Global Information Assurance Certification Paper

SANS GIAC Certified Firewall Analyst

Practical Assignment Version 2.0

Protecting Internet Fortune Cookies

By

Eu Jin, Justin Ng

24 October 2003

Table of Contents

Abstract

This paper examines the firewall and perimeter security for a GIAG Enterprises, which deals with bulk sales of fortune cookies sayings as part of the GIAC Certified Firewall Analyst practical assignment 2.0. The paper consists of four parts:

- Develop GIAC Enterprises' network security architecture, taking into considerations the needs of different parties that deals with GIAC.
- Define the security policy for GIAC Enterprises border router, firewall and VPN components.
- Validate the firewall policy to verify if the policies are correctly enforced.
- Examine the options to attack another network design.

Assignment 1 – Security Architecture

Introduction

GIAC Enterprises has been dealing with Fortune Cookies in the local market for over two years. It has recently decided to move its business online to reduce business costs and delivery time to customers. At the same time, GIAC Enterprises aims to reach the global fortune cookies market. To maintain low startup and operating costs, all connections outside of GIAC Enterprises office are performed via the Internet.

The requirements set out by the management for the online system include:

- Easy to access and used by business partners, suppliers, customers and public
- Provide security for network and IT resources
- Minimize investments required by stake-holders

Access Requirements

The connection parties to GIAC Enterprises includes:

- Online bulk purchases by customers
- Suppliers to be able to send fortune cookies sayings to GIAC Enterprises
- Partners who translates and resells GIAC Enterprises fortune cookie sayings
- GIAC Enterprises employees in the internal network
- GIAC Enterprises mobile sales force that should be able to access the sales applications and e-mail
- The general public to obtain general information on GIAC Enterprises

Customers

Customers connect to the GIAC Enterprises Web page to make their fortune cookie sayings purchases. Customers access the web application to make bulk purchases of fortune cookie sayings.

Ease of access is important to the customers. Therefore, SSL is used to protect the customers' personal information and access passwords.

Suppliers

Suppliers are companies or individuals who provide GIAC Enterprises with new fortune cookies sayings to supplement the in-house produced sayings. Suppliers submit new sayings to GIAC Enterprises in bulk via SSL web pages.

Suppliers' particulars, passwords and fortune cookies sayings are considered confidential and must be protected from unauthorized access. SSL is used to encrypt all transactions between the Suppliers and the External Web server.

Partners

Partners translate and resell GIAC Enterprises fortune cookies sayings. Partners connect to GIAC Enterprises web application to retrieve fortune cookies sayings. A web application hosted in the External Web server has been provided for partners to transfer data using XML. All transactions between partners and GIAC Enterprises External Web server are encrypted using SSL.

Internal Employees

GIAC Enterprises have about 50 employees. Employees have access to internal servers including database, applications, file and print and e-mail. Employees are able to reach any servers in GIAC office. Access to the different applications services is granted using Windows Active Directory accounts.

Employees are provided with Windows 2000 and XP workstations. They have only user rights on the workstations to prevent them from installing unauthorized software or from modifying workstation settings. Active Directory Group Policy has been configured to deploy software to workstations in the internal network. Group Policy is also utilized to restrict users rights and configure the workstations for automatic updates to patch security vulnerabilities.

Employees are allowed to browse the Internet using HTTP, HTTPS and download files using FTP. All Internet e-mails are sent and received through the corporate mails server.

Mobile Sales Force and Teleworkers

There are around 30 mobile sales staff and teleworkers employed by GIAC Enterprises. The remote employees need access to the database, file servers and e-mail servers.

Remote employees connect to the Intranet servers to access their e-mail and file servers. Their workstations are not joined to the Windows domain. Instead, they provide their credentials when connecting to each server in the network.

The remote employees primarily use Outlook Web Access 2000 http mail to access their e-mails. However, OWA2K provides limited features and requires users to be online to read mails. Therefore, GIAC has decided to allow the remote staff to access e-mails using Microsoft Outlook (MAPI) clients via VPN.

General Public

The web server contains some web pages for the public to retrieve general information on GIAC Enterprises. The public can also contact GIAC Enterprises via e-mail. The public web site publishes e-mail addresses for the public to reach the relevant departments in GIAC Enterprises such as Sales and Public Relations.

Security Requirements

As the e-business can be conducted across the globe, GIAC requires the system to be available 7 days by 24 hours. The perimeter network should protect the system from viruses and hackers that may disrupt the business operations. To reduce downtime in the event of a hardware failure, GIAC Enterprises has purchased servers with redundant power supplies, disks and network cards.

Fortune cookies sayings are the main asset for GIAC Enterprises. In addition, GIAC Enterprises business associates and customers' information and passwords are considered confidential. Therefore, it is important that the fortune cookies sayings and online business transactions are protected from theft or modified by unauthorized parties.

GIAC Enterprises have selected Microsoft Windows platform for its network, as the IT department has strong knowledge with Microsoft products. The exception is the firewall software where Check Point Firewall-1 is selected due to its ease of use.

To protect the servers from unauthorized access, the servers are installed with the latest service packs and are patched with all relevant hotfixes. The servers have been hardened using Microsoft Windows 2003 Security Guide[1] and NSA Windows 2000 Security Guides[2].

Network Design

GIAC Enterprises network infrastructure is based on two networks segments connected to the Internet via a single firewall.

The servers accessible by external parties such as customers, suppliers, partners and other Internet users are placed in a screened or DMZ network. To avoid having all DMZ services affected by a problem in one, each server in the DMZ provides a single service. The services are Web, DNS and Mail Relay. No direct incoming connections to GIAC Enterprises internal network are allowed without strong encryption.

The firewall and the border router filter both incoming and outgoing connections from GIAC Enterprises DMZ and internal network. This is done to minimize the exposure to the Internet. In addition, servers in the DMZ network are configured with Windows 2003's Internet Connection Firewall[3]. The built-in firewall provides stateful packet

[1] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/win2003/w2003hg/sgch00.asp
[2] http://www.nsa.gov/snac/index.html
[3] http://support.microsoft.com/default.aspx?scid=317530

filtering for outgoing connections and static port filtering for incoming traffic to the network interface.

The Mobile Sales Staff and Teleworkers need to access the resources in GIAC Enterprises' network via the Internet. To reduce the risks of exposing company's data to theft or sabotage, access between the remote users and internal network is encrypted with VPN authentication and encryption. In addition, the remote employees access are restricted to the servers and protocols they require. GIAC requires the remote employees to install client firewall software to protect the PCs from being used as a stepping-stone to attack GIAC's corporate network.

Despite these measures, malicious software may still be able to penetrate the defenses. Thus, the server administrators have been advised to patch the servers for critical vulnerabilities within a week from its release.

Public IP Addressing

GIAC Enterprises has obtained 16 IP addresses from the Internet Service Provider has allocated 16 IP addresses. For this paper, the address range is specified as A.B.202.224/28. In addition, the serial interface of the border router is given as A.B.212.58/30.

Private IP Addressing

The 192.168.0.0 private IP address range, as specified in RFC 1918[4], is used for GIAC Enterprises Internal and DMZ network segments.

The IP assignment for GIAC Enterprises is shown in Table 1.

Host	Interface	Private IP	Translate Public IP Address
Router GEBR01	Serial ISP	A.B.212.58/30	N.A.
	Ethernet to Firewall	A.B.202.225/28	N.A.
Firewall GEPF01	External Interface	A.B.202.226/28	N.A.
	DMZ Interface	192.168.64.1/24	N.A.
	Internal Interface	192.168.0.1/22	N.A.
DMZ Network			
Mail Relay GDMR01	DMZ	192.168.64.31/24	Static A.B.202.227
External Web Server GDWB01	DMZ	192.168.64.32/24	Static A.B.202.228
External DNS Server GDDN01	DMZ	192.168.64.33/24	Static A.B.202.229
Internal Network			
Active Directory (PDC) GEAD01	Intranet	192.168.0.31/22	N.A.

[4] http://www.ietf.org/rfc/rfc1918.txt

Host	Interface	Private IP	Translate Public IP Address
Active Directory (DC) GEAD02	Intranet	192.168.0.32/22	N.A.
Mail Server GEEM01	Intranet	192.168.0.33/22	N.A.
Database Server GEDB01	Intranet	192.168.0.34/22	N.A.
Syslog Server GESL01	Intranet	192.168.0.35/22	N.A.
Software Update Server GESU01	Intranet	192.168.0.36/22	N.A.
Proxy Server GEPX01	Intranet	192.168.0.37/22	N.A.
Employee Workstations (DHCP)	Intranet	192.168.0.64/22 – 192.168.0.223/22	N.A.
Mobile staff & Teleworkers	Extranet	192.168.28.64/24 – 192.168.28.223/24	N.A.
Network Printers	Intranet	192.168.0.224/22 – 192.168.0.254/22	N.A.

Table 1: IP Address Assignment

Network Address Translation is used to translate private network addresses used by GIAC Enterprises network to public addresses provided by the ISP. Only DMZ servers are assigned public address using static NAT.

Internet bound connections from the internal network are dynamically NATed to allow the return packets to reach GIAC Enterprises host and at the same time, helps prevent external hosts from initiating connections to the internal network.

The border router on the external network sends syslog messages to the Syslog server in the internal network. However, it was decided that the connection is performed without any address translation the syslog server's IP address. Instead, the border router is configured to route the syslog private address to the firewall.

Figure 1 shows the network infrastructure for GIAC Enterprises.

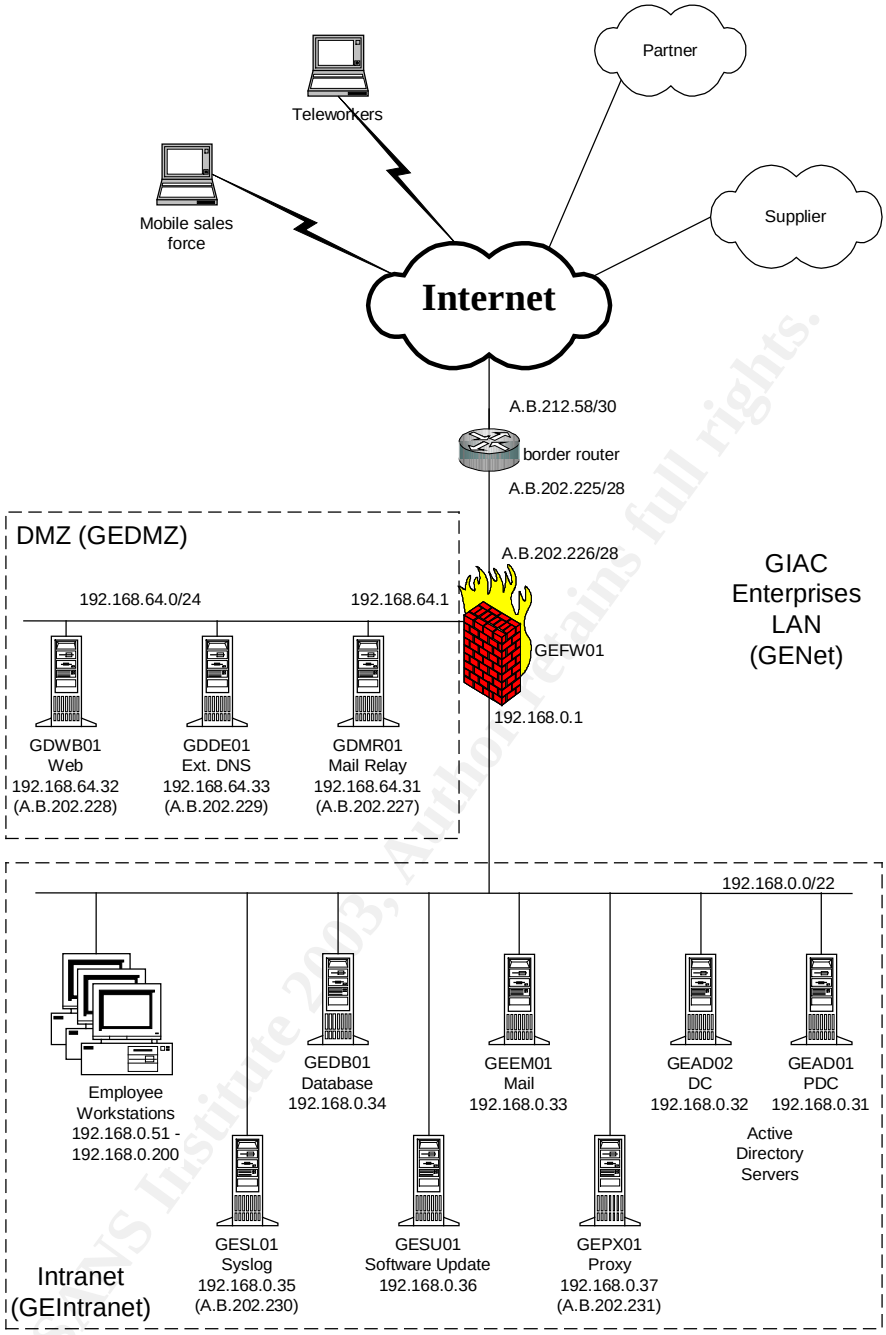


Figure 1: GIAC Enterprises Network Diagram

Hardware and Software

Border Router - GEBR01

Software: IOS 2.2T
Hardware: Cisco 2620

The border router is equipped with one serial interface and one fast Ethernet interface. It is hardened and configured to perform static ingress and egress filtering to protect itself, the firewall and the internal network.

Logs generated by the border router are sent to the syslog server in the internal network. To prevent the router being used to enter the network, the router is hardened and ACL is implemented on both of its interfaces. The router can only be managed from the console port.

Firewall - GEFW01

Software: Check Point VPN-1/Firewall-1 NG Feature Pack 3 with hotfix 2.
Hardware: Dell PowerEdge 2650 with dual Xeon 2.8GHz processors.
Operating System: Windows 2000 Server with Service Pack 4 and the latest security hotfixes. The server is installed as a stand-alone server and hardened as specified by Microsoft Windows 2003 Security Guide[5] for bastion hosts.

The firewall is managed from the server's console. The firewall is connected directly to the router using an Ethernet crossover cable and is the primary perimeter defense for GIAC Enterprises network. The server is equipped with three Fast Ethernet interfaces to create three networks segments with different trusts level.

- External interface connects to the border router
- Demilitarized zone interface connects to the protected network
- Internal interface connects to the GIAC Enterprises internal network

The firewall server provides IPSec based VPN gateway for the mobile staff and teleworkers to access the internal network. Check Point VPN utilizes the following protocols[6]:

- Internet Key Exchange (UDP Port 500)
- Encapsulating Security Payload (IP Protocol 50)
- FW1 SecureClient Verification keep alive (UDP Port 18233)
- FW1 Policy Server Logon Protocol (TCP Port 18231)
- FW1 topology request (TCP Port 264)
- VPN1 IPSec Transport Encapsulation Protocol (UDP Port 2746)
- FW1 SecuRemote Distribution Service (TCP Port 18232) – if configured
- Authentication Header (IP Protocol 51) – if configured
- IKE TCP (TCP Port 500) – if enabled

The firewall performs Network Address Translation to maximize the use of the limited IP address range assigned by the ISP.

External Web Server – GDWB01

Hardware: Dual Xeon 2.0GHz processor Dell PowerEdge 6650 server
Software: Microsoft Internet Information Server 6.0

[5] http://www.nsa.gov/snac/index.html
[6] Check Point Firewall-1 Desktop Security NG FP3 Manual pg 65

McAfee VirusScan 7.1.0
Operating System: Windows 2003.

The server is installed as a stand-alone server and patched with the latest security hotfixes and hardened according to the Microsoft Windows Server 2003 Security Guide. To reduce the risk of future vulnerabilities in IIS, URLScan 2.5[7] is installed and configured. URLScan is a URL filter that blocks access to http verbs, file extensions and specially crafted URLs.

The External Web server hosts the web applications that serve the customers, suppliers, partners and the public. All connections to the External Web server are performed via TCP ports 80 and 443.

The web server connects to the database server to retrieve customer or business associate information and to retrieve or upload fortune cookie sayings. The connection to the SQL server uses TCP port 1433[8].

Most of the customers and business associates connectivity to the External Web server requires encryption. 128bit SSLv3 is used for all secured transactions. To improve HTTPS performance, the External Web server is equipped with Compaq AXL300 SSL accelerator[9] to offload crypto-calculations from the server CPUs.

McAfee VirusScan 7.1.0 scans files for viruses. The software retrieves virus definition updates from the Software Update Server using HTTP protocol.

External DNS Server – GDDN01

Hardware: Single Xeon 2.4GHz processor Dell PowerEdge 2650 server
Software: Microsoft DNS Server
McAfee VirusScan 7.1.0
Operating System: Windows 2003.

The Windows 2003 DNS server is hardened and patched with the latest hotfixes. The secondary DNS servers are hosted by the ISP. To further protect the external DNS server from attacks or abuse, the following settings have been configured:

- Disable dynamic updates
- Disable recursions
- Enable Secure cache against pollution (default Windows DNS setting).
- Zone transfers only to ISP DNS servers

GIAC Enterprises utilize split DNS to protect the internal servers identity and IP addresses from would-be intruders. The External DNS server only provides name resolution for public access servers in the DMZ network. GIAC Enterprises has registered the name giacent.com as their public domain name.

[7] http://www.microsoft.com/technet/treeview/?url=/technet/security/tools/tools/urlscan.asp
[8] http://support.microsoft.com/default.aspx?scid=kb;en-us;287932
[9] http://h18004.www1.hp.com/products/servers/security/axl300/

Mail relay – GDMR01

Hardware: Single Xeon 2.4GHz processor Dell PowerEdge 2650 server
Software: McAfee WebShield SMTP MR1a Hotfix 8
McAfee VirusScan 7.1.0
Operating System: Windows 2003 patched with the latest hotfixes and hardened for bastion host operations

All Internet mails entering or leaving GIAC Enterprises Mail server are sent via the Mail Relay server. This ensures that viruses and malicious contents are stopped at the gateway. WebShield SMTP scans mails and attachments for viruses and removes or deletes them when found. WebShield SMTP uses FTP protocol to retrieve anti-virus definition updates.

GIAC requires the WebShield SMTP to block attachment types that are considered unsafe by Microsoft[10] from entering or leaving the network via e-mail. The anti-virus software obtains its updates from the Software Update server using FTP protocol.

To minimize the risk of the Mail Relay server being used by spammers, the server is configured to allow relaying only from the Exchange server and itself. The server limits the maximum mail size to 5MB to avoid overloading the leased line and the Mail Relay server.

The Mail Relay server uses the Internet Service Provider's cache DNS servers resolve addresses for outgoing messages. Incoming mails are sent directly to the Mail server's IP address.

Windows 2003 Active Directory Servers – GEAD01 & GEAD02

Hardware: Single Xeon 2.0GHz processor Dell PowerEdge 6650 server
Software: McAfee VirusScan 7.1.0
Operating System: Windows 2003 patched with the latest hotfixes and hardened according to the Microsoft Windows Server 2003 Security Guide.

The Microsoft Windows 2003 Active Directory servers provide single sign-on for internal users to access network shared folders, printers, Proxy server, Microsoft Exchange 2000 and SQL Server 2000. Access control for network services are granted based on the employee's account group memberships in the Active Directory.

Two servers provide high-availability and load sharing for Intranet DNS, Global Catalog, DHCP, and File and Print services. VirusScan 7.1.0 is installed on the AD servers to detect viruses in the server files.

The Intranet DNS is AD integrated to support secured Dynamic DNS updates. The internal DNS domain name is giacent.msad. The Intranet DNS is configured with a separate DNS zone for the public domain name, giacent.com. The internal copy of the

[10] http://support.microsoft.com/default.aspx?scid=kb;en-us;262631

public domain stores only the private address of the DMZ servers. The internal DNS servers are configured to:

- Enable secure dynamic updates
- Enable recursions
- Enable Secure cache against pollution (default Windows DNS setting).
- Disable Zone transfers

All internal clients send DNS queries to the AD servers. The AD servers forward any names that cannot be resolved locally to the ISP's cache DNS servers.

All Windows clients in a domain automatically synchronize their clocks with the domain controller. The AD server with the PDC Emulator role is configured to synchronize its clock with an Internet time source. The firewall and DMZ servers are manually configured to synchronize the clocks with the PDC Emulator using NTP UDP protocol.

Outlook MAPI clients retrieves the Global Address List from the Active Directory Global Catalog via the Name Service Provider Interface. NSPI uses a dynamically assigned port and is located via the DCE RPC endport mapper UUID f5cc5a18-4264-101a-8c59-08002b2f8426[11]. Since Check Point Firewall supports RPC protocol, there is no requirement to fix the port.

Database Server – GEDB01

Hardware: Single Xeon 2.0GHz processor Dell PowerEdge 6650 server
Software: Microsoft SQL Server 2000 Service Pack 3a and patched with MS03-031 cumulative patch[12].
Operating System: Windows 2003 patched with the latest hotfixes and hardened according to the Microsoft Windows Server 2003 Security Guide.

The database server stores all fortune cookies sayings and GIAC Enterprises transactions. The server is joined to the domain for internal users to access the database with their Windows domain accounts. SQL Server authentication is also enabled to allow the web server to access the database without using Windows domain accounts.

Mail Server – GEEM01

Hardware: Single Xeon 2.0GHz processor Dell PowerEdge 6650 server
Software: Microsoft Exchange 2000 Service Pack 3 with the latest MS03-046[13] hotfix
GroupShield Exchange 2000 5.2.1
Operating System: Windows 2000 Service Pack 4 patched with the latest hotfixes and hardened according to the Microsoft Windows Server 2003 Security Guide.

[11] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/isa/maintain/rpcwisa.asp
[12] http://www.microsoft.com/technet/security/bulletin/MS03-031.asp
[13] http://www.microsoft.com/technet/security/bulletin/MS03-046.asp

Exchange 2000 provides e-mail facility to GIAC Enterprises staff including mobile sales staff and teleworkers. Users are able to access their e-mails using either Microsoft Outlook MAPI or Outlook Web Access to access the e-mail.

Exchange Server requires Microsoft Internet Information Server 5.0 to be installed. The web service is hardened and installed with Microsoft's Lockdown Tool 2.1[14] and URLScan 2.5 HTTP filter.

McAfee GroupShield for Exchange 2000 is used to protect the Exchange server from e-mail viruses sent from the workstations. This is especially important for Outlook and Outlook Express based clients, as they are frequent targets of viruses and worms that may affect the availability of the mail server. To reduce the possibility of unknown virus and worm infection, Groupshield is configured to remove any attachments that are declared unsafe by Microsoft[15].

Outlook MAPI clients uses RPC protocol to access the Exchange server. The protocols used by the MAPI clients are[16]:

- Exchange System Attendant Directory Referrer – UUID: 1544f5e0-613c-11d1-93df-00c04fd7bd09
- Exchange Information Store – UUID: a4f1db00- ca47- 1067- b31f- 00dd010662da
- Exchange Directory Name Service Provider Interface Proxy (not required for Outlook 2000) – UUID: f5cc5a18-4264-101a-8c59-08002b2f8426

These ports are dynamically allocated during the Exchange server startup.

The Mobile Sales Staff and Teleworkers are also given Outlook Web Access service Outlook MAPI client. SSL has been configured and enabled on the Exchange server to provide end-to-end encryption for the remote users. The MAPI client is also provided to the remote employees, as some required features are not available on Exchange 2000 OWA.

Syslog server – GESL01

Hardware: Single Pentium 4 2.66GHz processor Dell Dimension 2400 PC
Software: Kiwi Syslog
McAfee VirusScan 7.1.0
Operating System: Windows XP Service Pack 1 patched with the latest hotfixes.

