Allow mail from Internet to be sent to Mail Relay
# using smtp proxy
# TCP Syn Flood Defense is enabled.
proxy   smtp/tcp       ALL_EXTERNAL   FIREWALL        TCPSYNFLD TCPSYNFLD_TIMEOUT=10
permit  smtp/tcp       FIREWALL       10.100.1.4

# Allow Mail Relay to send mail to Internet
# using smtp proxy
proxy   smtp/tcp       10.100.1.4     ALL_EXTERNAL

# End of SMTP proxy rules

# FTP proxy rules (added automatically)
# Proxy parameters (ftp): inToFirewall outThruFirewall
# Allow internal network to connect to Internet
# using ftp proxy
proxy   ftp/tcp        dec4_NETWORK   ALL_EXTERNAL
# End of FTP proxy rules

# Auditlogd Syslog rules (added automatically)
# Allow firewall to send syslog messages Log Server
# using syslog
permit  514/udp        FIREWALL       192.168.1.5
# End of Auditlogd Syslog rules

# Split DNS rules (added automatically)
# Allow DNS queries. Zone transfers are not allowed.
# TCP Syn Flood defense is enabled for DNS requests from Internet
permit  domain/tcp     ALL_EXTERNAL   EXTERNAL_INTERFACES    TCPSYNFLD
TCPSYNFLD_TIMEOUT=10
permit  domain/tcp     EXTERNAL_INTERFACES   ALL_EXTERNAL
permit  domain/udp     ALL_EXTERNAL   EXTERNAL_INTERFACES    ENABLE_REPLY
permit domain/udp    EXTERNAL_INTERFACES  ALL_EXTERNAL   ENABLE_REPLY
permit domain/tcp    ALL_INTERNAL  INTERNAL_INTERFACES
permit domain/tcp    INTERNAL_INTERFACES  ALL_INTERNAL
permit domain/udp    ALL_INTERNAL  INTERNAL_INTERFACES   ENABLE_REPLY
permit domain/udp    INTERNAL_INTERFACES  ALL_INTERNAL   ENABLE_REPLY
deny   domain/tcp    EVERYONE      EVERYONE
deny   domain/udp    EVERYONE      EVERYONE
# End of Split DNS rules

# SSL proxy rules (added automatically)
# Proxy parameters (ssl): inToFirewall outToFirewall outThruFirewall
# Allow access to Web Server and BizTalk Server
# using SSL proxy
# TCP Syn Flood defense is enabled.
proxy  https/tcp     ALL_EXTERNAL  FIREWALL       TCPSYNFLD TCPSYNFLD_TIMEOUT=10
permit https/tcp     FIREWALL      10.100.1.2
permit https/tcp     FIREWALL      10.100.2.2
# Allow internal network to access the Internet
# using SSL proxy
proxy  https/tcp     dec4_NETWORK  ALL_EXTERNAL
# End of SSL proxy rules

# HTTP proxy rules (added automatically)
# Proxy parameters (http): inToFirewall outThruFirewall
# Allow access to Web Server and BizTalk Server
# using HTTP proxy
# TCP Syn Flood defense is enabled.
proxy  80/tcp ALL_EXTERNAL  FIREWALL       TCPSYNFLD TCPSYNFLD_TIMEOUT=10
permit 80/tcp FIREWALL      10.100.1.2
permit 80/tcp FIREWALL      10.100.2.2
# Allow internal network to access the Internet
# using HTTP proxy
proxy  80/tcp dec4_NETWORK  ALL_EXTERNAL
# End of HTTP proxy rules

# Port Guard proxy rules (added automatically)
# Proxy parameters: inToFirewall outThruFirewall
# Allow SSH from Internet to SSH Server
# using generic pass-through proxy
# TCP Syn Flood Defense is enabled.
proxy  22/tcp ALL_EXTERNAL  FIREWALL       TCPSYNFLD TCPSYNFLD_TIMEOUT=10
permit 22/tcp FIREWALL      10.100.1.3
# End of Port Guard proxy rules

