



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Certified Firewall Analyst

**Firewalls, Perimeter Protection and VPN's
SANS GCFW Practical Assignment
Version 2.0**

February 3, 2004

By

Tom A. Jozwiak

© SANS Institute 2004, Author retains full rights.

Table of Contents

GIAC Certified Firewall Analyst.....	1
Abstract.....	4
GIAC Enterprises business background	4
1. Assignment 1 – GIAC Network Security architecture.....	4
1.1 Customers.....	5
1.2 Suppliers.....	5
1.3 Partners	5
1.4 Employees and mobile sales force	6
1.4.1 Internal Employees	6
1.4.2 Sales force and Telecommuters	6
1.5 General Public	6
1.6 Network security architecture components	7
1.6.1 Border router.....	7
1.6.2 Firewall.....	8
1.6.2.1 Optional (DMZ) network.....	9
1.6.2.2 Trusted (Internal) Network	10
1.7 VPN / remote connections	11
1.8 GIAC IP addressing scheme.....	11
1.8.2 Trusted (Internal) network.....	13
2. Assignment 2 – Security Policy and Tutorial.....	14
2.1 Security policy for Border Router	14
2.1.1. Router access.....	14
2.1.2 Ingress and Egress Packet filtering setup on the Border Router.....	18
2.1.2.1 Ingress packet filtering	18
2.1.2.2 Egress packet filtering.....	20
2.2 Security Policy for Primary Firewall.....	22
2.3 Security Policy for VPN.....	31
2.3.1 VPN client software.....	31
2.3.2 VPN type.....	31
2.3.3 Watchguard Firebox user authentication	31
2.3.4 VPN authentication	32
2.3.5 IPSec Setup details.....	33
2.3.6 Firewall Policy for VPN.....	33
2.4 Firewall Policy Implementation Tutorial.....	33
Blocked sites.....	38
3. Assignment 3 – Verify the Firewall Policy	70
3.1 Technical approach to our firewall assessment	70
3.1.1 Firewall Test.....	70
3.1.2 Firewall Rule Base Test	71
3.1.2.1 Scanning from the Internet.....	71
3.1.2.2 Scanning from the Optional (DMZ) network	72
3.1.2.3 Scanning from the Trusted (Internal) network	73
3.1.3 Audit date consideration.....	73
3.1.4 Estimate costs and level of effort	73

3.1.5 Risks associated with performing the firewall audit.....	74
3.2 Validation of Firewall Policy	74
3.2.1 Audit of the Firewall	74
3.2.2 Audit of the Firewall Rulebase	80
4. Assignment 4 – Design under Fire.....	97
4.1 Attack against the firewall	97
4.1.1 Countermeasures	99
4.2 Distributed denial of service attack (DDoS).	99
4.2.1. Compromise of 50 cable / DSL connected systems.....	99
4.2.2. Denial of Service attack	101
4.2.3. Countermeasures	101
4.3 Compromising an internal system.....	102
4.3.1 Countermeasures	103
5. References.....	103

© SANS Institute 2004, Author retains full rights.

Abstract

This paper will outline a proposed network security architecture for an e-business company called GIAC Enterprises. It will be divided into four sections.

First one will describe GIAC Enterprises overall business operations, mainly, interactions with its customers, suppliers, partners and employees. It will also specify recommended network security design and components to be used. Second section will provide security policies for the border router, primary firewall and VPN. It will also go into more detail of how to implement the security policy for the primary firewall. The third section will focus on planning, conducting and evaluating an audit of the security policy of GIAC's primary firewall. The last section will present three different types of attacks against a network design from a previous GCFW practical assignment – attack against the firewall, distributed denial of service attack as well as attack against one of the internal systems.

GIAC Enterprises business background

GIAC Enterprises (GE) is an e-business organization dealing with selling fortune cookie sayings online. The company's office is located in Toronto, Ontario, Canada. The annual revenue fluctuates between \$CDN 7 and 8 million. GE employs 80 people. Due to a recent increase of volume of business, the management of GE has decided to design, implement and maintain new, secure, cost-effective and scalable network architecture. Because of its limited resources GIAC will perform its IT restructuring project in-house.