Kiwi Syslog installed as a Windows service to receive and store logs from the border router.

Windows IPSec filter is used to limit access to and from the network[17]. The workstation system clock is synchronized with the PDC Emulator Active Directory server using NTP.

[14] http://www.microsoft.com/technet/treeview/?url=/technet/security/tools/tools/locktool.asp
[15] http://support.microsoft.com/default.aspx?scid=kb;en-us;262631
[16] http://support.microsoft.com/default.aspx?scid=kb;en-us;280132
[17] http://www.winnetmag.com/Web/Article/ArticleID/25935/Web_25935.html

Proxy Server – GEPX01

Hardware: Single Xeon 2.4GHz processor Dell PowerEdge 2650 server
Software: Microsoft Internet Security and Acceleration Server Service Pack 1
McAfee VirusScan 7.1.0
Operating System: Windows 2003 patched with the latest hotfixes and hardened for bastion host operations

The proxy server controls and monitors GIAC Enterprises employees' web surfing activities. The proxy server is the only server in the network that is able to access the Internet using HTTP, HTTPS and FTP protocols. The proxy server is configured to restrict the web sites employees and servers can connect to. Servers are allowed to access only specific web sites such as vendor sites to obtain patches and upgrades.

To provide single-sign-on for GIAC Employees, the Proxy server is installed as a member of the Active Directory domain.

Software Update server – GESU01

Hardware: Single Xeon 2.4GHz processor Dell PowerEdge 2650 server
Software: Software Update Service SP1,
McAfee AutoUpdate Architect v1.1.1,
ePolicy Orchestra v3.0.1
McAfee VirusScan 7.1.0
Internet Information Server 6.0.
Operating System: Windows 2003 patched with the latest hotfixes and hardened for bastion host operations

Regular updates of Windows patches and anti-virus patterns are required to minimize the risk of system failures and downtime for GIAC Enterprises business. Software updates are provided to clients and servers via IIS HTTP and FTP services. FTP is required because WebShield and GroupShield only support FTP updates. The FTP service is configured to allow anonymous logins and read only access.

IIS6 HTTP service is restrictive out of the box. Several file extensions such as .mct, and .log, have been defined in the IIS6 MIME database as application/octet-stream to allow files to be downloaded from the HTTP server[18]. URLScan 2.5 is installed to filter invalid or malformed requests to the HTTP server.

McAfee AutoUpdate Architect is used to provide anti-virus pattern updates and engine upgrades. The server checks for new virus patterns from Network Associates every day at 6:00am.

The Software Update server is also installed with the Microsoft Software Update Service to provide Windows hotfixes to GIAC Enterprises clients and servers. Client

[18] http://support.microsoft.com/default.aspx?scid=kb;en-us;326965

workstations are configured to install and restart every Thursday at 12pm. Updates are performed using HTTP protocol.

Mobile Sales Staff and Teleworkers Desktop Protection

Software: Check Point SecureClient NG FP3
Operating System: Windows 2000/XP Professional

Check Point SecureClient provides a centrally controlled desktop firewall for the remote staff. Desktop policies are managed from the Check Point management console. The purpose of the desktop firewall is to prevent unauthorized connections to the remote employee's workstations and notebooks.

Connectivity Requirements Summary

Table 2 shows the connectivity summary for GIAC Enterprises network.

Source	Destination	Protocol	Service
From Internet			
- Customers - Suppliers - Partners - Public	External Web server	HTTP HTTPS	TCP 80 TCP 443
	Mail Relay server	SMTP	TCP 25
	External DNS	DNS	UDP 53
Border router Firewall	Syslog server	SysLog	UDP 514
Form DMZ			
Mail Relay server	Mail server	SMTP	TCP 25
	ISP DNS server	DNS	TCP/UDP 53
External Web server	Database server	SQL Server	TCP 1433
Mail Relay server	Software Update server	FTP	TCP 21
Mail Relay server External DNS server External Web server	Software Update server	HTTP	TCP 80
Outgoing connections			
Active Directory servers	ISP DNS server	DNS	TCP/UDP 53
Active Directory server (PDC)	External NTP server	NTP	UDP 123
Proxy server	Internet	HTTP HTTPS FTP	TCP 80 TCP 443 TCP 21
Mail server	Mail Relay server	SMTP	TCP 25
Internal connections			
Internal Employees	Proxy server	HTTP Proxy	TCP 8080

Source	Destination	Protocol	Service
	Active Directory servers	CIFS (SMB) CIFS (NBT session) Kerberos DNS LDAP Global Catalog (LDAP) Active Directory Logon Exchange NSPI RPC endpoint mapper NTP	TCP/UDP 445 TCP 139 TCP/UDP 88 TCP/UDP 53 TCP/UDP 389 TCP 3268 TCP > 1023 TCP > 1023 TCP 135 UDP 123
	Mail server	CIFS (SMB) CIFS (NBT session) HTTP HTTPS RPC endpoint mapper Exchange SA RFR Exchange NSPI Proxy Exchange IS	TCP/UDP 445 TCP 139 TCP 80 TCP 443 TCP 135 TCP > 1023 TCP > 1023 TCP > 1023
	Database server	SQL Server	TCP 1433
	Software Update server	HTTP FTP	TCP 80 TCP 21
	External Web server	HTTP HTTPS	TCP 80 TCP 443
Mail server Proxy server Database server	Active Directory servers	CIFS (SMB) CIFS (NBT session) Kerberos DNS LDAP Global Catalog(LDAP) Active Directory Logon RPC endpoint mapper NTP	TCP/UDP 445 TCP 139 TCP/UPD 88 TCP/UDP 53 TCP/UDP 389 TCP 3268 TCP > 1023 TCP 135 UDP 123
Mail Server	Active Directory servers	Exchange NSPI	TCP > 1024
Syslog server Software Update server	Active Directory servers	NTP	UDP 123
Firewall	Active Directory server (PDC)	NTP	UDP 123
Active Directory servers	Network Printers	LPD	TCP 515
All GIAC workstations and servers	Software Update server	HTTP	TCP 80

Source	Destination	Protocol	Service
Software Update server	Proxy server	HTTP Proxy	TCP 8080
VPN			
Mobile sales force Teleworker (VPN Clients)	VPN server	ESP ISAKMP FW1 scv keep alive FW1 pslogon NG FW1 topology request	IP Protocol 50 UDP 500 UDP 18233 TCP 18231 TCP 264
	Active Directory servers	CIFS (SMB) DNS Global Catalog Exchange NSPI RPC endport mapper	TCP 445 TCP/UDP 53 TCP 3268 TCP > 1023 TCP 135
	Mail server	HTTP HTTPS RPC endpoint Mapper Exchange SA RFR Exchange NSPI Proxy Exchange IS	TCP 80 TCP 443 TCP 135 TCP > 1023 TCP > 1023 TCP > 1023
	Database server	SQL Server	TCP 1433
	External Web server	HTTP HTTPS	TCP 80 TCP 443
	Software Update server	HTTP	TCP 80

Table 2: TCP/IP Connection Summary

Assignment 2 – Security Policy and Tutorial

Border Router Security Policy

The border router is used to perform static packet filtering to remove unwanted addresses and connection protocols. The router is hardened using guidelines specified by the NSA Router Security Configuration Guide[19]. The complete router configuration is placed in Appendix A.

Disabled Router Services

The border router has several services running by default. As these services are not required, they are disabled to reduce the security risks to the router.

CDP Protocol

Cisco routers and switches use the Cisco Discovery Protocol to identify each other in a network segment. It may disclose some router configuration information.

```
GEBR01 (config)# no cdp run
```

[19] http://www.nsa.gov/snac/cisco/download.htm

TCP and UDP small servers

This is a collection of protocol standards that hosts are recommended to provide. However, these protocols are not desired on the border router.

```
GEBR01 (config)# no service tcp-small-servers
GEBR01 (config)# no service udp-small-servers
```

Finger Server

The finger server is used for querying hosts on the logged in users. This may provide an intruder with the user names used in the router. The service is disabled using:

```
GEBR01 (config)# no service finger
GEBR01 (config)# no ip finger
```

HTTP Server

The Cisco router provides a web interface for remote administration and may provide a means of monitoring, configuring and attacking the router. The service is disabled.

```
GEBR01 (config)# no ip http server
```

BootP & DHCP Server

Cisco routers are capable of providing bootp services for other Cisco routers to download the IOS software. Cisco IOS are also equipped with DHCP servers. Both services are not used on the border router and are disabled.

```
GEBR01 (config)# no ip bootp server
GEBR01 (config)# no service dhcp
```

Configuration Autoloading

Cisco routers are capable of loading their startup configuration from local or from the network. As the network is not secure, the feature is disabled explicitly.

```
GEBR01 (config)# no boot network
GEBR01 (config)# no service config
```

IP Source Routing

Source routing is an IP feature that allows individual packets to specify the routes to the destination. This feature is not required for normal IP traffic and should be disabled explicitly.

```
GEBR01 (config)# no ip source-route
```

Proxy ARP

Proxy ARP provides transparent access between different LAN segments. This feature is not required on the border router and is disabled at both the Fast Ethernet and serial interface of the router

```
GEBR01 (config)# interface fastethernet 0/0
GEBR01 (config-if)# no ip proxy-arp
GEBR01 (config-if)# interface serial 0/0
GEBR01 (config-if)# no ip proxy-arp
```

IP Directed Broadcasts

Broadcasts should not be allowed across different subnets. Each router interface is configured to disable this feature

```
GEBR01 (config)# interface fastethernet 0/0
GEBR01 (config-if)# no ip directed-broadcast
GEBR01 (config-if)# interface serial 0/0
GEBR01 (config-if)# no ip directed-broadcast
```

IP Unreachables, Redirects & Mask replies

By default, Cisco routers send ICMP messages in various conditions. The messages may provide information about the network to an attacker. Automatic generation of these messages should be disabled

```
GEBR01 (config)# interface fastethernet 0/0
GEBR01 (config-if)# no ip unreachable
GEBR01 (config-if)# no ip redirects
GEBR01 (config-if)# no ip mask-replies
GEBR01 (config-if)# interface serial 0/0
GEBR01 (config-if)# no ip unreachable
GEBR01 (config-if)# no ip redirects
GEBR01 (config-if)# no ip mask-replies
```

SNMP Server

The SNMP service is not used and will be disabled

```
GEBR01 (config)# no snmp-server enable traps
GEBR01 (config)# no snmp-server system-shutdown
GEBR01 (config)# no snmp-server trap-auth
GEBR01 (config)# no snmp-server
```

NTP Service

NTP is disabled and the router clock is set manually.

```
GEBR01 (config)# clock timezone CST
GEBR01 (config)# interface fastethernet 0/0
GEBR01 (config-if)# ntp disable
GEBR01 (config-if)# interface serial 0/0
GEBR01 (config-if)# ntp disable
GEBR01 (config-if)# exit
GEBR01 (config)# exit
GEBR01# clock set <hh>:<mm>:<ss> <dd> <mmm> <yyyy>
```

DNS Name resolution

By default, Cisco routers send DNS queries to the broadcast address but can be configured to use a specific DNS server. Domain lookup is not required in the border router and is disabled.

```
GEBR01 (config)# no ip domain-lookup
```

Enabled Router Services

Router Logging

The border router is configured to send informational logs, which includes access control logs to the syslog server. A static route is added to the router to be able to route to the syslog server using its private IP address.

```
GEBR01 (config)# service timestamps log datetime msec localtime show-
       timezone
GEBR01 (config)# logging facility local6
GEBR01 (config)# logging 192.168.0.35
```

Router Console

The router is managed via the console. The console port is enabled by default. It is configured to disconnect after 5 minutes idle.

```
GEBR01 (config)# line con 0
GEBR01 (config-line)# exec-timeout 5 0
GEBR01 (config-line)# login local
GEBR01 (config-line)# transport input none
```

The vty port is closed to prevent connections.

```
GEBR01 (config)# line vty 0 4
GEBR01 (config-line)# transport input none
GEBR01 (config-line)# exec-timeout 0 1
GEBR01 (config-line)# no login
GEBR01 (config-line)# no exec
```

The auxiliary port is disabled, as it's not required.

```
GEBR01 (config)# line aux 0
GEBR01 (config-line)# transport input none
GEBR01 (config-line)# no exec
GEBR01 (config-line)# no login
GEBR01 (config-line)# exec-timeout 0 1
```

An Administrator Account is created to login into the border router to enforce authentication. Privilege level 1 allows the login to User Exec mode (non-privilege). The Enable account is required to enter privilege Exec mode to modify router settings.

```
GEBR01 (config)# username gesuper privilege 1 password <password>
```

Password encryption is enabled to prevent it from being easily cracked.

```
GEBR01 (config)# service password-encryption
GEBR01 (config)# enable secret 5 <enable_password>
GEBR01 (config)# no enable password
```

Router Interface

External Interface

The external interface performs most of the filtering tasks as it faces the untrusted Internet. The ingress filter is created using Cisco IOS Extended Access List.

The first types of traffic to block are those that have invalid source IP address. The source IP address encompasses all incoming network packets and is the most general rule. The invalid source IP addresses includes:

- The historic net broadcast networks

```
access-list 105 deny   ip 0.0.0.0 0.255.255.255 any
```

- The RFC 1918 private networks

```
access-list 105 deny   ip 10.0.0.0 0.255.255.255 any
access-list 105 deny   ip 172.16.0.0 0.15.255.255 any
access-list 105 deny   ip 192.168.0.0 0.0.255.255 any
```

- The Class D (multicast) and Class E (reserved for future) networks

```
access-list 105 deny   ip 224.0.0.0 31.255.255.255 any
```

- The broadcast networks

```
access-list 105 deny   ip 255.0.0.0 0.255.255.255 any
```

- The loopback address

```
access-list 105 deny   ip 127.0.0.0 0.255.255.255 any
```

- TEST-NET network

```
access-list 105 deny   ip 192.0.2.0 0.0.0.255 any
```

- Link-local IP autoconfiguration networks

```
access-list 105 deny   ip 169.254.0.0 0.0.255.255 any
```

- And the IP network assigned to GIAC Enterprises. This rule also blocks LAND attacks where the source and destination address are the same.

```
access-list 105 deny   ip A.B.202.224 0.0.0.15 any
```

These packets are not logged since it would not be possible to trace the origin.

There are a few ICMP protocols that may be required for normal network operations and are allowed to any address in GIAC public address. All other ICMP packets are dropped.

```
access-list 105 permit icmp any A.B.202.224 0.0.0.15 source-quench log
access-list 105 permit icmp any A.B.202.224 0.0.0.15 parameter-problem log
access-list 105 permit icmp any A.B.202.224 0.0.0.15 time-exceeded log
access-list 105 permit icmp any A.B.202.224 0.0.0.15 unreachable log
access-list 105 deny   icmp any any log
```

Allow access to the Web server via http and https ports

```
access-list 105 permit tcp any host A.B.202.228 eq 80
access-list 105 permit tcp any host A.B.202.228 eq 443
```

Allow access to the DNS server via UDP dns port. Allow TCP dns only from ISP secondary servers.

```
access-list 105 permit udp any host A.B.202.229 eq 53
access-list 105 permit tcp A.B.200.88 host A.B.202.229 eq 53
access-list 105 permit tcp A.B.200.100 host A.B.202.229 eq 53
```

Allow access to the Mail Relay server via the smtp port. The Mail Relay server also initiates smtp and dns connections to the Internet. So TCP and UDP high ports are allowed to the server.

```
access-list 105 permit tcp any host A.B.202.227 eq 25
access-list 105 permit tcp any host A.B.202.227 gt 1023
access-list 105 permit udp any host A.B.202.227 gt 1023
```

Outbound connections from the Intranet network are translated by the firewall using hidden NAT to A.B.202.230. These packets should be allowed through. Firewall-1 Hidden NAT translates using the following port ranges:[20]

- low ports from 600 to 1023
- high ports from 10000 to 60000

```
access-list 105 permit tcp any host A.B.202.230 range 600 1023
access-list 105 permit tcp any host A.B.202.230 range 10000 60000
access-list 105 permit udp any host A.B.202.230 range 600 1023
access-list 105 permit udp any host A.B.202.230 range 10000 60000
```

The router allows network packets addressed to the firewall that are required for Check Point VPN connections. Any other connections to the firewall are blocked and logged.

```
access-list 105 permit udp any host A.B.202.226 eq 500
access-list 105 permit udp any host A.B.202.226 eq 2746
access-list 105 permit udp any host A.B.202.226 eq 18233
access-list 105 permit tcp any host A.B.202.226 eq 264
access-list 105 permit tcp any host A.B.202.226 range 18231 18232
access-list 105 permit esp any host A.B.202.226
access-list 105 deny   ip any host A.B.202.226 log
```

The border router should not initiate or receive packets. To protect the router from attacks, access to the all router interfaces from the Internet is prohibited.

```
access-list 105 deny   ip any host A.B.212.58 log
access-list 105 deny   ip any host A.B.202.225 log
```

And finally, if the packet does not match any previous rules, the connection is dropped and logged

```
access-list 105 deny   ip any any log
```

The Ingress filter is applied to incoming packets to the serial interface of the border router

```
GEBR01 (config)# interface Serial0/0
GEBR01 (config-if)# ip access-group 105 in
```

Internal Interface

Egress filtering is implemented at the router internal interface. The objective of this filter is to

[20] Check Point Firewall-1 Guide NG FP3 pg 71-72

- prevent GIAC network from being used to attack other Internet hosts using spoofed IP addresses and
- prevent Microsoft networking protocols from leaving the network.

Firstly, the filter blocks destination IP addresses that may invalid in the Internet.

```
access-list 106 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 106 deny   ip any 172.16.0.0 0.15.255.255 log
access-list 106 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 106 deny   ip any 192.0.2.0 0.0.0.255 log
access-list 106 deny   ip any 224.0.0.0 31.255.255.255 log
access-list 106 deny   ip any A.B.0.0 0.0.255.255 log
```

Next, the critical service ports are blocked. These protocols should not leave GIAC Enterprises as it may reveal information on the internal network. These includes

- NetBIOS protocols

```
access-list 106 deny   tcp any any range 135 139 log
access-list 106 deny   tcp any any eq 445 log
access-list 106 deny   udp any any range 135 139 log
access-list 106 deny   udp any any eq 445 log
```

- SNMP, remote login, syslog and lpd protocols

```
access-list 106 deny   udp any any range 161 162 log
access-list 106 deny   tcp any any range 513 515 log
access-list 106 deny   udp any any range 513 515 log
```

Only network packets with public source address should be allowed to the Internet. Any other address detected could mean that the NAT was misconfigured or has failed.

```
access-list 106 permit ip 10.50.202.224 0.0.0.15 any
```

Finally, all other outbound connections are dropped and logged.

```
access-list 106 deny   ip any any log
```

The Egress filter is applied to incoming packets to the Ethernet interface of the border router

```
GEBR01 (config)# interface FastEthernet0/0
GEBR01 (config-if)# ip access-group 106 in
```

Primary Firewall Security Policy

The primary firewall is configured to perform stateful packet filtering and Network address translation. The firewall software selected is Check Point VPN-1/Firewall-1 NG Feature Pack 3.

Check Point firewall requires all of the items used in the security policy be defined as objects. The objects used by GIAC Enterprises firewall policy include:

- Hosts objects – IP host nodes
- Network objects – IP network and sub-networks
- Service objects – IP protocols
- User objects – to define remote users

- Network Objects Group – group of Hosts and Network Objects.
- Services Group – group of Services objects
- Users Group – group of Users

Hosts Objects

Each server that is specified in the rule base must be defined as a host. The three DMZ servers are defined with Static NAT. Check Point Firewall-1 NG handles routing and Address Resolution Protocol for these hosts.

Host	IP	NAT	Comments
ISPCDNS1	A.B.200.80	Disabled	ISP Cache DNS 1
ISPCDNS2	A.B.200.11	Disabled	ISP Cache DNS 2
ISPSDNS1	A.B.200.88	Disabled	ISP Secondary DNS 1
ISPSDNS2	A.B.200.100	Disabled	ISP Secondary DNS 2
GDDN01	192.168.64.33	Static A.B.202.229	External DNS server
GDMR01	192.168.64.31	Static A.B.202.227	Mail relay server
GDWB01	192.168.64.32	Static A.B.202.228	External Web server
GEAD01	192.168.0.31	Disabled	AD PDC server
GEAD02	192.168.0.31	Disabled	AD PDC server
GEBR01	A.B.202.225	Disabled	Border router
GEDB01	192.168.0.34	Disabled	Database server
GEEM01	192.168.0.33	Disabled	Exchange Mail server
GEFW01	A.B.202.226 192.168.64.1 192.168.0.1	Disabled	Firewall External interface Firewall DMZ interface Firewall Intranet interface
GEPX01	192.168.0.37	Disabled	Proxy server
GESL01	192.168.0.35	Disabled	Syslog server
GESU01	192.168.0.36	Disabled	Software Update server
Ext_time_svr	A.B.244.18	Disabled	External time server

Table 3: Firewall Hosts objects

Network Objects

Network objects are defined for the firewall policy and the Network Address Translation rules. Intranet network addresses are translated using dynamic NAT.

Name	IP	Subnet mask	Include Broadcast	NAT	Comments
GEDMZ	192.168.64.0	255.255.255.0	No	Disabled	GE's DMZ network
GENet	192.168.0.0	255.255.0.0	No	Disabled	All GE networks
GEIntranet	192.168.0.0	255.255.252.0	No	Hide A.B.202.230	GE Internal network

Table 4: Firewall Network objects

Service objects

Service objects define the IP protocol and ports for each connection. Only the destination ports are defined.

Service Name	Protocol	Port	Comments
Bootp	UDP	67	Bootstrap Protocol Server, users automatically configured
domain-UDP	UDP	53	Domain Name System Queries
domain-TCP	TCP	53	Domain Name System Download
FTP	TCP	21	File Transfer Protocol
FW1_pslogon_NG	TCP	18231	Check Point NG Policy Server Logon protocol
FW1_topo	TCP	264	Check Point VPN-1 SecuRemote Topology Requests
FW1_scv_keep_alive	Udp	18233	Check Point SecureClient Verification Keepalive protocol
HTTP	TCP	80	Hypertext Transfer Protocol
HTTPS	TCP	443	HTTP protocol over TLS/SSL
IKE	UDP	500	IPSec Internet Key Exchange Protocol (formally ISAKMP/Oakley)
Microsoft-ds	TCP	445	Microsoft CIFS over TCP
MS-SQL-Server	TCP	1433	Microsoft SQL Server
Nbsession	TCP	139	NetBios Session Service
Nbdatagram	UDP	138	NetBios Datagram Service
Nbname	UDP	137	NetBios Name Service
ntp-udp	UDP	123	Network Time Protocol (UDP)
Smtp	TCP	25	Simple Mail Transfer Protocol
Syslog	UDP	514	UNIX syslog Protocol, control system log

Table 5: Firewall Service objects

By default, the Distributed Computing Environment Remote Procedure Call (DCE-RPC) ports used by Microsoft Exchange is allocated dynamically during server startup. Firewall-1 is able to read the RPC endpoint mapper traffic and open the TCP ports used by the Exchange server. Thus, the firewall policy can dynamically allow only the required ports. This feature is also able to detect and block attacks based on the published RPC vulnerabilities[21] on Windows.

Table 6 lists the DCE-RPC ports are used by Microsoft Exchange MAPI clients.