# End of automatically generated rules.
#
# This deny rule should always be the last rule.
#
deny   ALL    EVERYONE      EVERYONE       ENABLE_REPLY
```

Notes (taken from Cyberguard Firewall Manual):

- Cyberguard offers protection against TCP Syn Flood attacks. The TCP Syn Flood attack is a denial-of-service attack that exploits the TCP connection establishment protocol. Cyberguard Firewall circumvents these attacks by intercepting the SYN segment and responds to the client with a SYN/ACK. It then waits the specified timeout period for the return ACK from the client to complete the TCP handshake. If the firewall does not receive a return ACK, it drops the packet. If the firewall receives a return ACK, it establishes a connection with the requested server and forwards the original connection request.segment. TCP Syn Flood defense is enabled by TCPSYNFLD keyword in the filtering rules.

- Cyberguard enables keeping state for UDP protocol by ENABLE_REPLY keyword in the filtering rules.

## 2.3 VPN Policy

Cyberguard VPN is based on IPSEC (IP Security). To establish a Gateway-to-Gateway VPN connection between GIAC and Partner's network, two Cyberguard Firewall/VPN appliances will be used. This decision is made to minimize potential of connectivity, security, and support issues.

The rules for the site-to-set VPN connection between GIAC and IndoFortunes Inc. are specified in the Packet Filter Rules Configuration File (netguard.conf).