1. Assignment 1 – GIAC Network Security architecture

Access requirements/restrictions between the following groups will be taken under consideration:

- customers (companies or individuals that purchase bulk on-line fortune cookie sayings)
- suppliers (companies that supply GIAC Enterprises with their fortune sayings)
- partners (international companies that translate and resell fortunes)
- GIAC Enterprises employees located on GIAC Enterprise's internal network
- GIAC Enterprises mobile sales force and telecommuters
- general public (potential customers)

Use of the following networking hardware/software components to fulfill the company's e-business requirements will also be outlined:

- filtering routers
- firewalls
- VPN/remote connections
- IP addressing scheme

1.1 Customers

GIAC has an external SUN ONE secure reverse HTTP proxy server running on port 4000. This server forwards all external requests to the internal Lotus Notes web server running on port 9000. The Lotus Notes web server accesses GIAC's internal databases, which store GIAC fortune cookie sayings offerings. All communications between the client, external HTTP proxy server and Lotus Notes web server is protected using SSL 128bit encryption. Upon contacting the secure reverse proxy server customers are prompted to login with their username and password. The credentials are verified against GIAC LDAP server on port 636(TCP) using SSL 128bit encryption. When the login is successful, GE's customers can make their purchases using Lotus Notes developed application. There are minimum system and web browser requirements for this connection to work. The browser must support 128bit encryption. Anything lower (i.e. 40 bit encryption) will not work. Also, Microsoft JVM (java virtual machine) has to be installed for the Lotus Notes application to work.

1.2 Suppliers

For security reasons suppliers will only be allowed to access GIAC secure ftp (sftp) server using ssh(TCP port 22) protocol. This server will be residing on GIAC's DMZ network. Fortune cookie sayings will be uploaded onto that server on pre-determined basis. Suppliers will only be allowed to a specific, 'suppliers only' directory on the server. Only use of 'put' command will be allowed. Also, upon completion of data transfer, suppliers will be required to send an-email to GIAC's fortune cookie database administrators. The DBA's will review the newly uploaded data and perform cookie sayings selection. After the initial screening stage, all chosen fortune cookie sayings will be scanned for viruses using TrendMicro Scanmail for Lotus Notes, downloaded, and posted onto GIAC's Lotus Notes database server.

1.3 Partners

GE has setup international partnerships with several companies, which are allowed to purchase fortune cookie sayings at discounted prices. GIAC partners are also permitted to translate cookie sayings into their respective languages and dialects. To be able to purchase the sayings, partners will be required to sign in to GE's local Lotus Notes web server through SUN's secure reverse proxy server running on port 4001 on GE's DMZ network. The communication links between the partner, proxy and Lotus Notes web server will be encrypted using SSL 128bit protocol. Their credentials will be verified against GIAC's LDAP server running on TCP port 636 (secure LDAP). Upon successful login, GIAC partners will be allowed to browse through GE's cookie sayings offerings, place an order and download their selections for further resale.

They will use custom Lotus Notes developed application to view, purchase and download GIAC's offerings.

1.4 Employees and mobile sales force

1.4.1 Internal Employees

Internal Employees will be able to use the following Internet services:

- SMTP (to send and receive mail)
- HTTP and HTTPS (to browse insecure and secure web sites)
- FTP (for file download)
- DNS (for internet name resolution). All staff will also be allowed to access GE's internal file and print sharing, application and Internet servers.

GIAC's system administrators will have ssh access to all servers on the DMZ network. The ssh access will be controlled using TCP wrappers.

1.4.2 Sales force and Telecommuters

Sales force and telecommuters will use client VPN connection to access GE's local resources. Sales people will use laptops, which will be configured for them by local IT staff. They will be using VPN client software from Watchguard Technologies with Zone Alarm personal firewall and authenticating using digital certificates. The authentication will be performed on Watchguard Firebox III 1000 firewall appliance. The appliance will also be responsible for generating client certificates. Virus scanning software will also be installed on all remote laptops and setup to perform frequent virus definition updates and hard drive scans. Telecommuters will use their home computers and local ISP's to connect to GE's network. The machines will be setup the same way as the laptops used by GIAC's sales force.