Service Name	Interface UUID	Comment	Protocol Type
MSExchangeDSNSPI	f5cc5a18-4264-101a8c59-08002b2f8426	Microsoft Exchange Directory Services (NSPI)	Not defined

[21] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp

Service Name	Interface UUID	Comment	Protocol Type
MSExchangeDirRef	1544f5e0-613c-11d1-93df-00c04fd7bd09	Microsoft Exchange 2000 Directory Reference	Not defined
MSExchangeIS	a4f1db00- ca47-1067- b31f-00dd010662da	Microsoft Exchange Information Store	MSEXCHANGE

Table 6: MS Exchange DCE-RPC Services

Group Objects

Group objects simplify the rule base and are required for VPN configuration. Table 7 shows the groups that are defined in GIAC Enterprises firewall.

Name	Group Members	Comments
Network Groups		
ADServers	GEAD01 GEAD02	Active Directory Servers
DMZSvrs	GDWB01 GDDN01 GDMR01	Servers in the DMZ
VPNaccess	GEAD01 GEAD02 GEEM01 GEDB01 GESU01	Servers reachable from VPN clients.
Service Groups		
Dns	domain-TCP domain-UDP	Domain Name System (TCP/UDP)
NBT	Nbsession Nbdatagram Nbname	NetBios Services
User Groups		
VPNUsers		Mobile staff and teleworkers

Table 7: Firewall Group objects

VPN Community

Check Point Firewall-1 NG FP3 supports the concept of VPN Community to simplify the management of VPN connections. VPN Communities are specified in the policy rules in the IF VIA column.

Name	Gateway	User Group	Comment
RemoteAccess	GEFW01	VPNUsers	Mobile Sales staff and Teleworkers VPN access

Table 8: Firewall VPN Community

Firewall Policy Rule Base

The firewall rule base is configured to allow only the IP protocols that are required for the business to function based on the protocols that have been identified in the Security Architecture design.

In general, the firewall software scans through the firewall policy starting from top down when it receives a TCP SYN packet. When a rule is matched, the packet is permitted, dropped based on the matched rule. If none of the rules match, the firewall silently drops the packet. Once the connection is established, Firewall-1 adds the connection to the connections table[22].

If the network packet the firewall receives does not have the SYN flag enabled, the packet is matched against the firewall's connection table. If no match is found or the state table information has timed out, the packet is dropped.

The first rule in the firewall policy is to drop NetBIOS over TCP/IP and bootp protocols without logging. Windows servers and workstations often broadcast NetBIOS name announcements. NBT is not required across the firewall and can quickly fill the logs. This rule is the first because of the number of NetBIOS traffic in the network.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
1	Any	Any	Any	NBT Bootp	Drop	None	Drop netbios bootp traffic without logging

Table 9: NetBIOS Rule

VPN connections are allowed to the firewall through Rule 2. Rule 3 allows the firewall to initiate IKE connections.

Except for the VPN connections, there should not be any connections directly to the firewall. Rule 4 protects the firewall from any other external connections. Direct connections to the firewall are dropped and logged with Alert. Although the firewall drops all connections that are not explicitly allowed, placing this drop rule here ensures that the connection is not inadvertently allowed by another rule in the rule base.

[22] Check Point Firewall-1 Guide pg 163

No	Source	Destination	IF VIA	Service	Action	Track	Comments
2	Any	GEFW01	Any	FW1_topo IKE FW1_pslogo n_NG FW1_scv_ke ep_alive	accep t	Log	VPN access
3	GEFW01	Any	Any	IKE	accep t	Log	VPN access
4	Any	GEFW01	Any	Any	Drop	Alert	Firewall lockdown

Table 10: Firewall Stealth Rule

Except for the last rule, the order of the rest of the rules does not have any impact to the policy. Thus, these rules are arranged to maximize performance by placing the frequent connections near the top and least frequent connections at the bottom.

Rules 5 and 6 allows access to the External Web server applications. In rule 5, users from the Internet, which include customers, suppliers, partners and the public, are allowed to connect to the HTTP and HTTPS ports of the External Web server. Rule 6 allows the External Web server to connect to the SQL server via TCP port 1433.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
5	Any	GDWB01	Any	http https	accep t	Log	Anyone can http/s to Ext web server
6	GDWB01	GEDB01	Any	MS-SQL-server	accep t	Log	Ext web server needs data from sql server

Table 11: External Web server Access Rule

Rule 7 allows HTTP, HTTPS and FTP port connections from the Proxy server. Internal users must use the proxy server to surf the Internet and direct outbound connections are not allowed. The destination is restricted to non-GIAC network to block access to the DMZ servers. Users can still access the External Web server directly using rule 5 above.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
7	GEPX01	Not GENet	Any	http https ftp	accep t	Log	Only proxy can surf the Internet

Table 12: Web Surfing Rule

Rule 8 allows Internet hosts to query the External DNS server on UDP port 53. The DNS responses from the External DNS server are small enough to fit into the 512 bytes limit for UDP. Thus, TCP port 53 is not required to the External DNS.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
8	Any	GDDN01	Any	domain-UDP	accept	Log	Any host can query DNS server

Table 13: External DNS Rule

The Mail Relay and Active Directory servers need to resolve external domain names to perform their roles. As the internal servers are configured to forward locally unresolved DNS queries to the ISP cache DNS servers, access to the root DNS servers is not required. Rule 9 allows the servers to query only the Internet Service Provider's cache DNS servers.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
9	GDMR01 ADServers	ISPCDNS1 ISPCDNS2	Any	DNS	accept	Log	Only mail relay and ad servers can forward dns queries to ISP

Table 14: DNS Query Rule

The next set of rules permits connections using TCP port 25 (SMTP). Rule 10 allows only the Mail Relay in the DMZ network and Exchange server in the Intranet can connect using TCP port 25. All other servers and workstations in the network must use the Exchange server to send and receive e-mails. Rules 11 and 12 allows SMTP mails to be sent between Internet hosts and the Mail Relay server. This helps to prevent the Mail Relay server from accessing any hosts in other network segments.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
10	GEEM01 GDMR01	GDMR01 GEEM01	Any	smtp	accept	Log	Exch server can send/recv mails from relay svr
11	Not GENet	GDMR01	Any	smtp	accept	Log	Allow incoming mails from Internet via relay svr
12	GDMR01	Not GENet	Any	smtp	accept	Log	Relay server can send outgoing Internet mails

Table 15: Mail Relay Rules

Rules 13 through 16 provide Mobile Sales Staff and Teleworkers access to GIAC Enterprises internal network. The access is limited to specific servers and network services. The access granted is sufficient for the remote staff to perform their tasks without exposing the entire network.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
13	VPNUsers @Any	ADServers	RemoteAccess	Microsoft-ds Dns MSExchange DSNSPI	accept	Log	Access DNS, Directory and File shares
14	VPNUsers @Any	GEEM01	RemoteAccess	http https MSExchange DirRef MSExchange IS	accept	Log	Access exch server MAPI and OWA
15	VPNUsers @Any	GEDB01	RemoteAccess	MS-SQL-server	accept	Log	access sql server
16	VPNUsers @Any	GESU01	RemoteAccess	http	accept	Log	Get virus updates

Table 16: VPN Rules

Rule 17 allows the Border Router to send syslog messages to the Syslog server.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
17	GEBR01	GESL01	Any	Syslog	accept	Log	Border router syslog

Table 17: Border Router Syslog Rule

Rules 18 and 19 allow the servers to synchronize their clocks. The Active Directory servers synchronize their clocks to an external time source while the servers in the DMZ uses the Active Directory servers as their time reference. Once the clock is synchronized, Windows servers synchronize with the time source every 8 hours.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
18	DMZSvrs GEFW01	GEAD01	Any	Ntp-udp	accept	Log	time sync with AD server
19	ADServers	Ext_time_svr	Any	Ntp-udp	accept	Log	AD servers time sync with external time

Table 18: Time Synchronization Rules

Rules 20 and 21 permit Mail Relay, External DNS and External Web server to retrieve updates from Software Update server. The updates are checked daily.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
20	DMZSvrs	GESU01	Any	http	accept	Log	DMZ servers to get updates from software update server
21	GDMR01	GESU01	Any	ftp	accept	Log	relay svr to get updates using ftp

Table 19: Software Update Rule

Rule 22 allows the ISP Secondary DNS servers to perform zone transfers from the External DNS server. The connection is performed at most once a day.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
22	ISPSDNS1 ISPSDNS2	GDMR01	Any	domain-tcp	accept	Log	Secondary ISP DNS perform zone transfers

Table 20: Zone Transfer Rules

Rule 23 allows the firewall to send ICMP rejects to internal GIAC hosts.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
23	GEFW01	GEIntranet	Any	Dest-unreach	accept	Log	Firewall can send rejects

Table 21: Firewall Reject Rule

By default, Firewall-1 drops any packets that are not specifically allowed in the rule base. However, it does not log the dropped packets. Since we are interested to know what they are, the final rule is added to drop and log any unmatched connection.

No	Source	Destination	IF VIA	Service	Action	Track	Comments
24	Any	Any	Any	Any	Drop	Log	Drop & log everything else

Table 22: Drop Others and Log Rule

Network Address Translation

A manual NAT rule is added to the top of the NAT rules to prevent address translations for network traffic between the DMZ and the Intranet network. NAT should not be performed within GIAC hosts.

	Original Packet			Translated Packet			
No	Source	Destina-tion	Service	Source	Destina-tion	Service	Comments
1	GENet	GENet	Any	Original	Original	Any	No NAT for internal conns

Table 23: Manual NAT

Check Point Firewall-1 Automatic NAT configuration is selected for use in GIAC Enterprises firewall. Automatic NAT is defined in the NAT property in each host and network object. With Automatic NAT, routing and Address Resolution Protocol problems are handled by the firewall. The results of the Automatic NAT are shown in Table 24.

	Original Packet			Translated Packet			
No	Source	Destina-tion	Service	Source	Destina-tion	Service	Comments
2	GDDN01	Any	DNS	Static GDDN01 (Valid)	Original	Original	Automatic rule
3	Any	GDDN01 (Valid)	DNS	Original	Static GDDN01	Original	Automatic rule
4	GDMR01	Any	Any	Static GDMR01 (Valid)	Original	Original	Automatic rule
5	Any	GDMR01 (Valid)	SMTP	Original	Static GDMR01	Original	Automatic rule
6	GDWB01	Any	Any	Static GDWB01 (Valid)	Original	Original	Automatic rule
7	Any	GDWB01 (Valid)	Any	Original	Static GDWB01	Original	Automatic rule
8	GEIntranet	GEIntranet	Any	Original	Original	Original	Automatic rule
9	GEIntranet	Any	Any	GEIntranet (Hiding Address)	Original	Original	Automatic rule

Table 24: Automatic NAT Rules

Firewall-1 Implied Rules

The firewall software Global Properties contains settings that add additional rules that do not appear in the rule base by default. All implied rules are disabled as shown in Figure 14.

Anti Spoofing

IP Spoofing can be used to deceive the firewall that a packet source is a trusted host or from a trusted network. Check Point Firewall-1 prevents IP spoofing by defining the IP networks that are attached to each of the firewall's network interface. The firewall is configured to generate an alert when it detects a spoofed IP packet. The IP networks that are defined at GEFW01 interfaces are listed in Table 25.

Interface	IP Address	Network Mask	IP addresses behind interface
E100B1	192.168.0.1	255.255.254.0	This Network
E100B2	192.168.64.1	255.255.255.0	This Network
E100B3	A.B.202.226	255.255.255.224	External

Table 25 Anti-Spoofing Configuration

Session Timeouts

Check Point Firewall-1 Stateful Inspection is configured to reduce the TCP session timeout and UDP virtual session timeout to 1200 seconds and 30 seconds respectively.

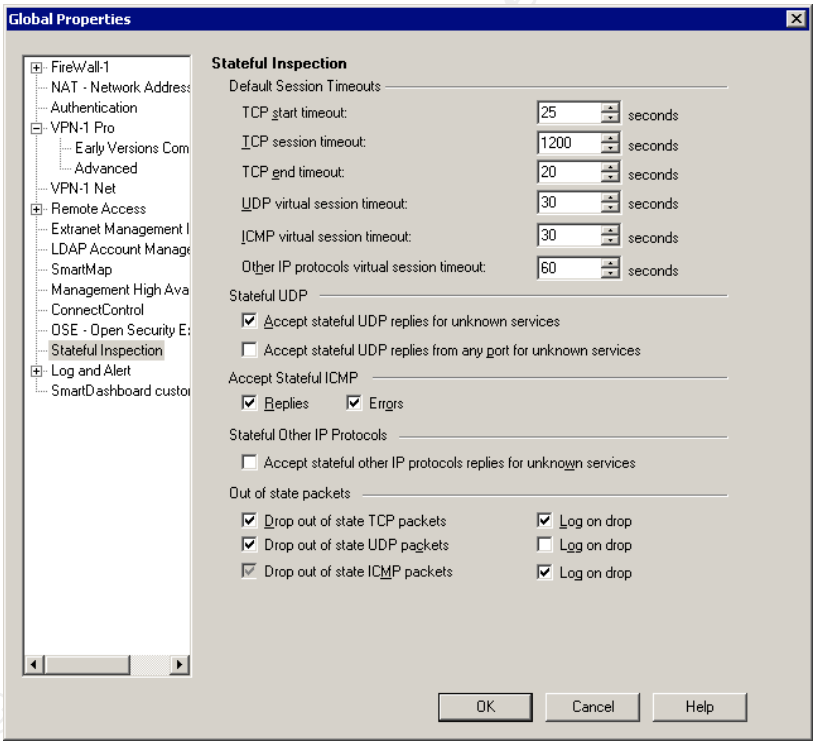


Figure 2: Stateful Inspection Properties

Check Point SmartDefense

Check Point SmartDefense is a scaled down Intrusion Detection System built into the firewall software. The firewall is configured to detect, block and log irregularities it receives.

Setting	Status	Tracking	Configurations
Denial of Service – Accumulate successive events	Enabled	Alert	Resolution: 10 seconds Time interval: 360 seconds Attempts number: 10
Teardrop	Enabled	Alert	None
Ping of Death	Enabled	Alert	None
LAND	Enabled	Alert	None
IP Fragment Sanity Check	Enabled	Log	None
IP Packet Sanity	Enabled	Log	None
Maximum Ping Size	Enabled	Log	Size 128 bytes
TCP SYN Attack	Enabled	Log Attacks only	Timeout 5 secs Attack threshold 200 SYN packets
TCP Small PMTU	Enabled	Log	Minimum MTU: 350 bytes
TCP Sequence Verifier	Enabled	Log	Only anomalous (do not normally appear in legitimate connections)
DNS - UDP protocol enforcement	Disabled	N.A.	This configuration interferes with normal DNS queries and is disabled.
FTP Bounce	Enabled	Alert	None
FTP Security Server	Not used	N.A.	None
General HTTP Worm catcher	Enabled	Alert	None
HTTP Security Server	Not used	N.A.	None
SMTP Security Server	Not used	N.A.	None
Successive Address Spoofing	Enabled	Alert	Resolution: 300secs Time Interval: 3600secs Attempts: 10
Successive Local Interface Spoofing	Enabled	Alert	Resolution: 10secs Time Interval: 360secs Attempts: 5
Successive Port Scanning	Enabled	Alert	Resolution: 5secs Time Interval: 120secs Attempts: 30
Successive Alerts	Enabled	Alert	Resolution: 60secs Time Interval: 600secs Attempts: 100
Successive Multiple Connections	Enabled	Log	Resolution: 10secs Time Interval: 60secs Attempts: 100

Table 26: SmartDefense Settings

VPN Security Policy

The firewall doubles as the VPN gateway for GIAC Enterprises. This allows the Mobile Sales Staff and Teleworkers to access the corporate network with reduced risk of information leakage.

At the client end, Check Point SecureClient NG FP3 provides IPSec encryption to the firewall. In addition, SecureClient has desktop firewall features that can be configured from the firewall management console.

To support SecureClient VPN, VPN-1 Pro and SecureClient Policy Server are enabled on the firewall object.

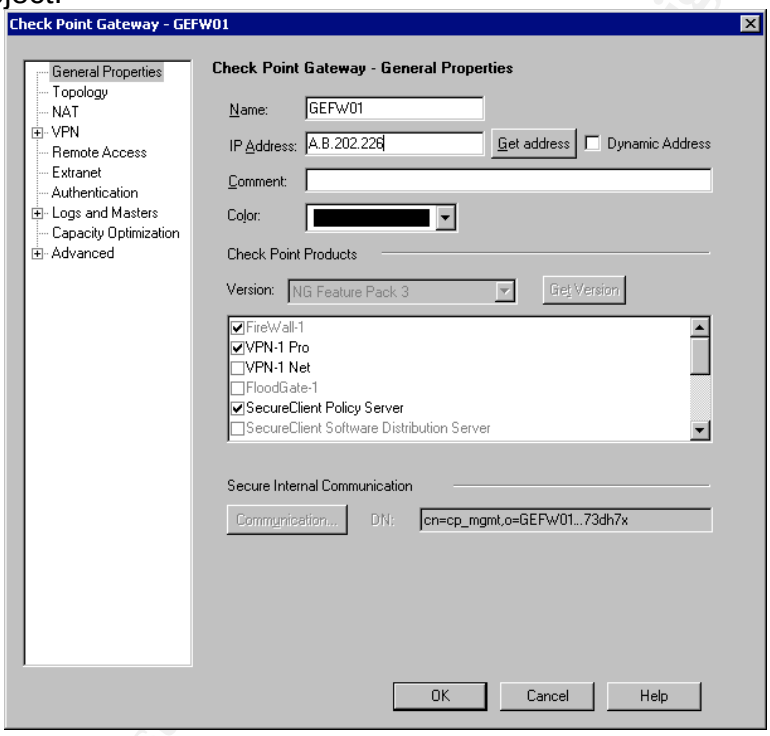


Figure 3: VPN-1 Pro and SecureClient Policy Server Enabled

The VPN Domain is the network or group of hosts that are assessable to the VPN clients. For GIAC Enterprises, the VPN Domain is configured to be the VPNaccess group.

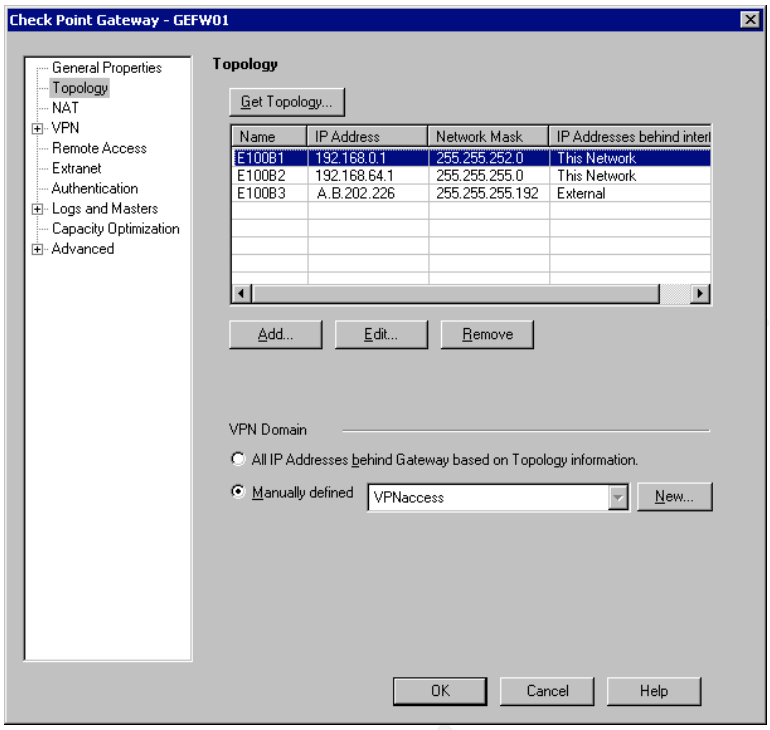


Figure 4: Firewall Module VPN Domain

The VPN module is configured to participate in a VPN Community and the Internal Certificate Authority is defined in the trusted Certificate List as shown in Figure 5.

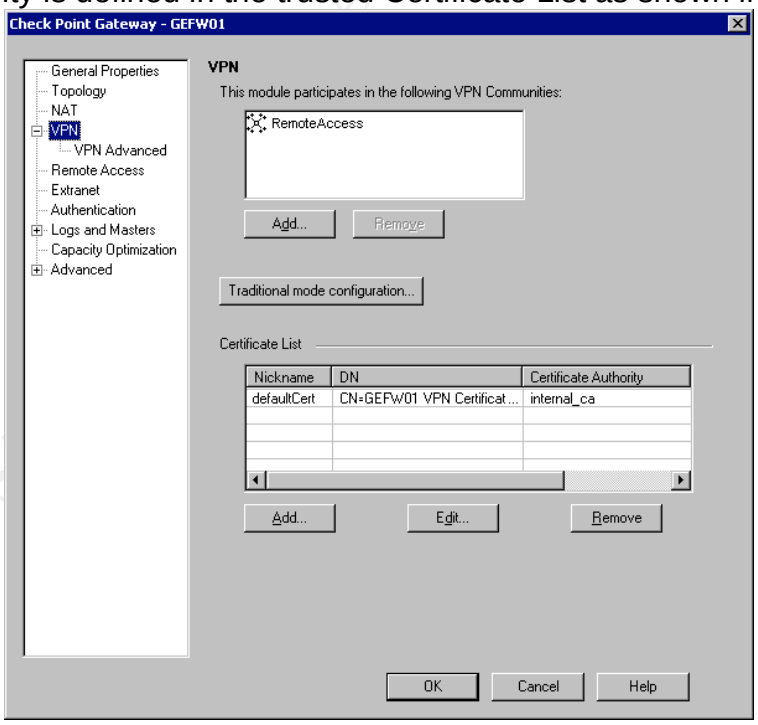


Figure 5: Firewall-1 Module VPN Configuration

The VPNUsers group is configured as the Policy Server users. Only members of this group are allowed to authenticate with the Policy Server to retrieve the SecureClient desktop policy.

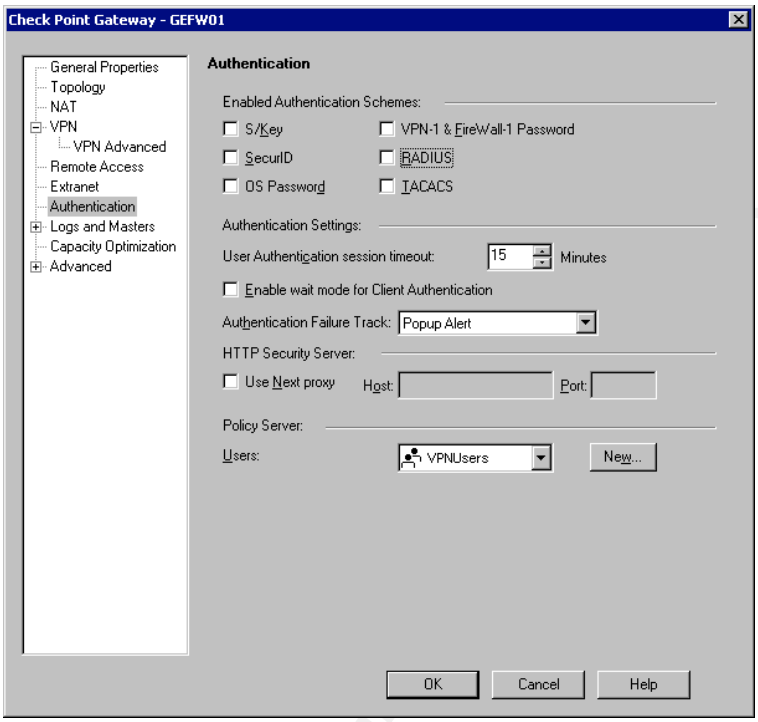


Figure 6: Firewall Module Policy Server Authentication

Internet Key Exchange

IKE supports either pre-shared key or certificates for the client to authenticate with the VPN gateway. Since Check Point Firewall-1 NG FP3 has an Internal Certificate Authority, GIAC Enterprises has opted to use certificate based IKE authentication.