```
# Allow GIAC's Partner to communicate to DMZ2 in both directions
# using http and https
# via Gateway-to-Gateway VPN between GIAC Firewall and Partner's Firewall
permit  http/tcp       172.16.0.0/24  10.100.2.0/28   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto
permit  http/tcp       10.100.2.0/28  172.16.0.0/24   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto
permit  https/tcp      172.16.0.0/24  10.100.2.0/28   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto
permit  https/tcp      10.100.2.0/28  172.16.0.0/24   ENABLE_REPLY ipsec=HighSecurity:sa-
per-net:0x2:auto:auto
```

## 2.4 Gateway-to-Gateway VPN Tutorial

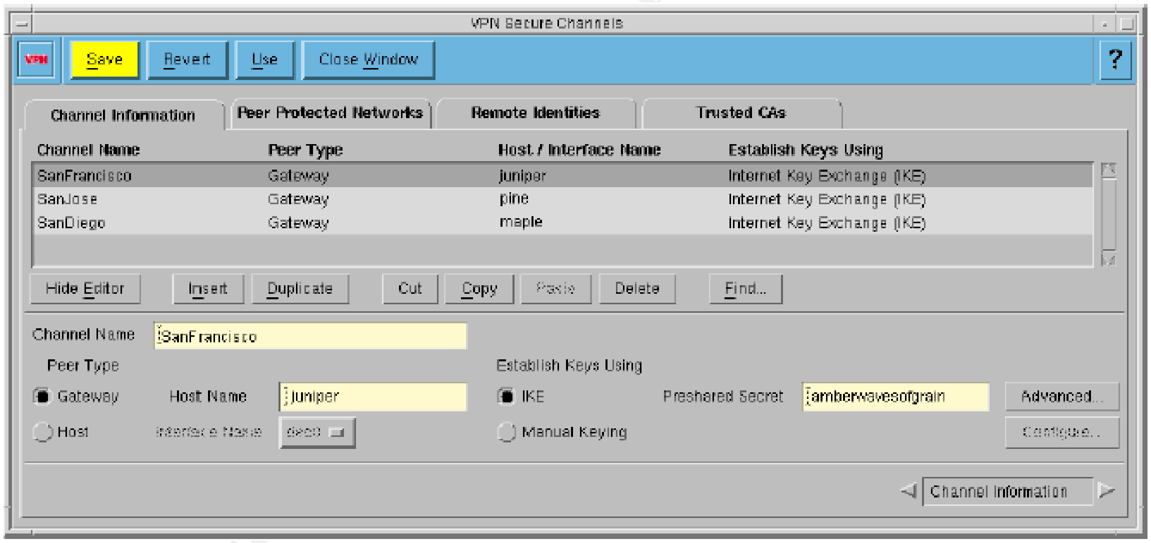
Cyberguard refers to VPN connections as "secure channels". This section describes a step-by-step guide in creating a secure channel between GIAC and its Partner network. This guide is excerpted from Cyberguard Firewall Manual: Configuring the Cyberguard Firewall (Release 5.0). The complete manual can be downloaded from ftp://ftp.cybg.com/Unix/5.0/Doc/Manual/

### 2.4.1 Create a Secure Channel to the Peer Gateway

First we need to define a channel to the IPSec peer that the CyberGuard VPN will communicate with.

- Select *Configuration* from the Control Panel.
- Select *VPN Secure Channels*. The VPN Secure Channels window appears.
- Click on the *Channel Information* tab. The Channel Information page appears.
- Click on *Show Editor*. The expanded Channel Information page appears.
- Click on *Insert* to begin creating a new secure channel.

- Type *IndoFI* (for IndoFortunes Inc.) in the *Channel Name* field.
- Select *Gateway* as the *Peer Type*.
- Type in Peer Gateway’s external IP address *bb.bb.bb.1* in the *Host Name* field.
- Select *IKE* (Internet Key Exchange, the key management protocol for IPSec) in the *Establish Keys Using* selection box.
- Type a <secret phrase> in the *Preshared Secret* field. Administrators of GIAC and IndoFortunes Inc. must have agreed upon a secret phrase, which must be entered on both gateways.
- Click on the *Advanced* button next to the *Preshared Secret* field.
- Check the *Use Identity* checkbox under the *Preshared Secret*.
- Under *IKE Data*, select *HighSecurity* in the *IKE Protection Strategy* list box.



| Channel Name | Peer Type | Host / Interface Name | Establish Keys Using |
|---|---|---|---|
| SanFrancisco | Gateway | juniper | Internet Key Exchange (IKE) |
| SanJose | Gateway | pine | Internet Key Exchange (IKE) |
| SanDiego | Gateway | maple | Internet Key Exchange (IKE) |

Channel Name: SanFrancisco

Peer Type: ● Gateway ○ Host

Host Name: juniper

Interface Name: dec0

Establish Keys Using: ● IKE ○ Manual Keying

Preshared Secret: amberwavesofgrain

*Figure 2. VPN Secure Channels Configuration Window*

*(This screenshot is taken from Cyberguard Firewall Manual.*
*It does not reflect the configuration described in this assignment)*

### 2.4.2 Identify Networks Protected by the Peer Gateway

Because the peer is a gateway, the next step is to identify the networks of interest that are protected by this peer.

- Click on the *Peer Protected Networks* tab of the VPN Secure Channels window.
- In the *VPN Secure Channels* list on the left side of the page, select *IndoFI*.
- Click on *Show Editor*.
- Click on *Insert*.
- In the *Network Address* field, type *172.16.0.0/255.255.255.0*.

### 2.4.3 Define Packet Filtering Rules

In this step, we will define packet-filtering rules that will be protected using IPSec and the newly defined VPN Secure Channel.

- Select *Configuration* from the Control Panel.
- Select *Packet-Filtering Rules*. The Packet-Filtering Rules window appears.
- Click on *Show Editor*. The expanded window appears.
- Click on the *Basic* tab. The Basic page appears.
- Enter the following rules:

```
permit  http/tcp   172.16.0.0/24   10.100.2.0/28
permit  http/tcp   10.100.2.0/28   172.16.0.0/24
permit  https/tcp  172.16.0.0/24   10.100.2.0/28
permit  https/tcp  10.100.2.0/28   172.16.0.0/24
```

- Select the rule and check the *Protect using IPSec* option.
- Select the *IPSec* tab.
- Select *HighSecurity* in the *IPSec Protection Strategy* list box.
- Click *Save*. Then click *Use* to apply changes immediately.

# 3. Assignment 3 – Verify the Firewall Policy

## 3.1 Planning the Audit

In order to verify that the security policy is correctly enforced on GIAC's primary firewall, a technical audit is planned. In order to examine the firewall policy, the following approach will be used:

- The objective of this audit is to verify GIAC Firewall Policy. It is not the intention of this audit to discover vulnerabilities on GIAC Servers/devices.
- NmapWin v1.3.1 (a Windows 2000/XP front-end for nmap v3.00) is selected due to its various types of scans and ease of use.
- After we test to make sure that normal Ping (ICMP echo request) does not work through the Firewall (because we didn't allow it), we will use "No Ping" options (-P0) to allow the scanning of networks that don't allow ICMP echo requests (or responses).
- A series of scans will be conducted from each network segment of the Firewall to other segments. These scans will include:
  - Connect Scan: We will use the connect() system call to open a connection to every port in the specified range on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable.
  - SYN Scan: This scan sends a SYN packet and wait for a response. A SYN|ACK indicates the port is listening. A RST indicates a non-listener. We believe this scan will not show anything more than the TCP Connect Scan. However, it may be useful to test Cyberguard Syn Flood Alert that is configured on the Firewall.
  - ACK Scan: This advanced method should be able to determine whether GIAC firewall is stateful or just blocks incoming SYN packets. This scan sends an ACK packet to the ports specified. If a RST comes back, the port is "unfiltered". If nothing comes back (or if an ICMP unreachable is returned), the port is classified as "filtered".
  - UDP Port Scan: We will send 0 byte udp packets to each port in the specified range on the target machine. If an ICMP port unreachable message is received, the port is closed. Otherwise we assume the port is open.

The assessment will start on Sunday morning 8:00 AM. GIAC users, Suppliers, and Partner are all informed about this assessment and have been requested to avoid working during that day. GIAC estimated the assessment should be finished in less than 12 hours and GIAC site can go back online on Sunday evening. The resources required for the assessment are 2 (two) GIAC System Adminsitrators overseen by the IT Manager.

Prior to audit, full backup will done on all systems and configurations. If a system fails during/after the audit, recovery will require 6 hours (maximum). Therefore at the latest, all systems can be brought back for operations at 2:00 AM Monday morning (the latest). All vendors are also informed about this planned assessment and are asked to stand-by for support in case of emergency.

## 3.2 Conducting the Audit

### 3.2.1 Access from External Network

Test Workstation is connected to the External segment network and assigned IP address of xx.yy.zz.3 subnet mask 255.255.255.248 with default gateway pointing to xx.yy.zz.2 (Firewall's External interface).

- Ping Test:

```
ping xx.yy.zz.2
Request timeout
Request timeout
Request timeout
```

Ping test on the Firewall failed.

- TCP Connect Scan

```
nmap -sT -P0 -p 1-65535 -v -T 3 xx.yy.zz.2

nmap -sT -P0 -p 1-65535 -v -T 3 xx.yy.zz.9
```

The results are as follows:

| IP address | Open Ports |
|---|---|
| xx.yy.zz.2 | 22/tcp, 25/tcp, 80/tcp, 443/tcp |
| xx.yy.zz.9 | - |

- TCP SYN Scan

```
nmap -sS -P0 -p 1-65535 -v -T 3 xx.yy.zz.2

nmap -sS -P0 -p 1-65535 -v -T 3 xx.yy.zz.9
```

TCP SYN Scan did not reveal more services. Cyberguard Firewall were able to detect TCP SYN flood and send log messages to to the Log Server.

- ACK Scan

```
nmap -sA -P0 -p 1-65535 -v -T 3 xx.yy.zz.2

nmap -sA -P0 -p 1-65535 -v -T 3 xx.yy.zz.9
```

ACK Scan did not reveal more services. But we tested to run MS Terminal Service on the Log Server; and if the Firewall was a static filter, ACK packets would have gone through to Log Server's Terminal Service (listening on port 3389). This proves the Firewall to be stateful.

- UDP Port Scan