1.5 General Public

General public will have full access to GIAC's public web server located on the DMZ network. They will be able to browse through samples of fortune cookie sayings. Should they decide to purchase GE's offerings, they will be asked to register. Registration will take place on GIAC secure 128bit SSL web server running on port TCP:443(HTTPS) located on DMZ network. New customers' data will be stored in GIAC's LDAP database. Once registered, their information will be verified by new customers registration clerk (either by phone or mail). Upon approval, new account will be created in GIAC's LDAP database and new customers will be e-mailed username and password in 2 separate messages for security reasons. Their new username and password will allow them to login to GIAC's customers' only web site and purchase fortune cookie sayings.

1.6 Network security architecture components

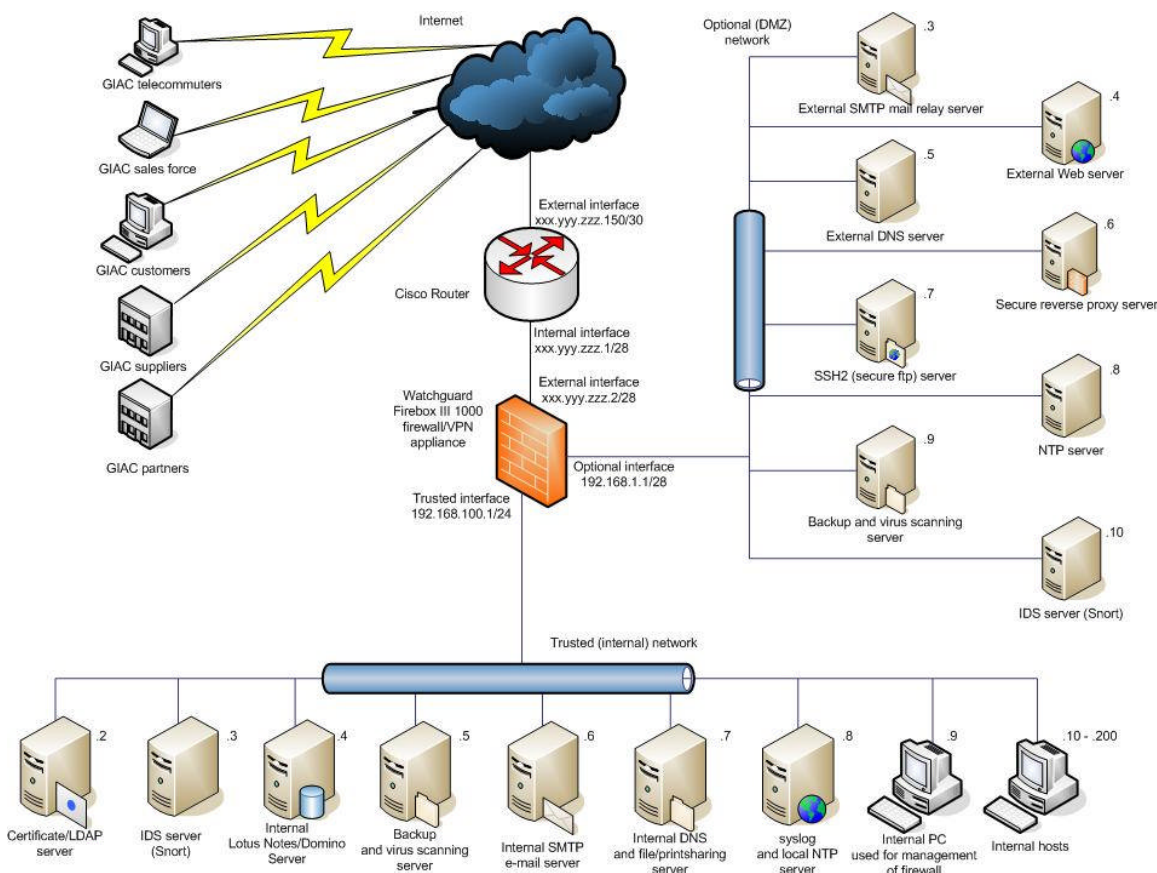


Figure 1.6 GIAC Enterprises network design

Note :Trusted (Internal) network IP address range .201 - .254 will be used for VPN clients (sales force and telecommuters)