Each Mobile Sales Staff and Teleworker and Firewall-1 are assigned a Firewall-1 account and certificate. These accounts are added to the VPNUsers group to allow them access to the Intranet resources based on the firewall policies.

Check Point SecureClient NG FP3 uses IPSec Encrypted Security Payload to encrypt data between the client and the VPN domain. IKE configuration is configured in the firewall Global Properties window as shown in Figure 7.

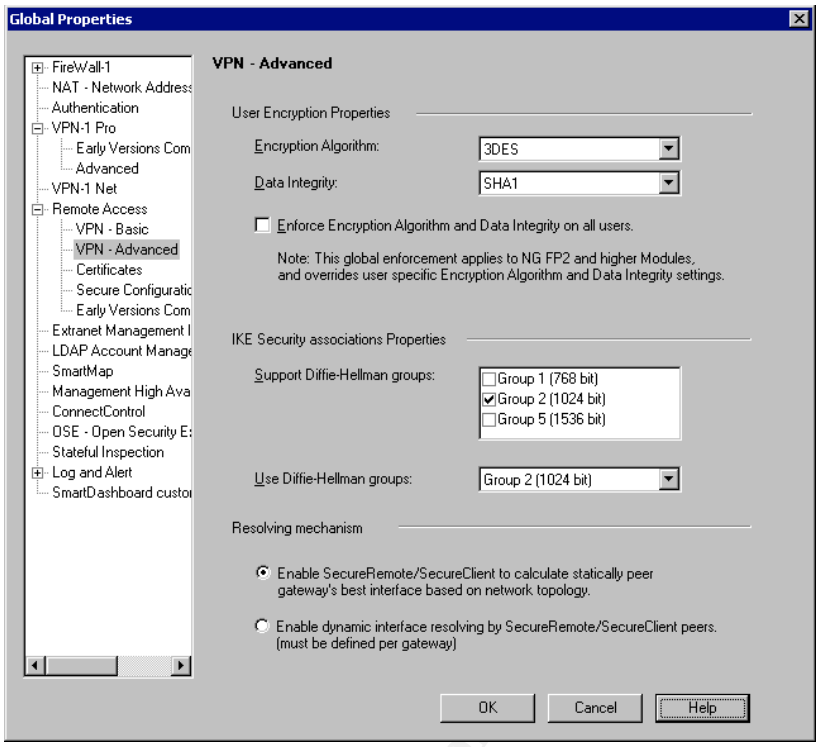


Figure 7: Client VPN IKE Settings

VPN Community

Check Point VPN-1/Firewalll-1 NG FP3 uses the concept of VPN community to simplify rule base creation. The RemoteAccess community is pre-defined in the firewall. By default, all VPN-1 users participate in RemoteAccess. We replaced All Users with VPNUsers to limit the users who can access the network via VPN.

Internal DNS Server

SecureClient is capable of redirecting the clients' DNS queries to a specified Intranet DNS server if the name matches some defined domain suffix. This allows the client to resolve the Intranet server names that cannot be resolved using any external DNS servers. The internal DNS server is specified via the SecuRemote DNS server object.

Configuration	Value
Name	GIAC_DNS
Domain suffix	Giacent.msad
Internal DNS Server	GEAD01
Maximum Prefix Label Count	1
Encrypt DNS traffic (to Internal DNS server)	Yes

Table 27: Internal DNS Server Configuration

Policy Server

The policy server provides SecureClient with the desktop firewall rules. Since there is only a single VPN-1/Firewall-1 gateway, GEFW01 is configured as the policy server.

The ruleset allows stateful outgoing connections from the workstation and blocks all incoming connections. All connections are logged as shown in Table 28 below.

No	Source	Desktop	Service	Action	Track	Comments
1	Any	All Users @any	Any	Block	Log	Deny Incoming connections
2	All Users @any	VPNaccess	Any	Encrypt	Log	Encrypt connections to corp office
3	All Users @any	Any	Any	Accept	Log	Allow outgoing connections

Table 28: Desktop Firewall Rules

Firewall Policy Tutorial

This section explains the process of configuring the firewall policy that was described above. The tutorial covers the following topics

1. A brief mention on Windows server and Check Point VPN-1 & Firewall-1 installation
2. Create and configure the Firewall-1 objects to be used in the firewall policy
3. Configure the Firewall Global Properties.
4. Configure the firewall policy rulebase

The VPN client, SecureClient, configuration is not discussed in this tutorial.

Installation

Windows 2000 Server installation

As the firewall is running on a Windows server, extra care is require during installation as the operating system has several vulnerabilities out-of-the box. When installing the Windows 2000 Server,

1. Do not connect the server to the office network until the firewall is installed and tested. During installation, the server does not have any firewall protection and may be vulnerable to any network worms or viruses.
2. Boot the server from a Windows 2000 CDROM to run the installation program.
3. Format all the disks with NTFS.
4. Install the minimum optional components. Components such as the IIS, Certificate Server, Accessibility Wizard, Games, Multimedia etc. are not required and should not be installed on the firewall.
5. Assign static IP Address for all network interfaces. You must only define the default gateway only on the network interface that will connect to the border router. Otherwise, routing to the Internet may fail.

6. Enable IP routing in Windows Registry as specified in Microsoft KB 230082[23].
7. Patch the server with the latest service pack and all required hotfixes. Use the Microsoft Baseline Security Analysis tool to ensure all the patches are successfully installed. MBSA verifies patches by comparing checksums of Windows files.
8. Refer to the Microsoft Windows 2003 Security Guide[24] to harden the server as a bastion host.

VPN-1 & Firewall-1

Place the Check Point VPN-1 & Firewall-1 CD into the firewall server and install the following components:

1. VPN-1 & Firewall-1 –
   Install both the Enforcement Module and the Management Server.
   Install the Enterprise Primary Management type
   Install without the backup compatibility package.
2. Smart Clients – install all clients
3. Policy Server

The SVN foundation is a mandatory module.

After the installation, you should

1. Enter the software licenses
2. Define the firewall administrator accounts and (strong) passwords
3. Key in random characters to seed cryptographic operations
4. Initiate the Internal Certificate Authority. This is an important step as the Certificate Authority enables the creation of a secured channel between the firewall module and the management server. You may not be able to logon to the firewall management clients if the CA is not properly initialized.
5. Since the firewall is managed locally, you do not need to define any management clients.
6. Install the latest hotfixes

For the optimum performance, tune the firewall and operating system as specified in the Check Point VPN-1 & Firewall-1 NG Performance Tuning Guide[25].

Secure the DCE-RPC

Firewall-1 is capable of inspecting DCE-RPC connections to allow only specific RPC services that need to pass the firewall based on the RPC service identifiers (UUID). We need to enhance the security for the Firewall's DCE-RPC inspection to prevent RPC worms such as Blaster and Nachi[26] from entering the network through the firewall.

1. Download and install the dcerpc.def inspect code from Check Point web site http://www.checkpoint.com/securitycenter/advisories/2003/files/cpai-2003-11/fp3/dcerpc.def.gz

[23] http://support.microsoft.com/default.aspx?scid=kb;EN-US;230082
[24] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/win2003/w2003hg/sgch00.asp
[25] http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html
[26] http://www.checkpoint.com/securitycenter/advisories/2003/cpai-2003-11.html

2. Disconnect the Firewall from the network
3. Stop the firewall service by running the CPSTOP command
4. Backup the existing $FWDIR\lib\dcerpc.def ($FWDIR is the root folder of the firewall installation)
5. Copy the downloaded inspect code to $FWDIR\lib\dcerpc.def

Edit $FWDIR\lib\table.def and replace the line that contains

```
dcerpc_binds = dynamic sync refresh expires TCP_TIMEOUT;
```

to

```
dcerpc_binds = dynamic sync refresh expires 40;
```

6. Start the firewall service by running the CPSTART command
7. Reinstall the policy for the changes to take effect.

Managing Firewall-1 Policy

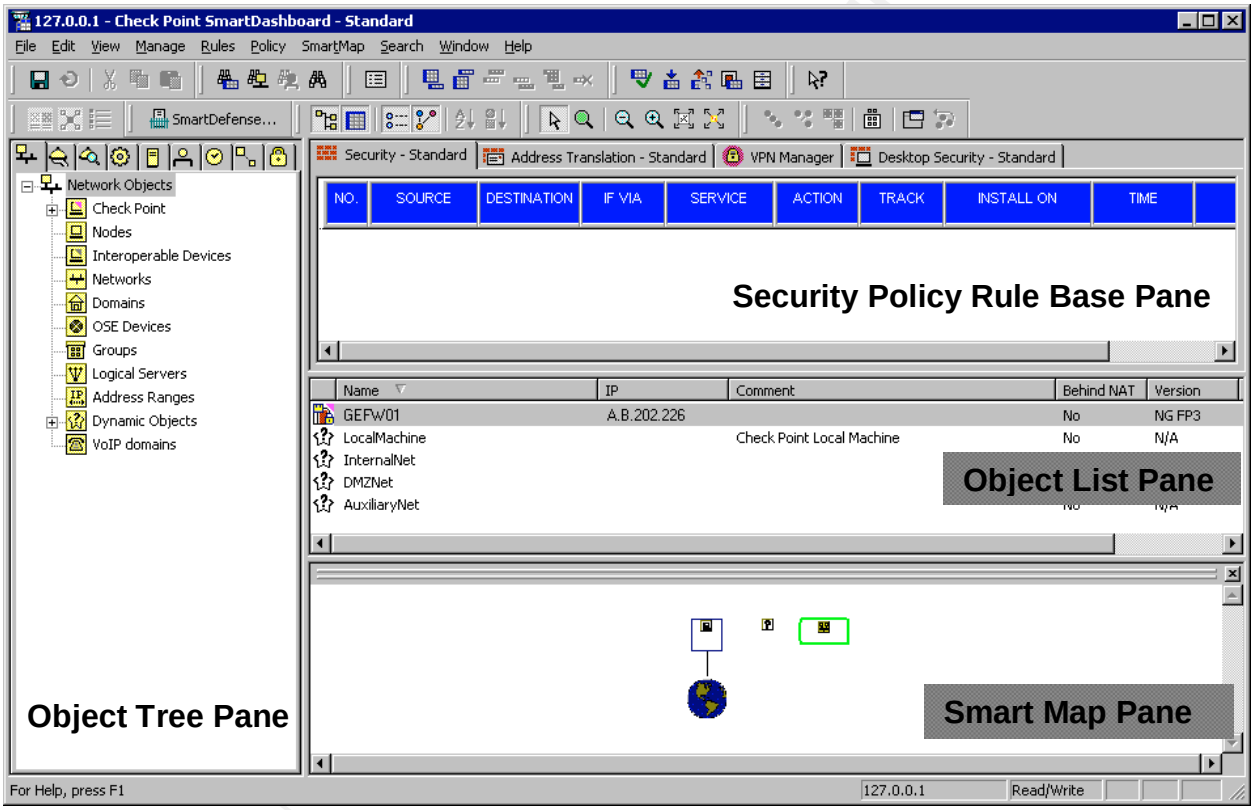


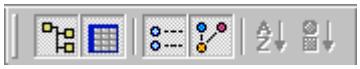
Figure 8: Check Point SmartDashboard

Check Point SmartDashboard is the tool you will be using to configure the firewall and policy rule base. You can start the SmartDashboard from *Windows Start Menu -> Program Files -> Check Point Smart Clients*. Login using the administrator account name and the password defined during installation. Note that both name and passwords are case sensitive.

SmartDashboard window comprises of four panes:

1. Objects Tree pane – where all objects are listed in a tree structure
2. Rule Base pane – the security rule base is displayed here

3. Object Lists pane – displays a summary of the objects in the selected container in the Objects Tree pane.
4. SmartMap – displays the network structure based on the objects defined. This pane may not be available without additional license.

The *Panes toolbar*  have buttons that allows you to toggle show or hide each of the four panes.

Create Objects

We will first create Network Objects that will be used in the firewall policy. Network Objects are nodes, gateways, networks or groups that can be specified as the source or destination in the policy.

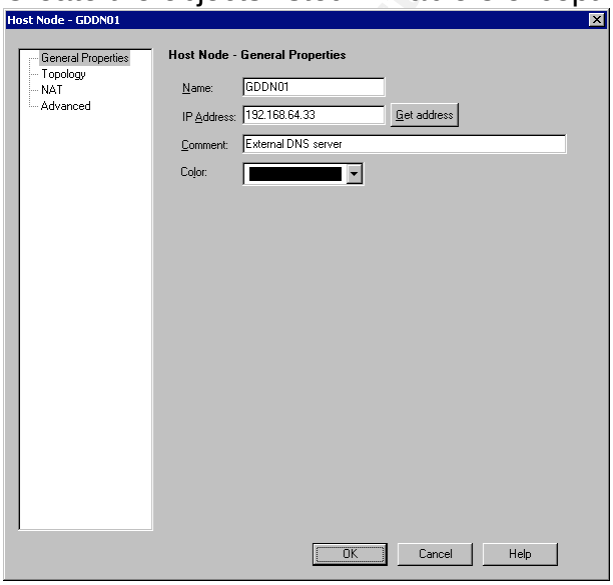
Before creating the Network Objects, first ensure the *Object Tree* view is visible as shown in Figure 8 – the Object View Tree on the left of the SmartDashboard window. If the tree is not visible, toggle the View Objects Tree toolbar button  .

Hosts

To create a new hosts,

1. Click on the *Network Objects* tab  in the *Object Tree pane*.
2. Right-click the *Nodes* container in the *Object Tree pane* and select *New Node -> Host*. The *Host Node* dialog box appears as in Figure 9.
3. Enter the host's *Name*, *IP Address* and *Comment*.
4. If the object has a NAT address, click on *NAT* in the navigation pane and fill in the NAT details of the host. Set the *Install on Gateway* value to *All*. Enabling NAT from the object properties automatically creates the Network Translation Rules for the object, provides automatic ARP configuration.
5. Click the *OK* button to save and close the window.

Create the objects listed in Table 3 except for the firewall object, GEFW01.



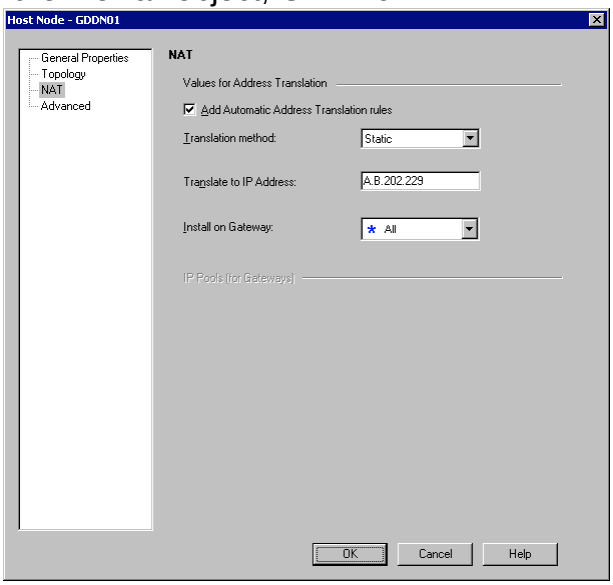


Figure 9: Host Node Properties

Networks

We then create the Networks:

1. Right-click the *Networks* container in the *Object Tree* pane and select *New Network*. The *Network Properties* dialog box appears as shown in Figure 10.
2. Enter the Network *Name*, *IP Address*, *Net Mask* and *Comment* fields.
3. If the object has a NAT address, click on *NAT* in the navigation pane and fill in the NAT details of the Network. Set the *Install on Gateway* value to All.
4. Click the *OK* button to save and close the window.

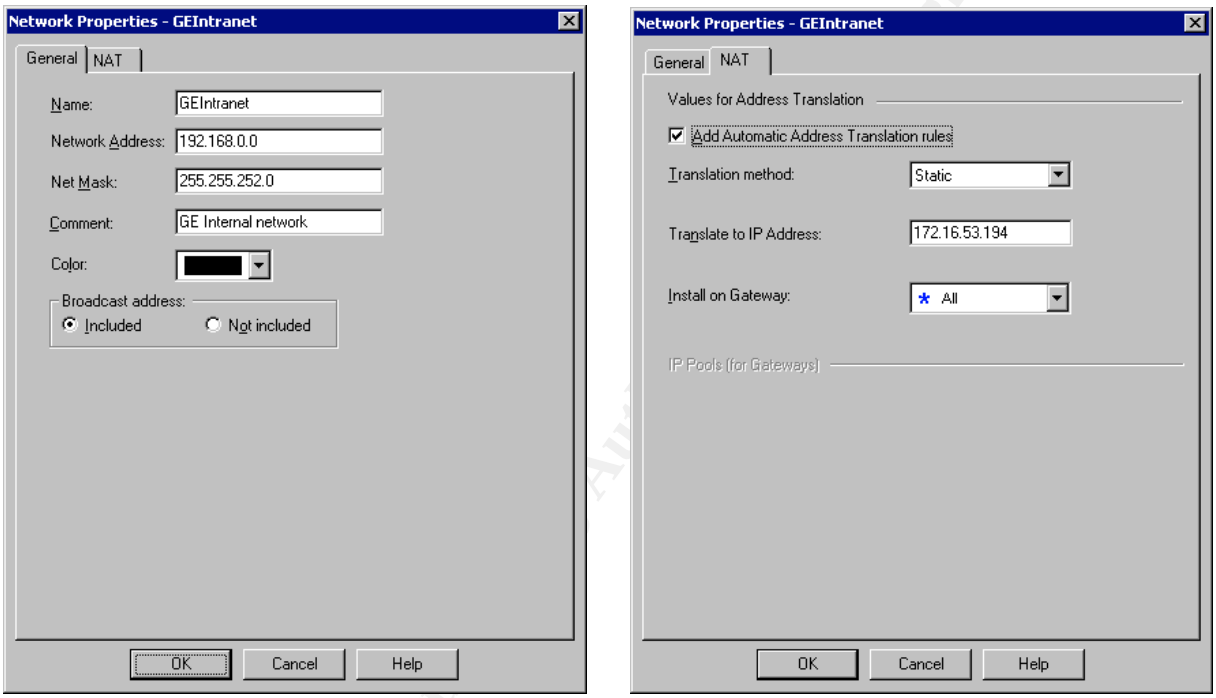


Figure 10: Network Properties

Network Groups

Next, we create the Network Groups listed in Table 7. For the use of our policy, we need only to create Simple Groups.

1. Click on the *Network Objects* tab  in the *Object Tree* pane.
2. Right-click the *Groups* container in the *Object Tree* pane and select *New Groups -> Simple Groups*. The *Group Properties* dialog box appears.
3. Enter the group *Name* and *Comment*.

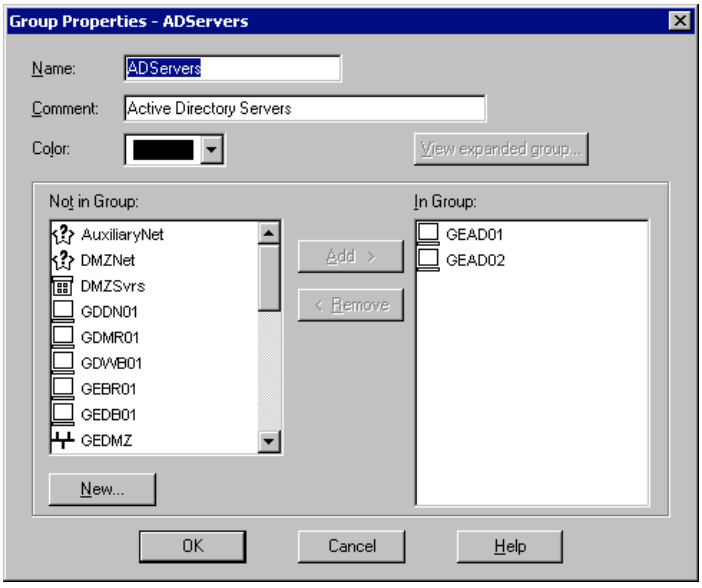


Figure 11: Groups

4. Select objects in the Not in Group list and click the Add button to move them to the In Group list.
5. Click the OK button to save and close the window.

Services

We do not need to define any services as all network services used by GIAC Enterprises have been pre-defined in SmartDashboard.

User Groups

Members of the VPNUsers group are granted VPN access to GIAC Enterprises network.

1. Click on the *Users and Administrators* tab in the *Object Tree* pane.
2. Right-click the *Groups* container in the *Object Tree* pane and select *New Group*. The *Group Properties* dialog box appears.
3. Fill the *Name* and *Comment* text boxes for the user group specified in Table 7.
4. Click the *OK* button to save and close the window.

Intranet DNS server

1. Click on the *Servers* tab in the Object Tree pane.
2. Right-click the *SecuRemote DNS* container in the *Object Tree* pane and select *New SecuRemote DNS*. The *SecuRemote DNS Properties* dialog box appears.
3. Fill the *Name* text box and other details as given in Table 27. The results should be similar to what is shown in Figure 12.

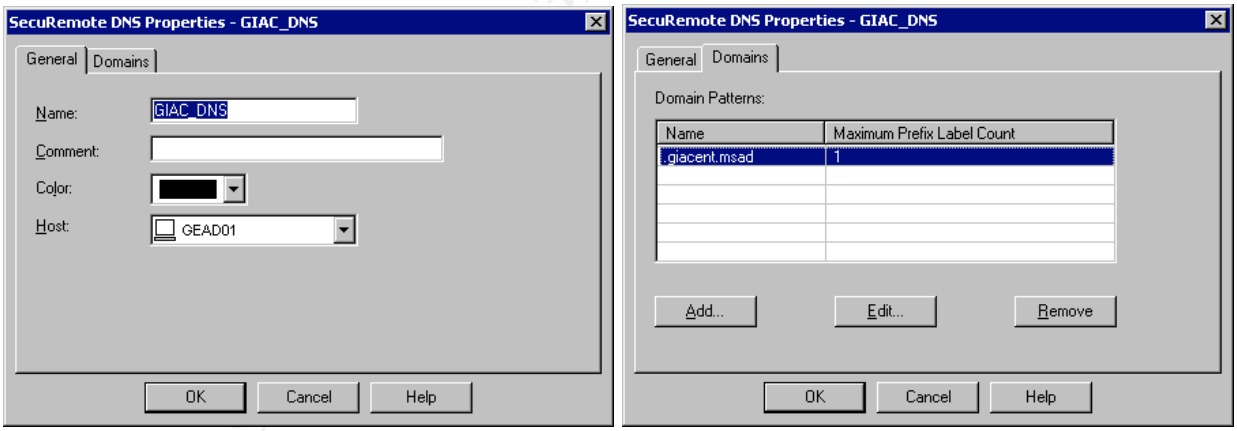


Figure 12: SecuRemote DNS Properties

VPN Community

Next, we configure the RemoteAccess VPN Community.

1. Click the *VPN Manager* VPN Manager tab in the *Rule Base* pane.
2. Double-click the *RemoteAccess* icon RemoteAccess

3. Select *Participating User Groups* in the Navigation pane. Remove All Users and add the VPNUsers group as shown in Figure 13.