```
nmap -sU -P0 -p 1-65535 -v -T 3 xx.yy.zz.2

nmap -sU -P0 -p 1-65535 -v -T 3 xx.yy.zz.9
```

The results are as follows:

| IP address | Open Ports |
|---|---|
| xx.yy.zz.2 | 53/udp |
| xx.yy.zz.9 | 123/udp, 514/udp |

### 3.2.2 Access from Remote Access Server

We disconnected Remote Access Server and replace it with Test Workstation. It is assigned IP address of 192.168.2.2 subnet mask 255.255.255.248 with default gateway pointing to 192.168.2.1 (Firewall's Remote Access network interface). From Test Workstation, we tried scanning servers in DMZ1, DMZ2, and Internal Network.

The results are as follows:

| Network Segment | IP address | Open Ports |
|---|---|---|
| DMZ1 | - | - |
| DMZ2 | xx.yy.zz.9 | 123/udp, 514/udp |
| Internal Network | 192.168.1.5 | 123/udp, 514/udp |
|  | 192.168.1.6 | 1645/udp, 1646/udp |

Note: Internal Mail Server (Exchange Server) and Terminal Server were not found open because the Firewall Policy only allow connections to them coming from RAS Clients (192.168.2.64/26).

### 3.2.3 Access from DMZ1

We disconnected Web Server and replace it with Test Workstation. It is assigned IP address of 10.100.1.2 subnet mask 255.255.255.240 with default gateway pointing to 10.100.1.1 (Firewall's DMZ1 network interface). From Test Workstation, we tried scanning servers in Remote Access segment, DMZ2, and Internal Network.

The results are as follows:

| Network Segment | IP address | Open Ports |
|---|---|---|
| Remote Access | - | - |
| DMZ2 | - | - |
| Internal Network | 192.168.1.5 | 123/udp, 514/udp |
|  | 192.168.1.3 | 1433/tcp |

### 3.2.4 Access from DMZ2

We disconnected BizTalk Server and replace it with Test Workstation. It is assigned IP address of 10.100.2.2 subnet mask 255.255.255.240 with default gateway pointing to 10.100.2.1 (Firewall's DMZ2 network interface). From Test Workstation, we tried scanning servers in Remote Access segment, DMZ1, and Internal Network.

The results are as follows:

| Network Segment | IP address | Open Ports |
|---|---|---|
| Remote Access | - | - |
| DMZ1 | - | - |
| Internal Network | 192.168.1.5 | 123/udp, 514/udp |
|  | 192.168.1.3 | 1433/tcp |