1.6.1 Border router

GIAC Enterprises will be using CISCO 2611 as its filtering, border router with the newest version of CISCO IOS – 12.3. The router will be placed between the Internet and GE's Watchguard firewall appliance. The router will provide the first line of defense for GIAC's networks by performing initial packet filtering of internet traffic. Our router will be hardened based on recommendations found in NSA/SNAC Router Security Configuration Guide -

<http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf>

1.6.2 Firewall

GIAC has chosen Watchguard Firebox III 1000 firewall appliance as their primary firewall system. The device is based on Linux kernel and it comes with 3 network interfaces : external, optional and trusted. GE's will use the newest (ver 7.0) high encryption software for access and maintenance of the appliance.

Based on Watchguard current information about their Firebox III 1000 firewall appliance, here is a list of most of its built-in security and management features :

Security features of Watchguard Firebox III 1000 appliance :

- application layer proxies
- dynamic stateful packet filtering
- branch office VPN
- mobile user VPN
- static, dynamic and one-to-one NAT
- IPSec NAT traversal (NAT-T)
- proprietary firewall authentication
- VPN authentication
- DHCP support
- McAfee VirusScan Asap
- PKI with Internal Certificate Authority
- web content filtering
- port and site blocking
- scan and spoof detection
- SYN flood protection
- PPPoE support

And its management features :

- quicksetup wizard
- VPN manager, 4-Node
- hostwatch
- secure encrypted failover logging
- notification
- security policy manager
- real time monitoring
- historical reporting
- colorized logging

The appliance has also successfully met the following certification criteria :

- ICSA firewall
- ICSA IPSec
- ICSA cryptography

As we can see, the extended list of options included with the firewall will allow us to custom-configure our device to meet the requirements of GIAC's perimeter protection policy.

The firewall will be placed between the CISCO border router and GIAC's Trusted(Internal) and Optional(DMZ) networks.

All 3 interfaces of the firewall will be utilized :

- External – connecting firewall to the border router
- Trusted – connecting firewall to GIAC's local, protected network
- Optional – connecting firewall to GIAC 's DMZ network

We will be screening our DMZ network using 1-to-1 NAT. To protect our Trusted (Internal) network, will be using dynamic NAT capabilities of the firewall.

There will be four(4) Watchguard proxy services implemented for additional protection : SMTP, DNS, FTP and HTTP :

- SMTP proxy – we will only be using incoming SMTP proxy service (outgoing SMTP proxy for ESMTP is not yet supported). The SMTP proxy will add e-mail content filtering protection to our external mail relay server.
- DNS Proxy will allow us to validate all incoming DNS traffic to our external DNS server and will block any DNS packets that are illegally formed or don't match a basic list of allowable transactions.
- FTP proxy will allow us to initiate connections to servers through a NATted firewalls. We will only be using outbound FTP proxy service. No incoming ftp connections will be allowed.
- HTTP proxy, similarly to SMTP proxy, will allow us to content filter all Incoming and Outgoing HTTP traffic. HTTP proxy will protect our web clients and web servers from potentially hostile entities on the Internet.

1.6.2.1 Optional (DMZ) network

The optional (DMZ) network will include the following servers :

- External SMTP Mail Relay Server. This machine will receive external e-mail, scan it for viruses and then forward the e-mail to GIAC internal mail server residing on Trusted (Internal) network. Virus scanner used will be Trendmicro InterScan Viruswall virus scanner. The virus scanner will obtain virus pattern updates from the main Virus scanner server on DMZ network. This system will also receive internal e-mail and relay it to the Internet.
- External Web server, which will host GIAC's public web page. This server will also perform additional task – it will run SSL 128bit secured

registration web page on port 443:TCP(HTTPS). This page will be responsible for updating customer's information in GIAC LDAP server residing on trusted network.