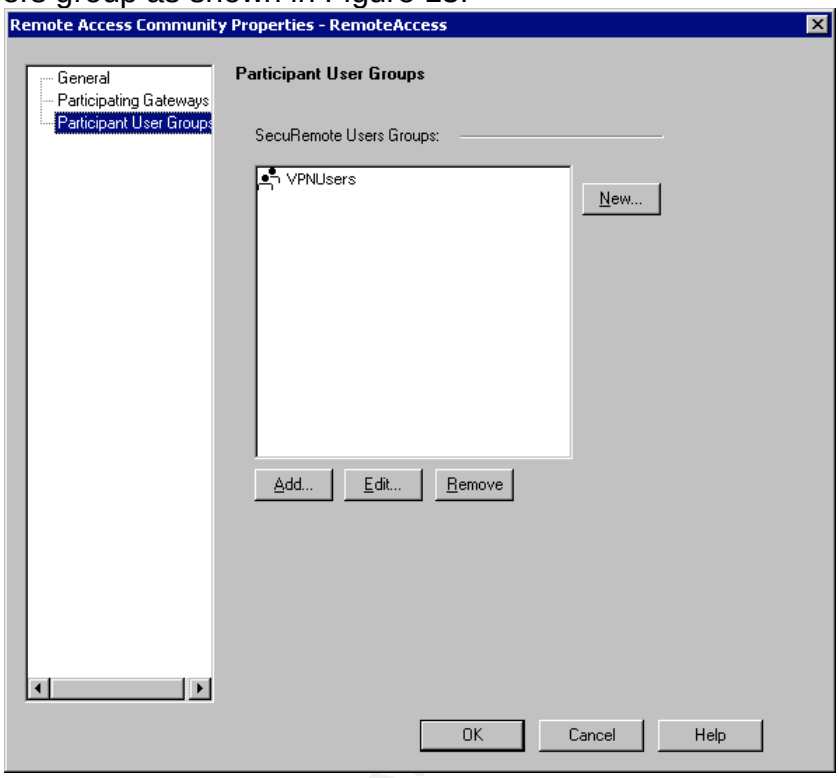


Figure 13: RemoteAccess Community Properties

Firewall Host Object

We can configure the firewall host object now that all required objects have been created. The host object is pre-created during software installation and placed in the Check Point container in the Object Tree. It requires further configuration.

1. Click on the *Network Objects* tab  in the *Object Tree* pane.
2. Navigate to the *Check Point* container in the *Object Tree* pane and double-click on the GEFW01 firewall object
3. In the Global Properties page, select to enable *VPN-1 Pro* and *SecureClient Policy Server* in the *Check Point Products* list box as shown in Figure 3.
4. Click on *Topology* in the Navigation pane. Note that the Interface names may be different from those specified in Table 25. If any changes are made to the network interfaces after the firewall has been installed, click on the *Get Topology* button to update the settings here.
5. Select each of the network interfaces and edit the network address connected to each interface.
6. In the *VPN Domain* section, select the *Manually defined* radio button. Select VPNaccess from the drop down list as shown in Figure 4.
7. Select *VPN* in the Navigation pane. Add *Remote Access* to the VPN Communities.
8. Click on the *Traditional mode configuration* button. If a dialog box appears with the message “Traditional mode configurations requires signed certificate”, click the *OK*

button to create a new certificate. The *Traditional mode IKE properties* window appears. In the *Support key exchange encryption* list box, uncheck *DES* and *CAST*.

9. Select the *Authentication* container in the Navigation pane and disable all authentication schemes as we do not require them.
10. In the *Policy Server Users* drop list box, select VPNUsers as shown in Figure 6.
11. Click the *OK* button to save the settings and close the window.

Firewall-1 Global Properties

The Check Point Firewall-1 Global Properties controls behavior of the firewall and can affect the policy you create. The default Global Properties configuration should be modified as follows:

1. Click on the *Edit Global Properties* button  in the SmartDashboard toolbar.
2. Disable the implied rules as shown in Figure 14. We will control these connections from the rule base.
3. Enable the *Log Implied Rules* checkbox.

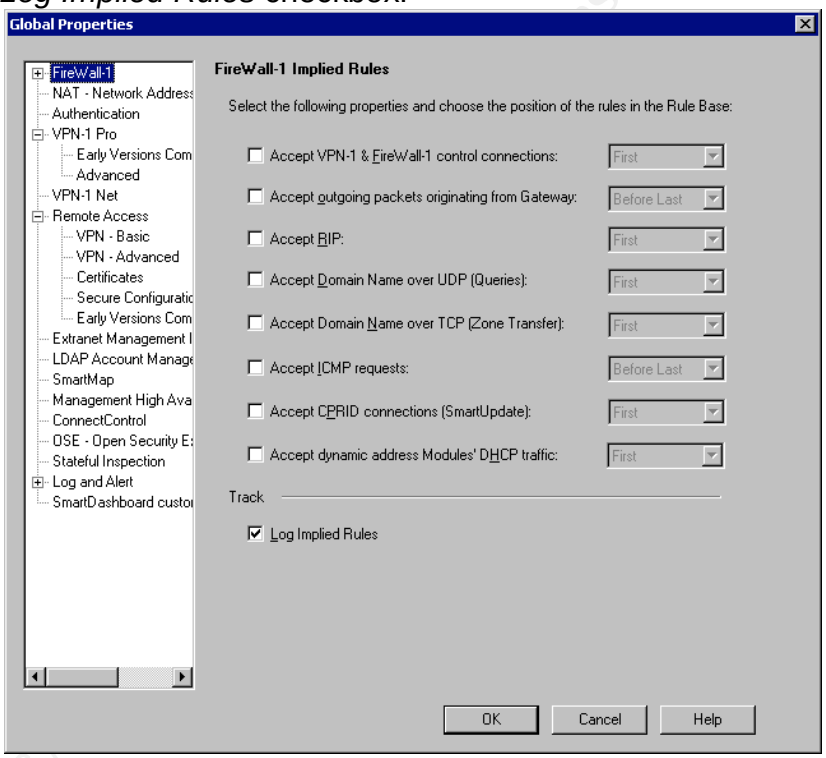


Figure 14: Firewall-1 Implied Rules

4. Select *NAT* in the Navigation pane. Ensure all the *Automatic NAT* and *Manual NAT* options are enabled as shown in Figure 15.

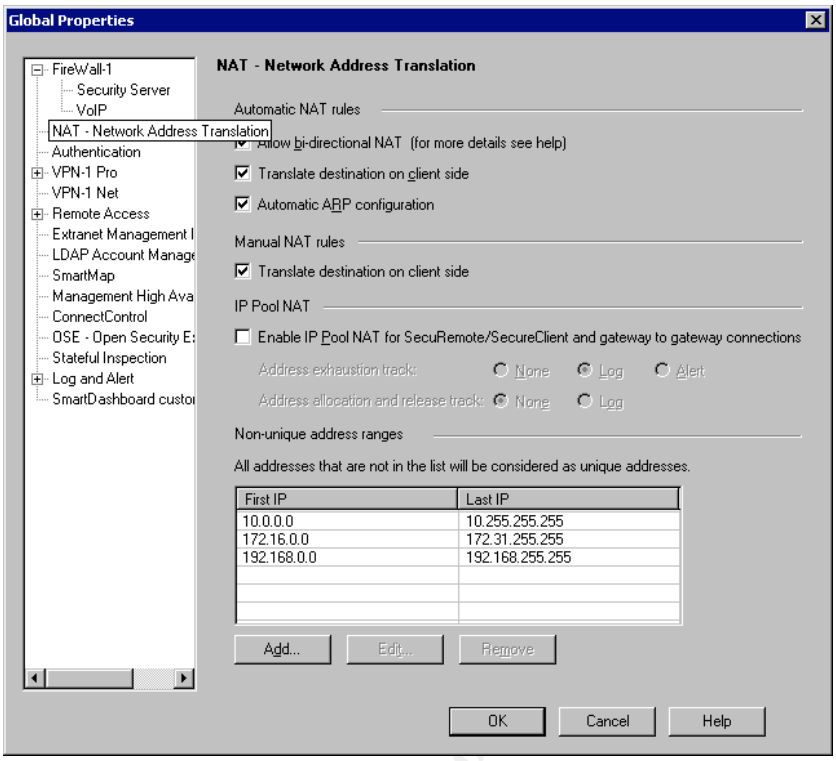


Figure 15: Firewall-1 Global NAT Properties

5. Select Authentication in the Navigation pane. Ensure the Authenticate internal users with this suffix only is selected and the suffix configured begins with OU=users,O=GEFW01 as shown in Figure 16.

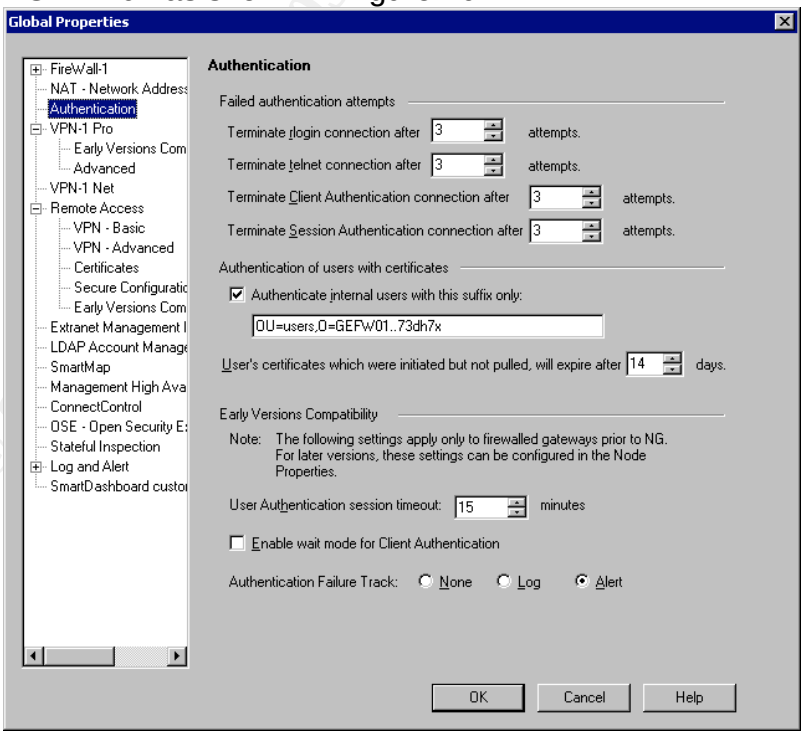


Figure 16: Global Properties - Authentication

6. Select *Remote Access* in the Navigation pane. Ensure *Encrypt DNS* is enabled

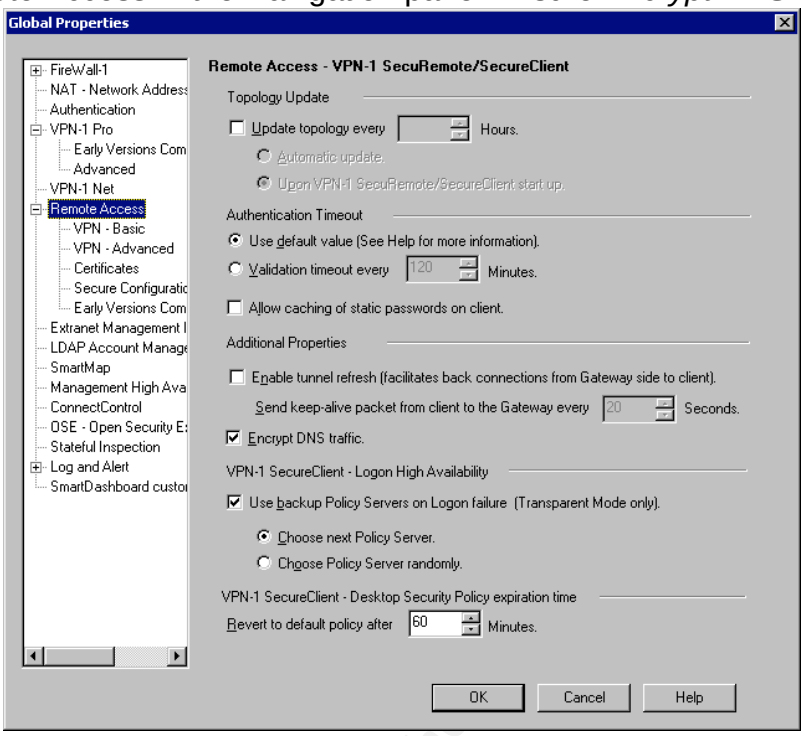


Figure 17: Remote Access Global Properties

7. Select *Remote Access – VPN Basic* in the Navigation pane. Uncheck *Hybrid Mode*. Ensure only *Public Key Signatures* and *Enable IP compression* is checked as shown in Figure 18.

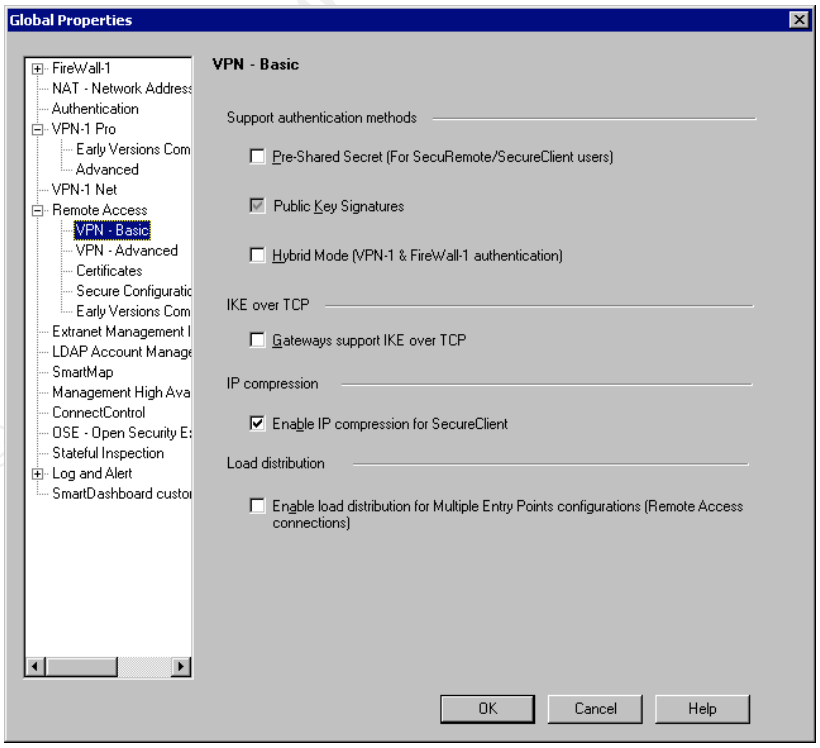


Figure 18: Remote Access VPN Basic Global Properties

8. Select *Remote Access – VPN Advanced* in the Navigation pane. Ensure the settings are the same as shown in Figure 7.
9. Select *Stateful Inspection* in the Navigation pane. Change the TCP session timeout and UDP virtual session timeout as shown in Figure 2.

Configure SmartDefense

1. Click on the SmartDefense button 

in the toolbar. The SmartDefense settings window appears.
2. Configure SmartDefense as specified in Table 26.

Configure the Firewall-1 Security Policy

You will be using the Check Point SmartDashboard Security Policy Rule Base Pane to define the firewall policy. The rule base is displayed in the form of a table.

Figure 19 Rule Base Fields

Each rule consists of 9 properties as shown in Figure 19.

Rule Base Property	Description
No.	The Rule Number is a running number starting from 1 for the first rule. The number of a rule can change when a rule above it is added or removed.
Source	Matches the source IP address of the IP packet. You can add or remove Network Objects, Groups or Users in this property. The property can be negated to match any source that is not specified.
Destination	Matches the destination IP address of the IP packet. You can add or remove Network Objects, Groups in this property. The property can be negated to match any destination that is not specified.
IF VIA	Specifies if the connection is from a VPN Community. Specify a VPN community or leave the value to Any to specify a non-VPN connection.
Service	Matches the protocol type or characteristics. For TCP and UDP, it matches the port number. ICMP packets are matched against the ICMP type and code. Firewall-1 support other IP protocols and dynamic RPC services. Specify The property can be negated to match any services that are not specified.
Action	Specifies the action that will be taken when the connection matches the rule. The actions supported are: Accept – the connection is routed to the destination Drop - the connection is blocked Reject – the connection is blocked. An ICMP port unreachable is sent to the client User Auth - grants access on per connection basis. Supports only TELNET, FTP, RLOGIN and HTTP protocols. Client Auth - grants access on a per host basis. Session Auth - grants access using the Session Authentication Agent. Works with any service.
Track	Specifies the logging method. The following methods are provided: None - no logging or alerting for the connection Log - log the connection Account - log in Accounting format Alert - issue an alert Mail – send a mail alert SNMP Trap - issue an SNMP trap User defined -issue a User Defined Alert
Install on	Specifies where the rule is installed on. Possible options are:

Rule Base Property	Description
	Gateway - enforce on all objects defined as Gateways Embedded devices - enforce on all embedded devices Targets - enforce on specified objects (inbound & outbound) Dst - enforce inbound connection to object(s) specified in the Destination property of the rule Src - enforce outbound connection from object(s) specified in the Source property of the rule OSE Device - enforce on Open Security Extension devices i.e., Cisco routers.
Time	Specifies the time of the day the rule is enforced.
Comment	Text field to comment on the rule. You can use it to note the purpose of the rule, the administrator who modified it and when it was last modified.

Table 29: Firewall-1 Rule Properties

The *Rules Toolbar*, 

, provides buttons for you to add and remove rules in the rule base as described in Table 30.

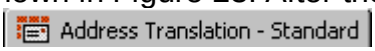
Button	Purpose
	Add new rule at the bottom of the rule base
	Add new rule at the top of the rule base
	Add new rule above the selected rule
	Add new rule below the selected rule
	Delete the selected rule

Table 30: SmartDashboard Rules Toolbar buttons

To add an object or action in a rule, right-click the relevant cell and select the *Add* command from the pop-up menu. The pop-up menu is context sensitive and shows only the relevant commands for each property in the rule base table.

To remove an item from a rule, select the item and press the *delete* key on the keyboard. If no items are specified in the *Source*, *Destination*, *IF VIA* or *Service* property, the property value defaults to *Any*.

You can exclude objects in the *Source*, *Destination* or *Service* property by *right-click* the property cell and select the *Negate cell* command from the pop-up menu. Note that all objects in the cell are negated – you cannot negate a single object in the cell.

Now you can construct the rule base as shown in Figure 23. After the rule base is created, click the *Address Translation* tab 

in the rule base pane to view the Network Address Translation rule base. Click on the *Add rule at the Top*  toolbar button to create the manual NAT rule in Table 23. The resultant NAT rule base should look the same as in Figure 20.

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	GENet	GENet	Any	Original	Original	Original	Policy Targets	no NAT for internal connections
2	GDDN01	Any	Any	GDDN01 (Valid Address)	Original	Original	All	Automatic rule (see the network object data).
3	Any	GDDN01 (Valid Address)	Any	Original	GDDN01	Original	All	Automatic rule (see the network object data).
4	GDMR01	Any	Any	GDMR01 (Valid Address)	Original	Original	All	Automatic rule (see the network object data).
5	Any	GDMR01 (Valid Address)	Any	Original	GDMR01	Original	All	Automatic rule (see the network object data).
6	GDWB01	Any	Any	GDWB01 (Valid Address)	Original	Original	All	Automatic rule (see the network object data).
7	Any	GDWB01 (Valid Address)	Any	Original	GDWB01	Original	All	Automatic rule (see the network object data).
8	GEIntranet	GEIntranet	Any	Original	Original	Original	All	Automatic rule (see the network object data).
9	GEIntranet	Any	Any	GEIntranet (Hiding Addres	Original	Original	All	Automatic rule (see the network object data).

Figure 20: NAT Rule Base

Once the rule base is complete you can verify it:

1. Click on the *Verify Policies*  toolbar button.
2. Dismiss the *Address Translation – Routing* warning window by clicking the OK button.
3. In the *Verify* window, ensure the *Security and Address Translation* is check and click the *OK* button.
4. If there's a problem with the policy, the policy verifier will indicate the rules that have problems. Click the OK button to close the window.
5. Correct any problems and repeat steps 1 through 4 until the rules are verified successfully.

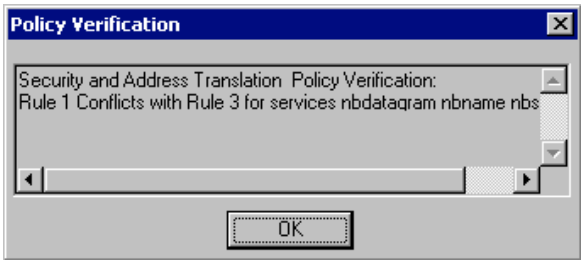


Figure 21: Verify Failure Sample

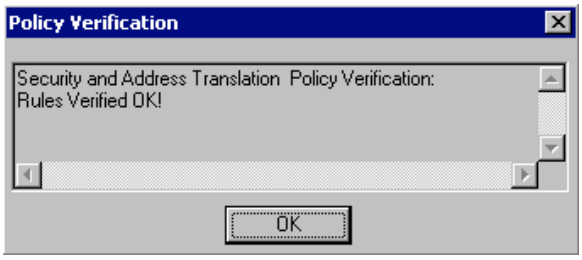


Figure 22: Verify Success

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Drop Rule								
1	* Any	* Any	* Any	NBT UDP bootp	drop	- None	* Policy Targets	* Any	Drop NetBIOS_bootp traffic without logging
2	* Any	GEFW01	* Any	TCP FW1_topo UDP IKE TCP FW1_pslogon_N UDP FW1_scv_keep_	accept	Log	* Policy Targets	* Any	VPN access
3	GEFW01	* Any	* Any	UDP IKE	accept	Log	* Policy Targets	* Any	VPN access
4	* Any	GEFW01	* Any	* Any	drop	Alert	* Policy Targets	* Any	Firewall stealth
	Web Applications								
5	* Any	GDWB01	* Any	TCP http TCP https	accept	Log	* Policy Targets	* Any	Anyone can http/s to ext web server
6	GDWB01	GEDB01	* Any	TCP MS-SQL-Server	accept	Log	* Policy Targets	* Any	ext web server needs data from sql server
7	GEPX01	GENet	* Any	TCP ftp TCP http TCP https	accept	Log	* Policy Targets	* Any	Only proxy server can surf the Internet
	DNS Queries								
8	* Any	GDDN01	* Any	UDP domain-udp	accept	Log	* Policy Targets	* Any	Any host can query DNS server
9	GDMR01 ADServers	ISPCDNS1 ISPCDNS2	* Any	dns	accept	Log	* Policy Targets	* Any	Only mail relay and ad servers can forward dns queries
	Mail relay								
10	GDMR01 GEEM01	GDMR01 GEEM01	* Any	TCP smtp	accept	Log	* Policy Targets	* Any	Exch server can send and recv mails from relay svr
11	GENet	GDMR01	* Any	TCP smtp	accept	Log	* Policy Targets	* Any	Incoming mails from Internet via relay svr
12	GDMR01	GENet	* Any	TCP smtp	accept	Log	* Policy Targets	* Any	relay server can send outgoing Internet mails
	Mobile Sales Staff and Teleworkers								
13	VPNusers@	ADServers	RemoteAccess	TCP microsoft-ds dns DCE MSExchangeDSI	accept	Log	* Policy Targets	* Any	access Directory, DNS and file service
14	VPNusers@	GEEM01	RemoteAccess	TCP http TCP https DCE MSExchangeDirF DCE MSExchangeIS	accept	Log	* Policy Targets	* Any	access Exch server MAPI and OWA
15	VPNusers@	GEDB01	RemoteAccess	TCP MS-SQL-Server	accept	Log	* Policy Targets	* Any	access the sql server
16	VPNusers@	GESU01	RemoteAccess	TCP http	accept	Log	* Policy Targets	* Any	get virus updates
	Border Router								
17	GEBR01	GESL01	* Any	UDP syslog	accept	Log	* Policy Targets	* Any	border router syslog
	Time Sync								
18	DMZSvrs GEFW01	ADServers	* Any	UDP ntp-udp	accept	Log	* Policy Targets	* Any	sync time with AD servers
19	ADServers	time.nist.gov	* Any	UDP syslog	accept	Log	* Policy Targets	* Any	AD servers sync time with external time
	Daily Connections								
20	DMZSvrs	GESU01	* Any	TCP http	accept	Log	* Policy Targets	* Any	DMZ servers gets updates from software update server
21	GDMR01	GESU01	* Any	TCP ftp	accept	Log	* Policy Targets	* Any	relay svr to get updates using ftp
22	ISPSDNS1 ISPSDNS2	GDDN01	* Any	TCP domain-tcp	accept	Log	* Policy Targets	* Any	allow ISP Secondary DNS servers to perform Zone transfers
	Firewall outgoing								
23	GEFW01	GEIntranet	* Any	ICMP dest-unreach	accept	Log	* Policy Targets	* Any	firewall can send rejects
	Last								
24	* Any	* Any	* Any	* Any	drop	Log	* Policy Targets	* Any	drop and log everything else

Figure 23: Firewall Policy

Now, you can install the policy into the firewall inspection module:

1. Click on the *Install Policies* toolbar button  .
2. Dismiss the *Address Translation – Routing warning* window by clicking the *OK* button.
3. Dismiss the *SmartDashboard Warning* window by clicking the *OK* button.
4. The *Install Policy* window shown in Figure 24 appears. Ensure the *Advanced Security checkbox* for the firewall is checked and click the *OK* button.
5. If the installation fails, click the *Show Errors* button to determine the problem and correct it. Repeat steps 1 through 4 to re-install the policy.
6. If the installation is successful, the click the *Close* button. The firewall is now successfully configured and ready for testing.