### 3.2.5 Access from Internal Network

We disconnected Internal Mail Server and replace it with Test Workstation. It is assigned IP address of 192.168.1.2 subnet mask 255.255.255.0 with default gateway pointing to 192.168.1.1 (Firewall's DMZ2 network interface). From Test Workstation, we tried scanning servers in Remote Access segment, DMZ1, and DMZ2.

The results are as follows:

| Network Segment | IP address | Open Ports |
|---|---|---|
| Remote Access | - | - |
| DMZ1 | 10.100.1.4 | 25/tcp |
| DMZ2 | - | - |

## 3.3 Audit Results and Analysis

GIAC Firewall were functioning properly in enforcing the Firewall's security policy. The following are some points noted:

- Firewall logging facility performed properly. It accurately recorded the audit activities. It was also able to detect TCP SYN scan and generate alerts on it as configured.
- The unsusccessful ACK scan proves the firewall's statefulness to be valuable.

GIAC's current architecture has some opportunity for improvements. The following are some points regarding future enhancements:

- A good alternative architecture is to have two-layer of Firewalls (see diagram below) to separate External Network and Internal Network, and place Proxy Servers (and Reverse Proxy Servers) in the Service Network between those two Firewalls. Therefore we can truly enforce to "never allow direct connection from the External Network to the Internal Network". GIAC should also consider creating an isolated network for Internal Servers to control access to them from internal users/workstation.

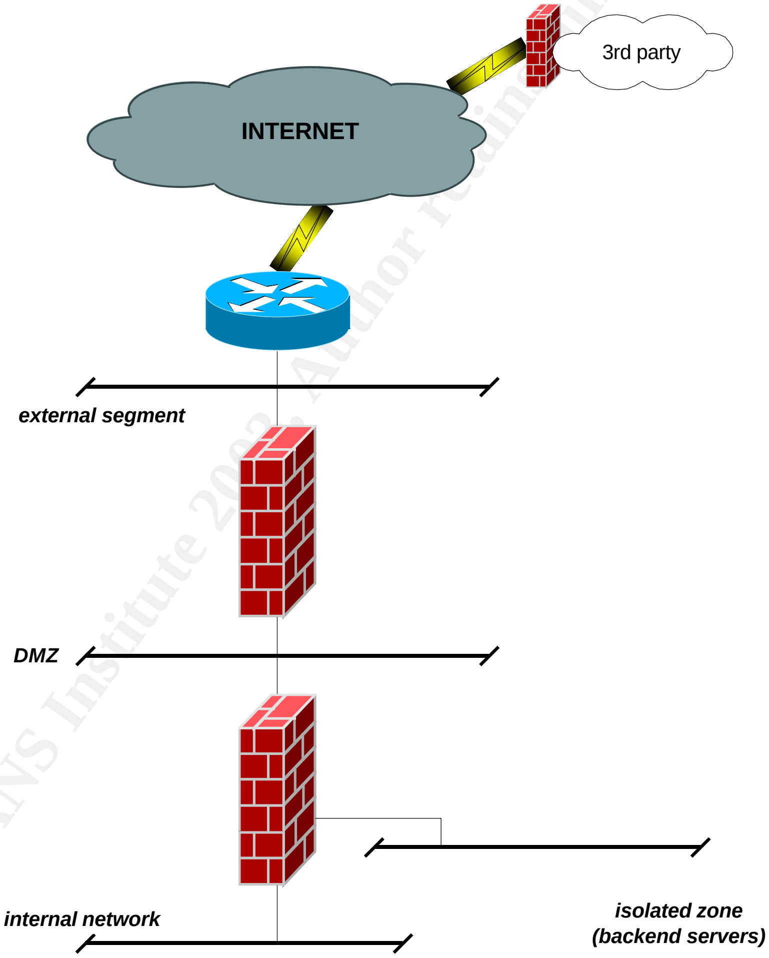


*Figure 3. Alternative Architecture*

- To avoid a single-point-of-failure, GIAC might also want to consider a redundant/HA architecture should the cost/benefit justify for it.

# 4. Assignment 4 – Design Under Fire

I selected Greg Surla's practical assignment posted in September 2002. http://www.giac.org/practical/Greg_Surla_GCFW.doc. The following is the network architecture diagram.

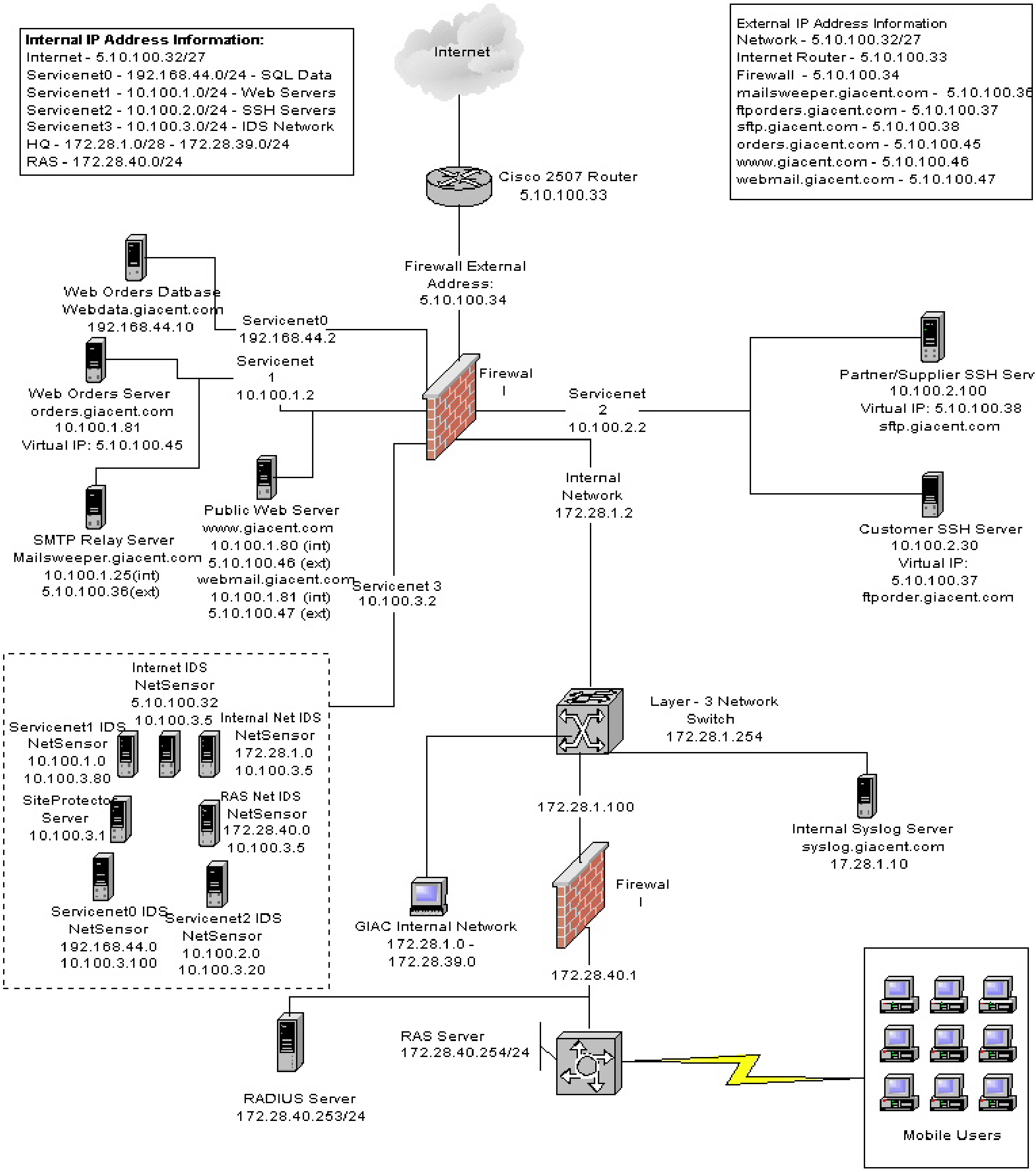


*Figure 4. Greg Surla's Network Diagram*

## 4.1 Attack Against the Firewall

The primary firewall of Greg Surla’s design is Symantec Enterprise Firewall (formally known as Axent’s Raptor) version 7.0. This firewall is running on a Windows 2000 Server machine.

After conducting a research, a security vulnerability was found reported on an advisory from Symantec Security Response dated October 13, 2002. This vulnerability was first discovered by a Scandinavian security consultancy firm, Advanced IT-Security (http://www.ai-sec.dk/). Their original advisory can be found at http://online.securityfocus.com/archive/1/295152.