- External DNS server which will contain public name resolution information of GIAC Enterprises
- Secure reverse proxy server responsible for accessing GIAC's Lotus Notes database. There will be 2 instances of this server running – one on port 4000 and the 2nd on port 4001. The former will be used by GIAC customers to access the Lotus Notes database, the latter will be used by GIAC partners to access separate part of Lotus Notes database designed specifically for them
- SSH2 server. This machine will provide secure ftp (SFTP) access for GIAC's fortune cookie sayings suppliers
- External NTP server, which will synchronize its time with outside stratum servers
- Backup and Virus scanning server. This machine will backup all servers on our DMZ network. The newest version (6.x) of Retrospect Server backup software will be used for this purpose. This system will be also responsible for scanning DMZ servers for viruses on weekly basis. Virus software running will be Trend Micro's NeatSuite. The server will be allowed to access the Internet to download Virus definition updates
- Intrusion detection server (IDS), which will watch packets for known attack patterns. In case of any Optional(DMZ) network compromise it will alarm GIAC's system administrators. The newest, stable version of Snort will be used, which, at the time of writing, was 2.0.2

1.6.2.2 Trusted (Internal) Network

Local network will have the following servers and clients in place :

- LDAP/Certificate server. LDAP server will contain all customer data. Lotus Notes server will rely on it for user access (login and password) verification.
Certificate server – GIAC has setup its own Certificate Authority server for issuing local certificates. All “servers to servers” and “clients to servers” communication will be encrypted using 128bit SSL protocol. All servers will have a server certificate installed, client PC's will have a client certificate installed. They will all trust GIAC Certificate Authority
- Internal IDS system detecting any network compromise on GIAC's LAN and alarming system administrators of such. Snort ver. 2.0.2 will be used
- Lotus Notes/Domino server version 5.0.12 containing GIAC's fortune cookie sayings databases. This system will also have a 128bit SSL, Lotus Notes/Domino driven, secure web server running on port 9000. The main page will have access links to Lotus Notes databases. All Lotus Notes databases will consult their user ACL's with GIAC's LDAP server (via 128bit SSL secure connection on port 636)

- Backup and Virus scanning server. TrendMicro Scanmail for Lotus Notes anti-virus software will be utilized to scan Lotus Notes databases upon access. The newest version (6.x) of Retrospect Server backup will backup all local servers and clients
- Internal SMTP/IMAP server. Internal SMTP server will be responsible for forwarding all internal e-mail messages to our external SMTP Mail Relay Server. IMAP server will allow users to retrieve their e-mail onto their desktops. GIAC has chosen to use IMAP server instead of POP. IMAP is much more secure than POP as it doesn't send e-mail passwords in plain text. Client PC's will also be configured to use SSL secured IMAP connection (IMAPS) running on port 993.
- Internal DNS and file / print sharing server. This server will be responsible for internal name resolution. It will store all internal server and client DNS names. Any external name resolution request originating from GIAC's local network will be forwarded, through this server, to GIAC's external DNS server (split DNS configuration)
The machine will also perform file and print sharing duties for local users
- Syslog and local NTP server. This machine will collect all syslog data from our border router as well as from all DMZ servers. It will also synchronize its time against GIAC's external NTP server. All local GIAC servers and workstations will synchronize their time against it.
- Watchguard Firebox III 1000 management and logging station will be responsible for accessing and maintaining GIAC's firewall. It will also collect firewall logs.
- Workstation PC's – various local end-user machines.

1.7 VPN / remote connections

Remote users will be using IPSec client VPN access to GIAC local network. Watchguard Firebox III 1000 firewall's VPN capabilities will be utilized to provide this service.