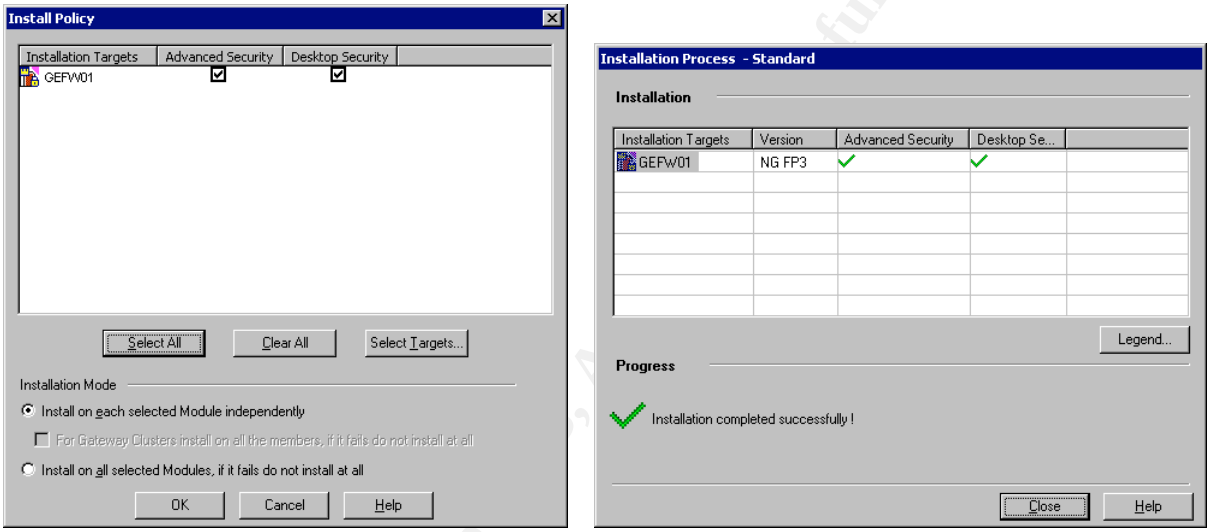


Figure 24: Install Policy

Assignment 3 - Verify the Firewall Policy

GIAC Enterprises requested an audit on the primary firewall to ensure that it is functioning as required in Assignments 1 and 2. The emphasis of the audit is to determine if the firewall blocks all undesired traffic. The audit does not include VPN components in the firewall.

Planning

Resources

To help shorten the testing period, three workstations are proposed:

- Audit Workstation 1 is connected to the firewall Internet interface
- Audit Workstation 2 is connected to the firewall DMZ interface
- Audit Workstation 3 is connected to the firewall Internal interface

The workstations are installed with the following tools:

- Nmap 3.48 win32 [27]– performs port scanning
- Windump 3.8 alpha[28] – sniffs the network
- WinPcap 3.0 alpha[29] – required to support Nmap and Windump
- NetCat 1.10[30] – network listener

Nmap 3.48 is used extensively in the firewall policy verification tests. The Nmap options used in the tests are:

Nmap options	Description
-sS	TCP SYN stealth port scan
-sU	UDP port scan. Nmap may not accurately report the status of UDP port scans across firewalls. However, we can determine the status by sniffing the network.
-O	Guess remote host operating system using TCP/IP fingerprinting. This option is used when scanning the firewall.
-p 1-65535	Scan all ports
-P0	Don't ping hosts before port scanning is required as the firewall blocks ICMP traffic.
-n	Never resolve IP address. DNS resolution is not required and slows down the scan.
-v	Verbose output

Table 31: NMap Options

WinDump is used to verify if the packets are blocked or forwarded by the firewall. The options used in the tests are:

Windump options	Description
-n	Don't resolve IP address

Table 32: WinDump Options

NetCat is used to simulate the servers in GIAC Enterprises. Table 33 explains the options used in the policy verification.

Netcat options	Description
-L	Listen mode (don't quit on disconnect)
-p <port number>	Port to listen to

Table 33: NetCat Options

During the tests, the firewall will be disconnected from the Internet and the corporate network. One audit workstation is connected to each of the networks separated by the firewall as shown Figure 25 below.

[27] http://www.insecure.org/nmap/nmap_download.html
[28] http://windump.polito.it/install/default.htm
[29] http://winpcap.polito.it/
[30] http://www.atstake.com/research/tools/network_utilities/

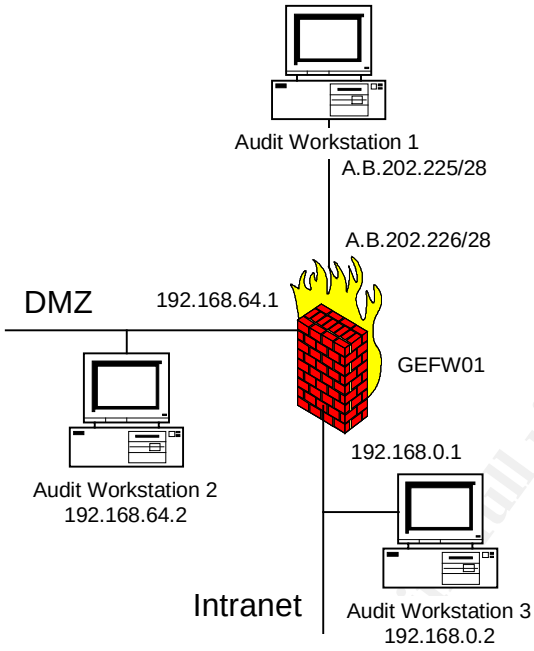


Figure 25: Network Connection for Audit

Port scanning will be conducted from each of the networks separated by the firewall i.e., DMZ, Intranet and border router. The scans will be performed as follows:

- Select the network segment to insert the test packets. The Audit Workstation in that network will run Nmap
- Run Windump on the remaining workstations
- Run Nmap on the selected workstation to scan the firewall interface
- Run Nmap on the selected workstation to scan the selected hosts in the other networks across the firewall
- Verify the results from the Nmap, firewall logs and Windump with the firewall policy.

Identify Risks

GIAC Enterprises online business is operational 24x7 with customers and business partners accessing from anywhere in the world. Since the firewall verification disrupts the Internet connectivity, the tests will be performed on a low peak period such as from Sunday 7:00pm to Monday 4:00am to minimize risk of affecting GIAC Enterprises staff, suppliers, partners and customers.

Announcements will be sent out to customers, business partners, suppliers and staff two weeks before the scheduled audit by e-mail. At the same time, a copy of the announcement is added to the External Web server home page and login page.

Costs

The audit will involve 2 experienced network staff working a total of 70 man-hours including planning, preparing, executing and reporting. At US$150 per man-hour, the total cost of the audit is estimated to be US$10,500.

Task	Estimated Effort (man hours)
Planning	12
Setup	8
Verification testing	18
Compile results	8
Reports	24
Total	70

Table 34: Effort Breakdown

Test Execution

1. Scan the Firewall interface from the Internet network

Procedure:

1. Set Audit Workstation 1 IP Address to A.B.202.225
2. At Audit Workstation 1, run the following commands:
```
Ping A.B.202.226
nmap -sS –O -p 1-65535 -v -P0 -n A.B.202.226
nmap -sU –p 1-65535 -v -P0 -n A.B.202.226
route add 192.168.0.0 mask 255.255.0.0 A.B.202.226
```
3. At Audit Workstation 1, run the following commands to test anti-spoofing:
```
nmap -sS –p 1-65535 -v -P0 -n A.B.202.226 –S A.B.202.226 –e eth0
nmap -sS –p 1-65535 -v -P0 -n 192.168.64.1 –S A.B.202.226 –e eth0
nmap -sS –p 1-65535 -v -P0 -n 192.168.0.36 –S 192.168.64.31 –e eth0
nmap -sS –p 1-65535 -v -P0 -n 192.168.0.33 –S 192.168.64.31 –e eth0
```

Results:

- Ping request timed out.

```
Pinging A.B.202.226 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for A.B.202.226:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Nmap TCP Stealth Scan

```
Interesting ports on A.B.202.226:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT      STATE  SERVICE
264/tcp   open   bgmp
```

```
18231/tcp open   unknown
Too many fingerprints match this host to give specific OS details
```

The firewall log shows the only the ports discovered by Nmap have been permitted. SmartDefense detected the port scan and generated alerts.

- Nmap UDP Scan

```
(no udp responses received – assuming all ports filtered)
All 65535 scanned ports on A.B.202.226 are: filtered
```

The firewall log shows that only UDP 500 is permitted. Probing UDP port 2746 on the firewall external interface causes the firewall to initiate an IKE connection to Audit Workstation 1. All other connections were dropped by rule 4 in the policy.

- Nmap TCP Stealth Scan with spoofed source A.B.202.226 to firewall external interface A.B.202.226

As expected, Nmap returns all ports filtered on the spoofed source A.B.202.226 to destination A.B.202.226.

```
All 65535 scanned ports on A.B.202.226 are: filtered
```

The firewall log shows that TCP ports 264 and 18231 are allowed.

- Nmap TCP Stealth Scan with spoofed source A.B.202.226 to firewall internal interface 192.168.0.1

```
All 65535 scanned ports on 192.168.0.1 are: filtered
```

The firewall log shows that all connections were dropped due to “Local interface address spoofing”

- Nmap TCP Stealth Scan with spoofed source 192.168.64.31 to Software Update server 192.168.0.36

```
All 65535 scanned ports on 192.168.0.36 are: filtered
```

- The firewall log shows that all connections were dropped due to “Address spoofing”. SmartDefense detected the port scans and address spoofing and initiated and logged the alerts.

- Nmap TCP Stealth Scan with spoofed source 192.168.64.31 to Mail server 192.168.0.33

```
All 65535 scanned ports on 192.168.0.36 are: filtered
```

The firewall log shows that all connections were dropped due to “Address spoofing”

Evaluation:
Nmap UDP port scanning does not provide accurate results with the firewall as it relies on ICMP unreachable packets to determine the status of a port. If Nmap does not receive any ICMP port unreachable message, it assumes the port is opened. Since the

firewall drops packets without sending any ICMP unreachable packets, Nmap is unable to accurately report the status of a UDP port.[31]

The firewall is able to detect all but one IP spoofed packets tested. It is not able to detect packets spoofed as its own interface address. However, the packet is still subjected to the rule base and only authorized connections are allowed.

The opened ports are explained below

Protocol/Port	Service	Remarks
TCP 264	VPN-1/Firewall-1 NG SecuRemote Topology Request	Allowed by Rule 2
TCP 18231	VPN-1/Firewall-1 NG Policy Server Logon	Allowed by Rule 2
UDP 500	IKE	Allowed by Rule 2
UDP 18233	Check Point SecureClient Verification Keepalive Protocol	Allowed by Rule 2

Table 35: Listening Ports on the Firewall

2. Scan the Internal network and DMZ network from the Border Router address

Procedure:

1. Add 192.168.64.31, 192.168.64.32 and 192.168.64.33 to Audit Workstation 2 secondary IP address
2. Run Netcat to listen to TCP ports 25, 80, and 443 on Audit Workstation 2
3. Add 192.168.0.31, 192.168.0.33, 192,168.0.34, 192.168.0.35 and 192.168.0.37 to Audit Workstation 3 secondary IP address
4. Run Windump in Audit Workstation 2 and Audit Workstation 3.
5. Set the IP Address of Audit Workstation 1 to the A.B.202.225 (The border router IP address)
6. At Audit Workstation 1, run the following commands

```
Route add 192.168.0.0 mask 255.255.0.0 A.B.202.226
Ping A.B.202.227
Ping A.B.202.228
Ping A.B.202.229
Ping 192.168.0.31
Ping 192.168.0.35
nmap -sS –O -p 1-65535 -v -P0 -n A.B.202.227-229 192.168.0.31 192.168.0.35
nmap -sU –p 1-65535 -v -P0 -n A.B.202.227-229 192.168.0.31 192.168.0.35
```

Results:

- All the Ping requests timed out

- Nmap TCP Stealth scan

```
Interesting ports on A.B.202.227:
```

[31] http://www.insecure.org/nmap/nmap_doc.html#port_unreach

```
(The 65534 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
25/tcp open  smtp

Interesting ports on A.B.202.228:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

All 65535 scanned ports on A.B.202.229 are: filtered

All 65535 scanned ports on 192.168.0.31 are: filtered

All 65535 scanned ports on 192.168.0.35 are: filtered
```

- UDP Port Scan

All ports reported filtered except for A.B.202.229

```
53/udp closed dns
```

and for 192.168.0.35

```
514/udp closed syslog
```

- Windump capture on Audit Workstation 2 shows only the allowed packets have passed the firewall

```
IP A.B.202.225.38349 > 192.168.64.32.443: S 793521603:793521603(0) win 3072
IP 192.168.64.32.443 > A.B.202.225.38349: s 1307150809:1307150809(0) ack 793521604 win
64240 (mss 1460) (DF)
IP A.B.202.225.38349 > 192.168.64.32.443: R 793521604:793521604(0) win 0
IP A.B.202.225.38349 > 192.168.64.32.443: S 793521603:793521603(0) win 3072
IP 192.168.64.32.443 > A.B.202.225.38349: s 1307150809:1307150809(0) ack 793521604 win
64240 (mss 1460) (DF)
IP A.B.202.225.38349 > 192.168.64.32.443: R 793521604:793521604(0) win 0
IP A.B.202.225.53591 > 192.168.64.33:  4 notify+ [b2&3=0x235b] [16a] [21631q] [42225n]
[6561au][|domain]
IP 192.168.64.33 > A.B.202.225: icmp 36: 192.168.64.33 udp port 53 unreachable
```

- Windump capture on Audit Workstation 3 captured the syslog packet to the syslog server.

```
IP A.B.202.225.40783 > 192.168.0.35.514: udp 0
IP 192.168.0.35 > A.B.202.225: icmp 36: 192.168.0.35 udp port 514 unreachable
```

- The firewall logs confirms the dropped and allowed ports for all tests.

Evaluation:

The TCP ports were detected as opened because Netcat responded to the TCP Sync packet.

The UDP ports scanning detected ICMP port unreachable packets because the UDP ports in the Audit Workstations are not active.

The traffic that is allowed through the firewall from the Internet network meets the firewall policy.

Protocol/Port	Service	Destination
TCP 25	SMTP	Mail Relay server
TCP 80	http	External Web server
TCP 443	https	External Web server
UDP 53	DNS	External DNS server
UDP 514	SYSLOG	Syslog server

Table 36: Forwarded traffic from the border router address

3. Scan the Internal network and DMZ network from the an unused external IP address

Procedure:

1. Add 192.168.64.31, 192.168.64.32 and 192.168.64.33 to Audit Workstation 2 secondary IP address
2. Add 192.168.0.31, 192.168.0.33, 192,168.0.34, 192.168.0.35 and 192.168.0.37 to Audit Workstation 3 secondary IP address
3. Run Windump in Audit Workstation 2 and Audit Workstation 3.
4. Set the IP Address of Audit Workstation 1 to the A.B.202.231
5. At Audit Workstation 1, run the following commands

```
Route add 192.168.0.0 mask 255.255.0.0 A.B.202.226
Ping A.B.202.227
Ping A.B.202.228
Ping A.B.202.229
Ping 192.168.0.31
Ping 192.168.0.35
nmap -sS –O -p 1-65535 -v -P0 -n A.B.202.227-229 192.168.0.31 192.168.0.35
nmap -sU –p 1-65535 -v -P0 -n A.B.202.227-229 192.168.0.31 192.168.0.35
```

Results:

- All Ping test timed out

- Nmap TCP Stealth scan

```
Interesting ports on A.B.202.227:
(The 65534 ports scanned but not shown below are in state: filtered)
PORT   STATE  SERVICE
25/tcp closed smtp

Interesting ports on A.B.202.228:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

All 65535 scanned ports on A.B.202.229 are: filtered

All 65535 scanned ports on 192.168.0.31 are: filtered
```

```
All 65535 scanned ports on 192.168.0.35 are: filtered
```

- Nmap UDP Port Scan showed all ports filtered except for A.B.202.229

```
53/udp closed dns
```

- Windump capture on Audit Workstation 2 shows only the allowed packets have passed the firewall

```
15:23:55.063892 IP A.B.202.231.54823 > 192.168.64.31.25: S 1304241738:13042417
38(0) win 1024
15:23:55.063988 IP 192.168.64.31.25 > A.B.202.231.54823: R 0:0(0) ack 13042417
39 win 0
15:24:06.321839 IP A.B.202.231.54822 > 192.168.64.32.80: S 1321863506:13218635
06(0) win 3072
15:24:06.321930 IP 192.168.64.32.80 > A.B.202.231.54822: R 0:0(0) ack 13218635
07 win 0
15:24:14.514674 IP A.B.202.231.54823 > 192.168.64.32.443: S 359750937:35975093
7(0) win 1024
15:24:14.514761 IP 192.168.64.32.443 > A.B.202.231.54823: R 0:0(0) ack 3597509
38 win 0
15:25:42.266606 IP A.B.202.231.49692 > 192.168.64.33.53:  4 notify+ [b2&3=0x23
5b] [16a] [21631q] [42225n] [6561au][|domain]
15:25:42.266681 IP 192.168.64.33 > A.B.202.231: icmp 36: 192.168.64.33 udp por
t 53 unreachable
```

- Windump capture on Audit Workstation 3 did not capture any packets.

- The firewall logs confirms the dropped and allowed ports for all tests.

Evaluation

Netcat was not enabled for this test. Thus, the servers returned a TCP Reset packet to the Nmap workstation, resulting the closed status reported by Nmap.

The firewall only allows any external hosts to connect to the following ports and servers.

Protocol/Port	Service	Destination
TCP 25	SMTP	Mail Relay server
TCP 80	http	External Web server
TCP 443	https	External Web server
UDP 53	DNS	External DNS server

Table 37: Forwarded traffic from the Internet

4. Scan the Firewall interface from the DMZ network

Procedure:

1. Set Audit Workstation 2 primary IP address to 192.168.64.33 and remove any secondary IP address.
2. At Audit Workstation 2, run the following commands:
   `Ping 192.168.64.1`

```
nmap -sS –O -p 1-65535 -v -P0 -n 192.168.64.1
nmap -sU p 1-65535 -v -P0 -n 192.168.64.1
```

Results:

- Ping Test request timed out

- Nmap TCP Stealth Scan

```
Interesting ports on A.B.202.226:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT      STATE  SERVICE
264/tcp   open   bgmp
18231/tcp open   unknown
Too many fingerprints match this host to give specific OS details
```

The firewall log shows the only the ports discovered by Nmap have been permitted.

- Nmap UDP Scan

```
(no udp responses received – assuming all ports filtered)
All 65535 scanned ports on 192.168.64.1 are: filtered
```

The firewall log shows that only UDP 500 is permitted. All other connections were dropped by rule 4 in the policy.

Evaluation:

The results are the same as Test 1 and are explained therein.

5. Scan the Internet network and Internal network from the External DNS server (DMZ network)

Procedure:

1. Set Audit Workstation 2 IP primary address to 192.168.64.33 (External DNS server) and remove any secondary IP address.
2. Add 192.168.0.31, 192.168.0.33, 192,168.0.34, 192.168.0.35 and 192.168.0.37 to Audit Workstation 3 secondary IP address
3. Run Netcat on Audit Workstation 3 to listen on port 80
4. Run Windump on Audit Workstation 1 and Audit Workstation 3.
5. At Audit Workstation 2, run the following

```
ping A.B.202.231
ping 192.168.0.31
ping 192.168.0.33
ping 192.168.0.34
ping 192.168.0.37
nmap -sS p 1-65535 -v -P0 -n A.B.202.231 192.168.0.31 192.168.0.33
       192.168.0.34 192.168.0.36
nmap -sU p 1-65535 -v -P0 -n A.B.202.231 192.168.0.31 192.168.0.33
       192.168.0.34 192.168.0.36
```

Results:

- All ping tests request timed out

- Nmap TCP Stealth Scan

```
All 65535 scanned ports on A.B.202.231 are: filtered

All 65535 scanned ports on 192.168.0.31 are: filtered

All 65535 scanned ports on 192.168.0.33 are: filtered

All 65535 scanned ports on 192.168.0.34 are: filtered

Interesting ports on 192.168.0.36:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp opened http
```

- Nmap UDP Port Scan

All ports are reported filtered except for 192.168.0.31

```
123/udp closed ntp
```

- Windump output from Audit Workstation 1 did not capture any packets.

- Windump output from Audit Workstation 3 captured the following

```
13:48:46.611230 IP 192.168.64.33.56228 > 192.168.0.36.21: S 926092612:926092612(
0) win 2048
13:48:46.611693 IP 192.168.0.36.21 > 192.168.64.33.56228: R 0:0(0) ack 926092613
 win 0
13:48:58.630263 IP 192.168.64.33.56228 > 192.168.0.36.80: S 926092612:926092612(
0) win 3072
13:48:58.631147 IP 192.168.0.36.80 > 192.168.64.33.56228: S 2695450458:269545045
8(0) ack 926092613 win 65535 <mss 1460> (DF)
13:48:58.631635 IP 192.168.64.33.56228 > 192.168.0.36.80: R 926092613:926092613(
0) win 0
14:00:56.888029 IP 192.168.64.33.39442 > 192.168.0.31.123:  [len=0] v0 -1s serve
r strat 44 poll 1 prec 0
14:00:56.888933 IP 192.168.0.31 > 192.168.64.33: icmp 36: 192.168.0.31 udp port
123 unreachable
```

Evaluation:

The firewall only allows the DNS server to connect as shown below. All other connections are blocked.

Protocol/Port	Service	Destination
TCP 21	ftp	Software Update server
TCP 80	http	Software Update server
UDP 123	Ntp	Active Directory server

Table 38: Forwarded traffic from the External DNS server address

6. Scan the Internet network and Internal network from the External Web server (DMZ network)

Procedure:

1. Set Audit Workstation 2 IP primary address to 192.168.64.32 (External Web server)
2. Add 192.168.0.31, 192.168.0.33, 192,168.0.34, 192.168.0.35 and 192.168.0.37 to Audit Workstation 3 secondary IP address
3. Run Netcat on Audit Workstation 3 to listen on ports 80 and 1433
4. Run Windump on Audit Workstation 1 and Audit Workstation 3.
5. At Audit Workstation 2, run the following commands