The security vulnerability poses a denial-of-service (DoS) issue with the web proxy component in the Symantec Enterprise Firewall. A malicious user who can establish a remote connection to the proxy server could cause the proxy server to timeout for an extended period of time by requesting multiple connections to a non-existent or erroneous internal URL. During this timeout, the server will be unable to process further connection requests.

Symantec’s Response to this advisory can be found at http://securityresponse.symantec.com/avcenter/security/Content/2002.10.11.html . Software patches are currently available for download from Symantec Enterprise Support Site (http://www.symantec.com/techsupp/)

The primary firewall in Greg Surla’s design utilizes the proxy server discussed in the above mentioned advisories. To exploit the vulnerability, an attacker could try to connect to the published IP addresses of GIAC web servers and issue a HTTP-style CONNECT to a domain with a missing or erroneous DNS-server. The Proxy Server will wait for timeout (usually up to 300 seconds). Sending further requests for other hostnames in the same crooked domain will make the Proxy Server unavailable for porcessing requests. It has been reported that this exploit works regardless if the domainname in question is allowed or not in the firewall rules.

## 4.2 Denial of Service (DoS) Attack

50 cable modem/DSL systems have been compromised with TFN2K (Tribe FloodNet 2K) servers installed. TFN2K is a client-server tool that can be used to launch a distributed denial-of-service (DDoS) attack. The following is quoted from a paper titled “TFN2K – An Analysis” by Jason Barlow and Woody Thrower (http://www.packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt).

> “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."

We begin by installing TFN2K client (the master) on my Linux laptop and prepare a text file (addresslist) containing the 50 IP addresses of compromised hosts with TFN2K servers.

We can then execute the following command on TFN2K client machine (my laptop) to launch the attack from those 50 servers. For example:

```
./tfn –f addresslist –i www.giac.com –p 80 –c 5
```

The above command launches a TCP SYN flood to destination port 80 of victim www.giac.com from all servers in the addresslist file.

Countermeasures that can be put into place to mitigate this attack are as follows:

- If your firewall has a SYN Flood Defense feature (e.g. Cyberguard Firewall's SYN Flood Defense, Checkpoint Firewall-1's SYN Defender), enable it on your publicly accessible services.
- Set up a network intrusion detection system that will update Border Router's access-list to drop packets coming from the 50 attackers.
- If possible, implement OS level protection from TCP SYN attacks. (e.g. MS Windows 2000 can be configured using registry edit to detect TCP SYN attacks).

## 4.3 Attack Against an Internal System

The Customer SSH Server (ftporders.giac.com) is running on alternate service port number (tcp/1984). Due to the recently publicized SSH vulnerabilities found on many SSH implementations, a disgruntled customer (who knows the SSH Server's port number) may be taunted to play around.

SANS Critical Vulnerability Analysis Vol 1 No 22 noted that these vulnerabilities pose risks of remote root/SYSTEM-level compromise of SSH servers, SSH client compromise, and denial of service.

The malicious user can download an automated tool called SSHredder, which is SSH Protocol Test Suite to test against SSH2 vulnerabilities as described in an advisory published by Rapid7 on December 16, 2002 (http://www.rapid7.com/advisories/R7-0009.txt). It contains test packets in binary form (PDU file).

This malicious user can then create a client program using netcat to connect to port 1984 (the port number where Customer SSH Server runs) and send a PDU file. He/she can continue to test sending each PDU to the SSH Server.

However, we know that this attack will no succeed because the Customer SSH Server is OpenSSH 3.4p1, which is among the few implementations that are not affected by these vulnerabilities.

## References

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

CyberGuard Firewall FS Series Data Sheet
http://www.cyberguard.com/PDF/datasheet_FS_5_1.pdf

CyberGuard Firewall Manual
ftp://ftp.cybg.com/Unix/5.0/Doc/

RSA SecurID ACE/Server Data Sheet
http://www.rsasecurity.com/products/securid/datasheets/dsace50.html

Nmap network security scanner man page
http://www.insecure.org/nmap/data/nmap_manpage.html

Advanced IT-Security Advisory #01-10-2002: Multiple Symantec Firewall Secure Webserver timeout DoS
http://online.securityfocus.com/archive/1/295152

Symantec Security Response Advisory: Symantec Firewall Secure Webserver timeout DoS
http://securityresponse.symantec.com/avcenter/security/Content/2002.10.11.html

TFN2K - An Analysis
http://www.packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt

Greg Surla GCFW Practical Assignment
http://www.giac.org/practical/Greg_Surla_GCFW.doc

Rapid 7 Advisory R7-0009: Vulnerabilities in SSH2 Implementations from Multiple Vendors
http://www.rapid7.com/advisories/R7-0009.txt