Remote users laptops and PC's will be configured with the newest version of Watchguard's client VPN software with high encryption – 6.1.2 and Zone Alarm personal firewall to connect to GIAC's firewall appliance. We will be using digital certificates issued by our firewall's certificate authority (CA) as means of VPN authentication. There will be no serial dial in / dial out devices on GIAC network (i.e. modem pools)

1.8 GIAC IP addressing scheme

1.8.1 External Network

GIAC has obtained the following, subnetted public IP address range from its ISP: xxx.yyy.zzz.0/28 (xxx.yyy.zzz.0 network subnet, useable addresses range will be xxx.yyy.zzz.1 – xxx.yyy.zzz.14 and broadcast will be xxx.yyy.zzz.15).

We will assign the following external IP addresses to GIAC External devices :

- xxx.yyy.zzz.1 – internal address of the Cisco border router
- xxx.yyy.zzz.2 – external address of the Watchguard firewall

1.8.2 Optional (DMZ) Network

We will assign the following external IP addresses to GIAC Optional (DMZ) servers :

- xxx.yyy.zzz.3 – external SMTP mail relay server
- xxx.yyy.zzz.4 – Web server
- xxx.yyy.zzz.5 – external DNS server
- xxx.yyy.zzz.6 – Secure reverse proxy server
- xxx.yyy.zzz.7 – SSH2 (secure FTP) server

The 7 remaining public IP addresses will be available for future expansion.

The external NTP, Backup / Virus scanning and IDS servers won't require external (routable) IP addresses since no incoming traffic will be allowed to those servers. They will be assigned 192.168.1.8, 192.168.1.9, 192.168.1.10 IP addresses respectively.

Our firewall appliance will be configured in 'routed mode', which requires us to use private addresses on our optional (DMZ) network. To allow access to our external servers from the Internet we will implement 1-to-1 NAT setup.

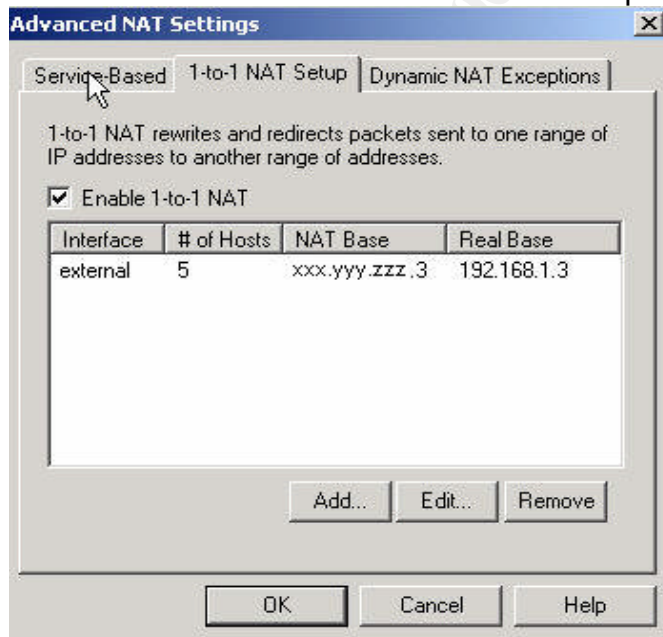


Figure 1.8.1

We will assign 192.168.1.3 real base to xxx.yyy.zzz.3 NAT base for 5 hosts. The way this works is that 192.168.1.3 real IP address will be mapped to xxx.yyy.zzz.3 IP address, 192.168.1.4 will be mapped to xxx.yyy.zzz.4 and so on. Also, we will need to apply Dynamic NAT exceptions for the addresses used for 1-to-1 NAT.