```
Ping A.B.202.231
Ping 192.168.0.31
Ping 192.168.0.33
Ping 192.168.0.34
Ping 192.168.0.36
nmap -sS p 1-65535 -v -P0 -n A.B.202.231 192.168.0.31 192.168.0.33
       192.168.0.34 192.168.0.36
nmap -sU p 1-65535 -v -P0 -n A.B.202.231 192.168.0.31 192.168.0.33
       192.168.0.34 192.168.0.36
```

Results:

- All ping test request timed out

- Nmap TCP Stealth Scan

```
All 65535 scanned ports on A.B.202.231 are: filtered

All 65535 scanned ports on 192.168.0.31 are: filtered

All 65535 scanned ports on 192.168.0.33 are: filtered

Interesting ports on 192.168.0.34:
(The 65534 ports scanned but not shown below are in state: filtered)
PORT     STATE SERVICE
1433/tcp open  ms-sql-s

Interesting ports on 192.168.0.36:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp opened http
```

- Nmap UDP Port Scan reveals all ports are filtered except for 192.168.0.31

```
123/udp closed ntp
```

- Windump output from Audit Workstation 1 did not capture any traffic.

- Windump output from Audit Workstation 3 captured the following

```
15:02:21.278387 IP 192.168.64.32.48044 > 192.168.0.34.1433: S 1458993391:1458993
391(0) win 2048
15:02:21.281422 IP 192.168.0.34.1433 > 192.168.64.32.48044: S 3953486517:3953486
```

```
517(0) ack 1458993392 win 65535 <mss 1460> (DF)
15:02:21.282215 IP 192.168.64.32.48044 > 192.168.0.34.1433: R 1458993392:1458993
392(0) win 0
15:06:07.827727 IP 192.168.64.32.35101 > 192.168.0.36.21: S 1845840509:184584050
9(0) win 4096
15:06:07.828163 IP 192.168.0.36.21 > 192.168.64.32.35101: R 0:0(0) ack 184584051
0 win 0
15:06:34.291947 IP 192.168.64.32.35101 > 192.168.0.36.80: S 1845840509:184584050
9(0) win 1024
15:06:34.292770 IP 192.168.0.36.80 > 192.168.64.32.35101: S 4026936920:402693692
0(0) ack 1845840510 win 65535 <mss 1460> (DF)
15:06:34.293259 IP 192.168.64.32.35101 > 192.168.0.36.80: R 1845840510:184584051
0(0) win 0
15:07:57.732272 IP 192.168.64.32.57767 > 192.168.0.31.123: [len=0] v0 unspec st
rat 0 poll 0 prec 80
15:07:57.733385 IP 192.168.0.31 > 192.168.64.32: icmp 36: 192.168.0.31 udp port
123 unreachable
```

Evaluation:

The firewall only allows the External Web server to connect as shown in Table 39. The results are consistent with the firewall policy.

Protocol/Port	Service	Destination
TCP 21	ftp	Software Update server
TCP 80	http	Software Update server
TCP 1433	Ms-sql-server	Database server
UDP 123	Ntp	Active Directory server

Table 39: Forwarded traffic from the External Web server address

7. Scan the Internet network and Internal network from the Mail Relay server (DMZ network)

Procedure:

1. Set Audit Workstation 2 IP primary address to 192.168.64.31 (Mail Relay server)
2. Add 192.168.0.31, 192.168.0.33, 192,168.0.34, 192.168.0.35 and 192.168.0.37 to Audit Workstation 3 secondary IP address
3. Run Netcat on Audit Workstation 3 to listen on ports 25 and 80
4. Run Windump on Audit Workstation 1 and Audit Workstation 3.
5. At Audit Workstation 2, run the following commands

```
Ping A.B.202.231
Ping 192.168.0.31
Ping 192.168.0.33
Ping 192.168.0.34
Ping 192.168.0.36
nmap -sS p 1-65535 -v -P0 -n A.B.202.231 192.168.0.31 192.168.0.33
      192.168.0.34 192.168.0.36
nmap -sU p 1-65535 -v -P0 -n A.B.202.231 192.168.0.31 192.168.0.33
      192.168.0.34 192.168.0.36
```

Results:

- All ping tests request timed out

- Nmap TCP Stealth Scan

```
All 65535 scanned ports on A.B.202.231 are: filtered

All 65535 scanned ports on 192.168.0.31 are: filtered

Interesting ports on 192.168.0.36:
(The 65534 ports scanned but not shown below are in state: filtered)
PORT   STATE  SERVICE
25/tcp open smtp

All 65535 scanned ports on 192.168.0.34 are: filtered

Interesting ports on 192.168.0.36:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp opened http
```

- Nmap UDP Port Scan reveals all ports are filtered except for 192.168.0.31

```
123/udp closed ntp
```

- Windump output from Audit Workstation 1 did not capture any traffic.

- Windump output from Audit Workstation 3 captured the following packets

```
15:31:11.864579 IP 192.168.64.31.36991 > 192.168.0.33.25: S 444628378:444628378(
0) win 3072
15:31:11.865397 IP 192.168.0.33.25 > 192.168.64.31.36991: S 153675732:153675732(
0) ack 444628379 win 65535 <mss 1460> (DF)
15:31:11.866612 IP 192.168.64.31.36991 > 192.168.0.33.25: R 444628379:444628379(
0) win 0
15:33:51.202327 IP 192.168.64.31.36991 > 192.168.0.36.80: S 610296688:610296688(
0) win 4096
15:33:51.202856 IP 192.168.0.36.80 > 192.168.64.31.36991: S 202649486:202649486(
0) ack 610296689 win 65535 <mss 1460> (DF)
15:33:51.203655 IP 192.168.64.31.36991 > 192.168.0.36.80: R 610296689:610296689(
0) win 0
15:34:02.014915 IP 192.168.64.31.36991 > 192.168.0.36.21: S 610296688:610296688(
0) win 2048
15:34:02.015662 IP 192.168.0.36.21 > 192.168.64.31.36991: R 0:0(0) ack 610296689
 win 0
15:36:33.934917 IP 192.168.64.31.56927 > 192.168.0.31.123:  [len=0] v0 unspec st
rat 0 poll 0 prec 80
15:36:33.936149 IP 192.168.0.31 > 192.168.64.31: icmp 36: 192.168.0.31 udp port
123 unreachable
```

Evaluation:

The firewall only allows the Mail Relay server to connect as shown Table 40. The results are inline with the firewall policy.

Protocol/Port	Service	Destination

TCP 21	ftp	Software Update server
TCP 80	http	Software Update server
TCP 25	smtp	Mail server
UDP 123	Ntp	Active Directory server

Table 40: Forwarded traffic from the Mail Relay server address

8. Scan the Firewall interface from the Intranet network

Procedure:

1. Set Audit Workstation 3 IP address to 192.168.0.2
2. At Audit Workstation 3, run the following commands:

```
Ping 192.168.0.1
nmap -sS –O -p 1-65535 -v -P0 -n 192.168.0.1
nmap -sU p 1-65535 -v -P0 -n 192.168.0.1
```

Results:

- Ping Test request timed out

- Nmap TCP Stealth Scan

```
Interesting ports on 192.168.0.1:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT      STATE  SERVICE
264/tcp   open   bgmp
18231/tcp open   unknown
Too many fingerprints match this host to give specific OS details
```

The firewall log shows the only the ports discovered by Nmap have been permitted.

- Nmap UDP Scan

```
(no udp responses received – assuming all ports filtered)
All 65535 scanned ports on 192.168.0.1 are: filtered
```

The firewall log shows that only UDP 500 is permitted. All other connections were dropped by rule 4 in the policy.

Evaluation:

The results is the same as Test 1 above.

9. Scan the Internet network and DMZ network from the Internal network

Procedure:

1. Set Audit Workstation 1 IP primary address to A.B.202.225 (border router address)
2. Set Audit Workstation 3 IP primary address to 192.168.0.2
3. Add 192.168.64.31, 192.168.64.32 and 192,168.64.33 to Audit Workstation 2 secondary IP address
4. Run Windump on Audit Workstation 1 and Audit Workstation 2.
5. At Audit Workstation 3, run the following commands

```
Ping A.B.202.225
Ping 192.168.64.31
Ping 192.168.64.32
Ping 192.168.64.33
nmap -sS p 1-65535 -v -P0 -n A.B.202.225 192.168.64.31 192.168.64.32
      192.168.64.33
nmap -sU p 1-65535 -v -P0 -n A.B.202.225 192.168.64.31 192.168.64.32
      192.168.64.33
```

Results:

- All ping tests request timed out

- Nmap TCP Stealth Scan

```
All 65535 scanned ports on A.B.202.225 are: filtered

All 65535 scanned ports on 192.168.64.31 are: filtered

Interesting ports on 192.168.64.32:
(The 65533 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

All 65535 scanned ports on 192.168.64.33 are: filtered
```

- Nmap UDP Port Scan reveals all ports are filtered except for 192.168.64.33 where

```
123/udp closed ntp
```

- Windump on Audit Workstation 1 did not capture any packets

- Windump on Audit Workstation 2 captured the following packets.

```
15:54:23.730371 IP 192.168.0.2.62028 > 192.168.64.32.443: S 1452697257:145269725
7(0) win 1024
15:54:23.730446 IP 192.168.64.32.443 > 192.168.0.2.62028: R 0:0(0) ack 145269725
8 win 0
15:54:31.851246 IP 192.168.0.2.62028 > 192.168.64.32.80: S 1452697257:1452697257
(0) win 3072
15:54:31.851338 IP 192.168.64.32.80 > 192.168.0.2.62028: R 0:0(0) ack 1452697258
 win 0
15:58:23.904770 IP 192.168.0.2.55324 > 192.168.64.33.53:  8224 notify$ [8224a] [
8224q] [8224n] [8224au][|domain]
15:58:23.904846 IP 192.168.64.33 > 192.168.0.2: icmp 36: 192.168.64.33 udp port
53 unreachable
```

Evaluation:

The Intranet users only have access to the External Web server via the http and https ports and to the External DNS server via the dns udp port. The results is consistent with the firewall policy.

Test Summary

Nmap TCP port scan accurately reports the status of the ports on each server. However, UDP results are less accurate because the firewall drops blocked packets without sending ICMP unreachable packet back to Nmap. The UDP scan is verified against Windump network captures.

The tests shows the firewall is implementing the installed policy correctly.

Recommendations

VPN Server

Having VPN and firewall in the same server may save some implementation and maintenance costs. However, the configuration requires some network ports to be accessible from the Internet. If there is any vulnerability in the services, these ports may be used to attack the firewall, affecting the entire GIAC Enterprises online business.

Having a separate VPN server will remove the requirement for the firewall to have any listening ports on the external interface. Thus the risk of any unauthorized access to the firewall is reduced. Furthermore, any attack to the VPN server will only affect remote employees.

DMZ servers

GIAC Enterprises DMZ servers are exposed to the Internet and can become victims to hackers, viruses and Internet worms. As such, the DMZ servers should not be trusted to initiate any connections to the Intranet network.

- A staging database server can be introduced to store copies of data that should be accessible by the External Web server. The internal Database server can initiate connections to the staging server to retrieve updated data. The proposed architecture helps prevent any malicious code in the External Web server from infiltrating the Database server.
- The DMZ servers can be configured to use an external time source instead of the AD servers.
- the DMZ servers retrieve virus updates directly from the Internet.

Intrusion Detection System

Intrusion Detection Systems can be added to the network to detect suspicious activities and alert the administrator. The IDS can be placed in the Internet, DMZ and Intranet network segments to detect any suspicious activities in the network.

The proposed changes are shown in Figure 26.

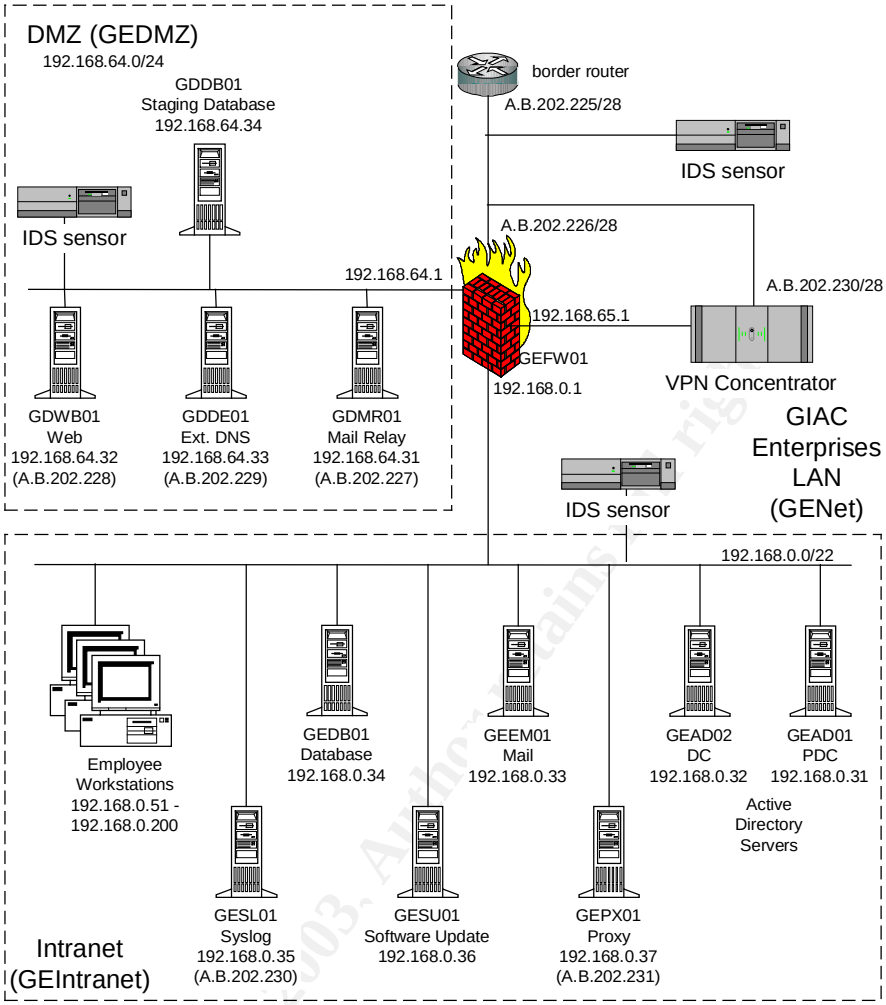


Figure 26: Proposed GIAC Network

Assigmement 4 – Design Under Fire

The network design that is selected for this assignment is from Lawrence Manalo http://www.giac.org/practical/GCFW/Lawrence_Manalo_GCFW.pdf. A copy of the network design is shown in Figure 27.

Reconnaissance

To launch an attack on the system, we need to find out more information on GIAC Enterprises. The first task is to surf their web site www.giacfortunes.com to learn about the GIAC's operations and obtain some contact e-mail addresses. The HTTP server header tells us the server is IIS5.0, which we know only runs on Windows 2000 server.

We Telnet to the mail relay server at port 25 and find that it is running SendMail 8.12.9 from the SMTP banner. To determine the internal e-mail server, we send e-mail to an arbitrary (non-existent) e-mail address. The undelivered message will contain the mail server name, product name and version. It should also contain the IP addresses of the mail server and the SMTP relay server.

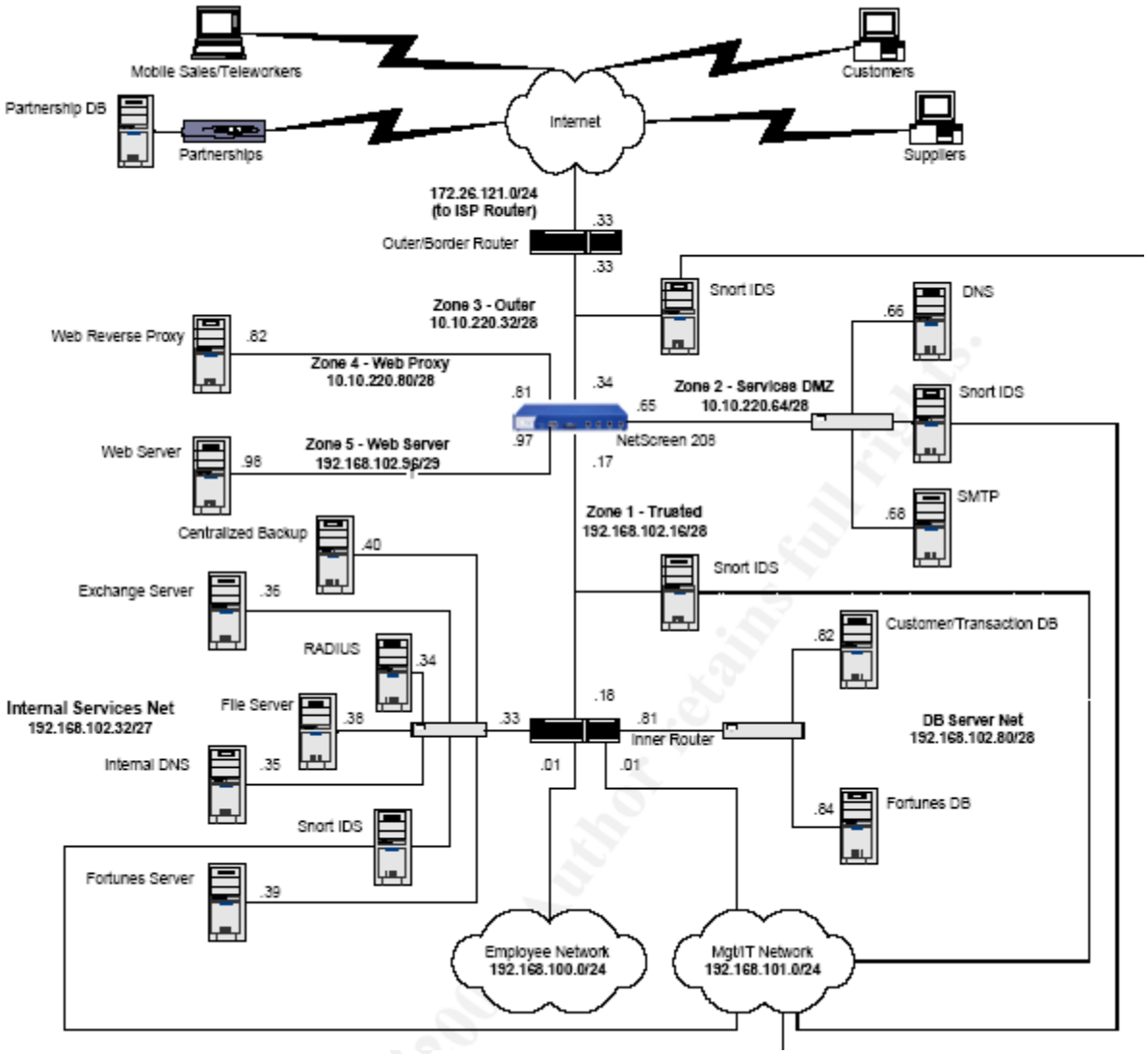


Figure 27: Lawrence Manalo Network Design

Nslookup can be used to determine the DNS server address and possibly another useful e-mail address from the DNS Start of Authority.

```
Nslookup
Server 10.10.220.66
Set type=all
Giacfortunes.com
```

Next we run DiG[32] to find the the DNS is running BIND 9.2.2.

```
dig @giacfortunes.com version.bind txt chaos

; <<>> DiG 9.2.1 <<>> @giacfortunes.com version.bind txt chaos
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45608
```

[32] The SANS Institute. Track 2.1 TCP/IP for Firewalls. Bethesda: SANS Press, 2002 Pg 7-26

```
;; flags: qr aa d ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
:version.bind                   CH      TXT

;; ANSWER SECTION:
VERSION.BIND.           0       CH      TXT      "9.2.2"
```

We go to ARIN Whois[33] web site to discover the IP block assigned to GIAC Enterprises. We may also obtain another e-mail address here.

To attack the firewall, we need to determine the make and version of the firewall. Since the router drops packets to the firewall except for UDP port 500 and ESP, it is not possible to accurately fingerprint the firewall using Nmap. One way of getting the information is to obtain from internal sources. We call the different contacts we have obtained previously to obtain different information on the organization. If we are lucky, we may be able to contact an employee that may divulge the make and version of the firewall to us.

Attack against the firewall

The firewall is a Netscreen 208 with ScreenOS 4.03r1. There are a few vulnerabilities reported in www.securityfocus.com on the ScreenOS version:

- http://www.securityfocus.com/bid/8762 - Netscreen ScreenOS DHCP Packet Buffer Padding Information Leakage. This vulnerability allows the attacker to obtain additional information from the firewall including usernames and passwords.The DHCP service is only available to the Netscreen "Trust" security zone. Hence, this vulnerability can only be performed from the internal network.
- http://www.securityfocus.com/bid/8302 - TCP Window Size Remote Denial Of Service Vulnerability. The vulnerability can only be performed from devices that have management services such as Web, Telnet, or SSH enabled on an interface.
- http://www.securityfocus.com/bid/8150 - Non-IP Traffic Firewall Bypass Vulnerability. This vulnerability only affects Netscreens installed as transparent mode and the attacker is in the same broadcast domain as the Netscreen[34].

Since all vulnerabilities of the ScreenOS can only be attacked from the "Trust" zone, we need to either:

- Get control of an internal host in the Trust zone. This may be a little difficult as connection from the Internet can only reach the DMZ zone and the Public Web zones. The other method is to attack GIAC's external employees to gain access to the internal servers.
- Connect directly to the Trust zone. Either we scan around GIAC Enterprises office for a wireless transceiver (WiFi) in GIAC's network or we plant one in an unused network point in GIAC's office.

[33] http://www.arin.net/whois/index.html
[34] http://www.netscreen.com/services/security/alerts/advisory-57605.txt

We need to gain access to GIAC's internal network. The first thing we do is to wardrive around GIAC's office with a Windows 2000 Server notebook equipped with a LinkSys WPC11 WiFi PC-Card and Aerosol v0.65[35]. We have detected an unsecured wireless transceiver in the network. We connect the workstation to the WiFi hub and run Windump. We can get the IP address, subnet mask of the network and other information from the broadcast traffic such as ARP, NetBIOS, CDP, DHCP etc.

Next, we restart the notebook to Linux and turned on IP forwarding. The copy of Linux is installed with dsniff 2.3 for Linux[36]. To minimize the impact to the network and alerting the IT staff of the breach, we run arpspoof to spoof a single workstation MAC address.

```
arpspoof –i eth0 –t 192.168.100.60 192.168.100.1
```

Arpspoof repetitively sends arp replies to the target host and may be detected by an IDS if there's one. Once the target host performs an arp-request, it will receive the arp reply from the actual host. However, the arp data will soon be replaced by one of many arpspoof's arp replies.

Monitoring the workstation traffic may provide us with more IP addresses, protocols used at each destination.

```
tcpdump –i eth0 –nXs0 –w tcpdump1.txt
```

We use p0f[37] version 1.8.3 for Windows to perform passive OS fingerprinting from the captured traffic.

```
p0f-1.8.3 –f p0f.fp.txt –vt –s tcpdump1.txt
```

We run Nmap to slowly scan the network individual ports to prevent IDS detection. We scan both Exchange server subnet and the user network subnet for popular protocols used by firewalls:

```
Nmap –sS –p 80 –P0 –T1 192.168.100.0/24
Nmap –sS –p 22 –P0 –T1 192.168.100.0/24
Nmap –sS –p 80 –P0 –T1 192.168.102.0/24
Nmap –sS –p 22 –P0 –T1 192.168.102.0/24
```

After a (long) while, we should be able to map out the servers. The process can be repeated for other interesting protocols until the network is well mapped.

Attack Procedure

To attack the firewall, we select the TCP Window Size Remote Denial Of Service (BID 8302). We setup a Windows 2000 server SP2 and add the following registry keys[38]:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
      Tcp1323Opts= DWORD 3
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\
      TcpWindowSize = DWORD 131400 (decimal)
```

[35] http://www.stolenshoes.net/sniph/aerosol.html
[36] http://monkey.org/~dugsong/dsniff
[37] http://www.stearns.org/p0f
[38] http://www.securityfocus.com/archive/1/330882

Reboot the workstation and connect to GIAC's network. To verify the attack, we need to connect to a server via the firewall.

We test the firewall by accessing the public web server, 10.10. 220.82 – it is successful – the firewall is running. Then, we Telnet to the firewall IP address 192.168.102.17 port 80. If the attack is successful, the firewall will core dump and reboot. We telnet again to the public we server and the connection times out – the firewall is confirmed down.

The countermeasure for this vulnerability is to patch the firewall to ScreenOS to 4.0.3r3 and above.

Distributed Denial of Service Attack

We will be using Tribe Flood Network 2000[39] to perform the DDoS attack on GIAC's network. Based on the analysis from Jason Barlow and Woody Thrower [40], TFN2K allows the client to request a number of agents running the daemon to coordinate an attack against one or more targets. The features includes:

- Sending commands from the client to the daemons via TCP, UDP, ICMP or all three.
- Attacks are performed from the daemon using TCP/SYN, UDP, ICMP/PING, or BROADCAST PING (SMURF) packet flood.
- Packet headers between client and daemons are randomized, with the exception of ICMP, which always uses a type code of ICMP_ECHOREPLY (ping response)
- The daemon is completely silent and does not acknowledge the client's commands. Instead, the client issues the commands 20 times relying on the probability that the daemon receives at least once.
- Commands are non-string and are encrypted using CAST-256. The key is defined during compile time and is used as the client password
- All encrypted data are Base 64 encoded before it is sent
- The daemon spawns a child process for each attack against the victim. The child process name can be falsified in some systems
- All packets from the client or daemon are spoofed by default
- The UDP packet length is always three bytes longer than the actual packet length
- The TCP header length is always zero
- The UDP and TCP checksums do not include the 12-byte pseudo-header and are consequently incorrect.

The distributed files are the source codes and must be compiled before using. The default makefile supports Linux/BSD and *nixes other than Solaris. For Solaris and Windows (cygwin), some modifications will be required. Two executables, tfn (client) and td (daemon) will be created after running make. TFN displays the following help text if no options are specified.

```
usage: ./tfn <options>
[-P protocol]   Protocol for server communication. Can be ICMP, UDP or TCP.
                Uses a random protocol as default
[-D n]          Send out n bogus requests for each real one to decoy targets
```

[39] http://mixter.void.ru/tfn2k.tgz
[40] http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt

```
[-S host/ip]    Specify your source IP. Randomly spoofed by default, you need
                to use your real IP if you are behind spoof-filtering routers
[-f hostlist]   Filename containing a list of hosts with TFN servers to contact
[-h hostname]   To contact only a single host running a TFN server
[-i target string]      Contains options/targets separated by '@', see below
[-p port]               A TCP destination port can be specified for SYN floods
<-c command ID> 0 - Halt all current floods on server(s) immediately
                1 - Change IP antispoof-level (evade rfc2267 filtering)
                    usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
                2 - Change Packet size, usage: -i <packet size in bytes>
                3 - Bind root shell to a port, usage: -i <remote port>
                4 - UDP flood, usage: -i victim@victim2@victim3@...
                5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
                6 - ICMP/PING flood, usage: -i victim@...
                7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
                8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
                9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
                10 - Blindly execute remote shell command, usage -i command
```

To compromise the 50 cable/DSL systems, we send bulk e-mail to users informing them of a serious vulnerability on their computer and requests them to download a software patch from a URL link that points to a web site managed by the attacker. The URL web page can determine the client operating system from the HTTP GET requests the client browser sends. The correct version of TFN2K can be send to different clients depending on the OS. At the same time, the server logs the client IP address. When the unsuspecting user installs the 'patch', the TFN2K daemon is installed instead.

We will attack GIAC's reverse proxy servers using the HTTP protocol as it has the most significant impact on GIAC's business. GIAC's border router and the firewall allow the HTTP protocol through. To start the attack on GIAC we run the following command from the client host:

```
./tfn –f agentip.txt –c 5 –p 80 –i 10.10.220.34
```

Where

./tfn	is the executable (in the current folder)
-f agentip.txt	get the agents' IP address from the agentip.txt file
-c 5	specify the attack type as SYN Flood
-p 80	specify the TCP port
-i 10.10.220.34	specify the target host

TFN2K daemons that receive the command will initiate multiple TCP SYN connections from spoofed source IP addresses. The GIAC's reverse proxy sever will be swamped with TCP SYN requests but will not receive any SYN ACK. Each SYN request takes up resources in the reverse proxy and bandwidth in GIAC's link to the ISP.

DDoS Countermeasures

DDoS traffic appears very similar to normal TCP/IP traffic and is very difficult to stop it from affecting the performance of an Internet system. However, there are a few action that can be taken to reduce the impact of DDoS to one's network.

Configure SYN-Flood protection

Netscreen firewalls can provide syn-flood protection to the network[41]. Mr Manalo has enabled syn-flood and syn-ack-ack proxy on all of the firewall ports which helps to reduce the impact of the DDoS. Netscreen syn-flood can be tuned to specify the Attack Threshold, queue size, timeout, destination threshold to better handle a DDoS attack.

Enable Ingress and Egress filtering

Anti-spoofing policy rules at the router or firewall can reduce the number of DDoS traffic into the Internet. Ingress filtering reduces the incoming attacks while egress filters reduce the risk of GIAC servers being used as a DDoS zombie.

It would be ideal if the filtering were performed at the ISP routers so that the DDoS traffic will not use up bandwidth between GIAC and the ISP.

IDS

The IDS placed in GIAC's outer zone will be able to detect the high number of TCP SYN traffic to the firewall and give the administrators a heads up on the situation although it will not prevent or reduce the impact of the attack.

Attack an Internal System

For this exercise, the target selected is the Exchange server. Most organizations are very dependent on emails and have high impact to the business operations and we assume that this is also the case for GIAC Enterprises. In addition, there is a path from the Internet to the Exchange server via the SMTP relay server.

We first search the Internet for Sendmail 8.12.9 vulnerabilities and found this:

- CERT® Advisory CA-2003-25 Buffer Overflow in Sendmail[42]. According to CERT, it may be possible for attackers to run arbitrary codes.

A search on Exchange 2000 vulnerabilities produced this

- MS03-046 : Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (829436)[43]. On Exchange 2000 server, the vulnerability can either cause the SMTP virtual server to fail or even cause a buffer overrun to run an arbitrary code.

We assume GIAC has patched their Windows 2000 Servers to Service Pack 4. Windows 2000 SP4 vulnerabilities that can be attacked remotely are listed below:

- MS03-039 : Buffer Overrun In RPCSS Service Could Allow Code Execution (824146)[44]. Three new vulnerabilities, two of which can lead to code execution. A sample exploit code for the RPC dcom vulnerability has been published[45].

[41] ScreenOS manual http://www.netscreen.com/services/support/product/downloads/screen_os/ce_all.pdf vol 2, pg 43
[42] http://www.cert.org/advisories/CA-2003-25.html
[43] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-046.asp
[44] http://www.microsoft.com/technet/security/bulletin/MS03-039.asp
[45] http://www.securityfocus.com/bid/8811/exploit/

- MS03-041 : Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)[46]. This vulnerability requires the use of Internet Explorer to download an ActiveX component without presenting any approval dialog box.
- MS03-042 : Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution (826232)[47]. Microsoft Local Troubleshooter ActiveX control is assessable from Internet Explorer and has a buffer overflow condition.
- MS03-043 : Buffer Overrun in Messenger Service Could Allow Code Execution (828035)[48]. The messenger service does not validate the length of a message before passing it to an allocated buffer.
- MS03-044 : Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (825119)[49]. Although the Help and Support Center protocol is not supported on Windows 2000, the affected code is still present in the OS.

We will attack the Exchange server with the MS03-039 sample exploit code[50]. We obtain the exploit code for MS03-039 from the Internet and run it against the Exchange server

```
Rpc3 192.168.102.36
```

We use Microsoft's portqry[51] utility to verify if the RPCSS is down:

```
portqry –n 192.168.102.36 –e 135
```

If the attack is successful, portqry will fail to retrieve the endpoint mapper database. Thus, users that have not logged onto Exchange, will not be able to do so. The server is still vulnerable even after installing the patch.

Countermeasures

Install Snort signature[52] for the vulnerability to detect and alert the security administrator that the Exchange problem is due to a DoS attack.

```
alert TCP any any -> any 135 (msg:"RPC Vulnerability - bind
initiation";sid:1; rev:1; content:"|05 00 0B 03 10 00 00 00 48 00 00 00
7F 00 00 00 D0 16 D0 16 00 00 00 00 01 00 00 00 01 00 01 00 a0 01 00 00
00 00 00 00 C0 00 00 00 00 00 00 46 00 00 00 00 04 5D 88 8A EB 1C C9 11
9F E8 08 00 2B10 48 60 02 00 00 00|";
flow:to_server,established;classtype:attempted-admin;)
```

Install the latest patches (when they are released).

[46] http://www.microsoft.com/technet/security/bulletin/MS03-041.asp
[47] http://www.microsoft.com/technet/security/bulletin/MS03-042.asp
[48] http://www.microsoft.com/technet/security/bulletin/MS03-043.asp
[49] http://www.microsoft.com/technet/security/bulletin/MS03-044.asp
[50] http://www.securityfocus.com/data/vulnerabilities/exploits/rpc3.zip
[51] http://support.microsoft.com/default.aspx?scid=kb;en-us;310099
[52] http://www.securityfocus.com/archive/1/341034/2003-10-08/2003-10-14/0

Appendix A – Router Configuration File

```
version 12.2
no service single-slot-reload-enable
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname GEBR01
!
logging buffered 10000 informational
enable secret 5 <enable_password>
!
username gesuper password 7 <password>
clock timezone CST
ip subnet-zero
no ip source-route
!
no ip finger
no ip domain-lookup
!
no ip bootp server
!
interface FastEthernet0/0
 description **Connected to FW
 ip address A.B.202.225 255.255.255.240
 ip access-group 106 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 ntp disable
 no cdp enable
!
interface Serial0/0
 description **2048kbps to ISP
 ip address A.B.212.58 255.255.255.252
 ip access-group 105 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ntp disable
 no fair-queue
 no cdp enable
!
no ip classless
ip route 0.0.0.0 0.0.0.0 A.B.212.57
ip route 192.168.0.35 255.255.255.255 A.B.202.226
no ip http server
!
logging facility local6
logging source-interface FastEthernet0/0
logging 192.168.0.35
!
access-list 105 deny   ip 0.0.0.0 0.255.255.255 any
```

```
access-list 105 deny   ip 10.0.0.0 0.255.255.255 any
access-list 105 deny   ip 172.16.0.0 0.15.255.255 any
access-list 105 deny   ip 192.168.0.0 0.0.255.255 any
access-list 105 deny   ip 224.0.0.0 31.255.255.255 any
access-list 105 deny   ip 255.0.0.0 0.255.255.255 any
access-list 105 deny   ip 127.0.0.0 0.255.255.255 any
access-list 105 deny   ip 192.0.2.0 0.0.0.255 any
access-list 105 deny   ip 169.254.0.0 0.0.255.255 any
access-list 105 deny   ip A.B.202.224 0.0.0.15 any
access-list 105 permit icmp any A.B.202.224 0.0.0.15 source-quench log
access-list 105 permit icmp any A.B.202.224 0.0.0.15 parameter-problem log
access-list 105 permit icmp any A.B.202.224 0.0.0.15 time-exceeded log
access-list 105 permit icmp any A.B.202.224 0.0.0.15 unreachable log
access-list 105 deny   icmp any any log
access-list 105 permit tcp any host A.B.202.228 eq 80
access-list 105 permit tcp any host A.B.202.228 eq 443
access-list 105 permit udp any host A.B.202.229 eq 53
access-list 105 permit tcp A.B.200.88 host A.B.202.229 eq 53
access-list 105 permit tcp A.B.200.100 host A.B.202.229 eq 53
access-list 105 permit tcp any host A.B.202.227 eq 25
access-list 105 permit tcp any host A.B.202.227 gt 1023
access-list 105 permit udp any host A.B.202.227 gt 1023
access-list 105 permit tcp any host A.B.202.230 range 600 1023
access-list 105 permit tcp any host A.B.202.230 range 10000 60000
access-list 105 permit udp any host A.B.202.230 range 600 1023
access-list 105 permit udp any host A.B.202.230 range 10000 60000
access-list 105 permit udp any host A.B.202.226 eq 500
access-list 105 permit udp any host A.B.202.226 eq 2746
access-list 105 permit udp any host A.B.202.226 eq 18233
access-list 105 permit tcp any host A.B.202.226 eq 264
access-list 105 permit tcp any host A.B.202.226 range 18231 18232
access-list 105 permit esp any host A.B.202.226
access-list 105 permit ah any host A.B.202.226
access-list 105 deny   ip any host A.B.202.226 log
access-list 105 deny   ip any host A.B.212.58 log
access-list 105 deny   ip any host A.B.202.225 log
access-list 105 deny   ip any any log
!
access-list 106 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 106 deny   ip any 172.16.0.0 0.15.255.255 log
access-list 106 deny   ip any 192.168.0.0 0.0.255.255 log
access-list 106 deny   ip any 192.0.2.0 0.0.0.255 log
access-list 106 deny   ip any 224.0.0.0 31.255.255.255 log
access-list 106 deny   ip any A.B.0.0 0.0.255.255 log
access-list 106 deny   tcp any any range 135 139 log
access-list 106 deny   tcp any any eq 445 log
access-list 106 deny   udp any any range 135 139 log
access-list 106 deny   udp any any eq 445 log
access-list 106 deny   udp any any range 161 162 log
access-list 106 deny   tcp any any range 513 515 log
access-list 106 deny   udp any any range 513 515 log
access-list 106 permit ip A.B.202.224 0.0.0.15 any
access-list 106 deny   ip any any log
no cdp run
!
dial-peer cor custom
!
```

```
!
!
banner motd ^CWARNING:  You must have specific authorization to access or
  use this system.  All connections to this system
  are logged and monitored.  Unauthorized access or
  use will be prosecuted.^C
!
line con 0
 exec-timeout 5 0
 login local
 transport input none
line aux 0
 no exec
 exec-timeout 0 1
line vty 0 4
 no exec
 exec-timeout 0 1
 no login
 transport input none
!
no scheduler allocate
end
```

References

1. The SANS Institute. Track 2.1 TCP/IP for Firewalls. Bethesda: SANS Press, 2002.

2. The SANS Institute. Track 2.2 Packet Filters. Bethesda: SANS Press, 2002.

3. The SANS Institute. Track 2.3 Firewalls. Bethesda: SANS Press, 2002.

4. Microsoft Corporation. "Microsoft Windows 2003 Security Guide.". 23 April 2003. URL: http://www.microsoft.com/technet/security/prodtech/windows/win2003/w2003hg/sgch00.asp (21 October 2003).

5. Microsoft Corporation. "HOW TO: Turn On the Internet Connection Firewall Feature in Windows Server 2003". 6 July 2003. URL: http://support.microsoft.com/default.aspx?scid=317530 (21 October 2003).

6. Microsoft Corporation. "INFO: Using URLScan on IIS". 6.0. 23 May 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;307608 (21 October 2003).

7. Microsoft Corporation. "INF: TCP Ports Needed for Communication to SQL Server Through a Firewall". 3.0. 16 August 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;287932 (21 October 2003).

8. Microsoft Corporation. "OL2000: Information About the Outlook E-mail Security Update". 3.1. 17 August 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;262631 (21 October 2003).

9. Microsoft Corporation. "XCCC: Exchange 2000 Windows 2000 Connectivity Through Firewalls". 3.0. 19 August 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;280132 (21 October 2003).

10. Microsoft Corporation. "IIS 6.0 Does Not Serve Unknown MIME Types". 4.0. 11 October 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;326965 (21 October 2003).

11. Microsoft Corporation. "Description of the Portqry.exe Command-Line Utility". 5.0. 10 October 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;310099 (21 October 2003).

12. Microsoft Corporation. "Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available". 12.0 10 October 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;303215 (21 October 2003).

13. Microsoft Corporation. “HOW TO: Enable TCP/IP Forwarding in Windows 2000”. 2.0. 14 May 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;230082 (21 October 2003).

14. Microsoft Corporation. “Protecting Windows RPC Traffic”. August 2002. URL: http://www.microsoft.com/technet/prodtechnol/isa/maintain/rpcwisa.asp (21 October 2003).

15. Microsoft Corporation. “IIS Lockdown Tool”. 2.1. October 2002. URL: http://www.microsoft.com/technet/security/tools/tools/locktool.asp (21 October 2003).

16. Microsoft Corporation. “Cumulative Patch for Microsoft SQL Server”. 1.2. 18 September 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-031.asp (21 October 2003).

17. National Security Agency. “Security Recommendation Guides - Windows 2000 Guides.”. 5 March 03. URL: http://www.nsa.gov/snac/win2k/download.htm (21 October 2003).

18. National Security Agency. ”Security Recommendation Guides - Cisco Router Guides.”. 10 February 2003. URL: http://www.nsa.gov/snac/cisco/download.htm (21 October 2003).

19. Microsoft Corporation. “MS03-026 : Buffer Overrun In RPC Interface Could Allow Code Execution (823980)”. 2.0. 10 September 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-026.asp (21 October 2003)

20. Microsoft Corporation. “MS03-039 : Buffer Overrun In RPCSS Service Could Allow Code Execution (824146)”. 1.0. 10 September 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-039.asp (20 September 2003)

21. Microsoft Corporation. “MS03-046 : Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (829436)”. 1.1. 15 October 2003 http://www.microsoft.com/technet/security/bulletin/MS03-046.asp (21 October 2003)

22. Rekhter, Y. RFC 1918. ”Address Allocation for Private Internets”. February 1996. URL: http://www.ietf.org/rfc/rfc1918.txt (21 October 2003).

23. Check Point Software Technologies Ltd. Check Point Firewall-1 Getting Started Guide NG FP3. Ramat Gan: Check Point Software Technologies Ltd. September 2002.

24. Check Point Software Technologies Ltd. Check Point Firewall-1 Guide NG FP3. Ramat Gan: Check Point Software Technologies Ltd. September 2002.

25. Check Point Software Technologies Ltd. Check Point Firewall-1 SmartCenter Guide NG FP3. Ramat Gan: Check Point Software Technologies Ltd. September 2002.

26. Check Point Software Technologies Ltd. Check Point Firewall-1 Virtual Private Networks Guide NG FP3. Ramat Gan: Check Point Software Technologies Ltd. September 2002.

27. Check Point Software Technologies Ltd. Check Point Firewall-1 Desktop Security NG FP3. Ramat Gan: Check Point Software Technologies Ltd. June 2002.

28. Check Point Software Technologies Ltd. "Check Point VPN-1 & FireWall-1 NG Performance Tuning Guide". 29 Jul 2003 URL: http://www.checkpoint.com/techsupport/documentation/FW-1_VPN-1_performance.html (21 October 2003).

29. Check Point Software Technologies Ltd. "Microsoft DCE-RPC denial of service". 14 August 2003. URL: http://www.checkpoint.com/securitycenter/advisories/2003/cpai-2003-11.html (21 October 2003).

30. Fyodor. "Nmap stealth port scanner". 6 Oct 2003. URL: http://www.insecure.org/nmap (21 October 2003).

31. Fyodor. "The Art of Port Scanning" 6 September 1997. URL: http://www.insecure.org/nmap/nmap_doc.html#port_unreach (23 October 2003)

32. Politecnico di Torino. "Windump: tcpdump for Windows". 3.6.2. 8 August 2002. URL: http://windump.polito.it (21 October 2003).

33. Politecnico di Torino. "WinPcap: the Free Packet Capture Architecture for Windows". 3.0. 12 September 2003. URL: http://windump.polito.it (21 October 2003).

34. Pond, Weld. "NetCat 1.1 for NT". 6 February 1998. URL: http://www.atstake.com/research/tools/network_utilities/nc11nt.zip (21 October 2003).

35. Manalo, Lawrence. "GIAC Certified Firewall Analyst (GCFW) Practical Assignment version 1.9 Taking the cookie saying world by storm!". 7 August 2003. URL: http://www.giac.org/practical/GCFW/Lawrence_Manalo_GCFW.pdf (1 October 2003).

36. Netsreen. "Netscreen Advisory 57605 - Potential denial of service, compromise of hosts running non-IP protocols". 10 July 2003. URL: http://www.netscreen.com/services/security/alerts/advisory-57605.txt (21 October 2003).

37. Sniph. “Aerosol v0.65 wardriving utility”. 23 January 2003. URL: http://www.stolenshoes.net/sniph/aerosol.html (21 October 2003).

38. Song, Dug. “Dsniff monitoring tools”. December 2000. URL: http://monkey.org/~dugsong/dsniff/ (21 October 2003).

39. Dunston, Duane. “Network Monitoring with Dsniff”. 29 May 2001. URL: http://www.linuxsecurity.com/feature_stories/feature_story-89.html (21 October 2003).

40. Stearns, William. “p0f passive OS fingerprinting tool”. 1.8.3. 7 Feb 2003. URL: http://www.stearns.org/p0f (21 October 2003).

41. Security Focus. “NetScreen ScreenOS 4.0.3r2 DOS Vulnerability”. 29 Jul 2003. URL: http://www.securityfocus.com/archive/1/330882 (21 October 2003).

42. Mixter. “Tribe Flood Network 2000”. 19 December 1999. URL: http://mixter.void.ru/tfn2k.tgz (21 October 2003).

43. Barlow, Jason. “TFN2K - An Analysis 1.3”. 10 February 2000. URL: http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt (21 October 2003).

44. NetScreen. “NetScreen Concept & Examples – ScreenOS Reference Guide. ScreenOS”. 4.0.0 Rev. F. 17 December 2002 http://www.netscreen.com/services/support/product/downloads/screen_os/ce_all.pdf (21 October 2003).

45. CERT Coordination Center. “CERT® Advisory CA-2003-25 Buffer Overflow in Sendmail” 29 September 2003. URL: http://www.cert.org/advisories/CA-2003-25.html (21 October 2003)

46. VigilantMinds Security Operations Center. “Bad news on RPC DCOM vulnerability”. 11 October 2003. URL: http://www.securityfocus.com/archive/1/341034/2003-10-08/2003-10-14/0 (21 October 2003)

47. Smith, Randy. “IPSec Packet Filtering”. Windows Web Solutions. September 2002.URL: http://www.winnetmag.com/Web/Article/ArticleID/25935/Web_25935.html (23 October 2003)