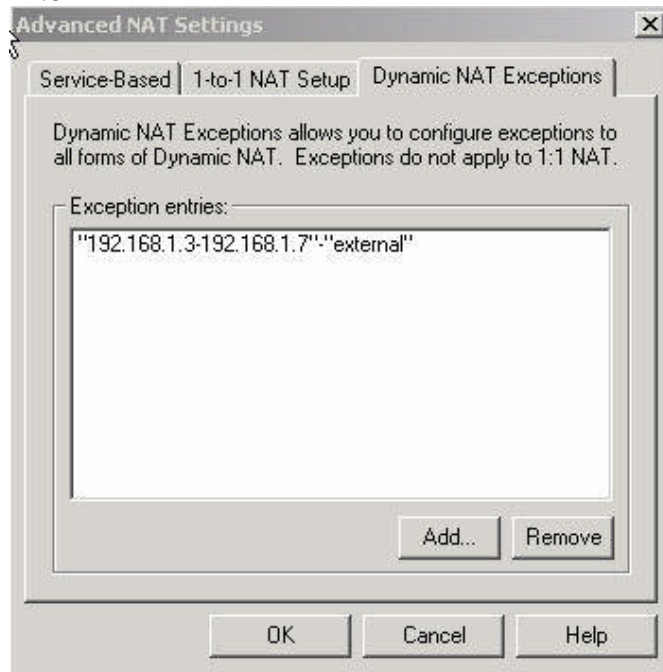


Figure 1.8.2

This will exclude 1-to-1 NAT addresses from being used by dynamic NAT.

1.8.2 Trusted (Internal) network

IP addresses subnet for our Trusted (Internal) network will be 192.168.100.0/24, IP address range will be 192.168.100.1 – 192.168.100.200. Addresses between 192.168.100.201 – 192.168.100.254 will be assigned to IPSec VPN clients. Broadcast address will be 192.168.100.255. Internal addresses (except the client VPN range) will be using dynamic NAT to communicate with the Internet.

The following IP addresses will be assigned to the main Trusted (Internal) network devices :

- 192.168.100.1 – internal address of the Watchguard firewall
- 192.168.100.2 – Certificate / LDAP server
- 192.168.100.3 – IDS (Snort) server
- 192.168.100.4 – Lotus Notes / Domino server
- 192.168.100.5 – Backup and Virus scanning server
- 192.168.100.6 – SMTP e-mail server
- 192.168.100.7 – DNS / file and print sharing server
- 192.168.100.8 – Syslog and NTP server
- 192.168.100.9 – Watchguard firewall management console

Use of Watchguard Firebox III 1000 firewall appliance has been influenced by its very good feature versus cost ratio. It was decided that there would be only one, main firewall system protecting GIAC's internal and DMZ networks. After researching Watchguard's Firebox III products it was determined that Firebox III 1000 firewall appliance would be able to perform the required role without compromises to GIAC's perimeter security. Its built in proxy services would provide GIAC network with additional security for its main Internet services – SMTP, FTP, HTTP and DNS. Also, Firebox's built in VPN components would address the problem of allowing secure, encrypted access, by GIAC's remote users, to company's network.

Other firewall products have been considered, but our IT staff was already familiar with Watchguard products and the cost involved in retraining GIAC's technical staff on other firewall solutions would be too great. Also, comparable devices were simply more expensive.

Choice of free IDS solution (Snort) was also applauded by GIAC's management staff.

2. Assignment 2 – Security Policy and Tutorial

Based on the security architecture defined in **Assignment 1** we will provide security policies for the following devices :

- Border Router
- Primary Firewall
- VPN

2.1 Security policy for Border Router

GIAC will implement CISCO's packet filtering capabilities to perform initial screening of GE network. This will relieve GIAC's main firewall from processing unwanted, Internet traffic. As stated in section 1, we have used the NSA/SNAC Router Security Configuration Guide as a reference of how to harden a CISCO border router.

First step in securing our border router will be to address the problem of accessing the router itself.

2.1.1. Router access

We will turn off all unnecessary services running on the router :

no cdp run

CDP (CISCO Discovery Protocol) is a CISCO proprietary protocol used by CISCO routers to identify each other on the network. It is considered to be very insecure and in most cases it is not needed.

no service tcp-small-servers
no service udp-small-servers

The above two lines disable simple services (echo, chargen, discard and daytime) running on the router. These services, in most cases, are not required.

In our next step we will disable finger service :

no ip finger
no service finger

The finger service is used for checking what and how many users are logged in on a specific host. By leaving this service on an attacker could obtain very useful information about who is logged in to our router and from where.

In the next step we will disable the following services :

no ip source route
no ip classless
no ip bootp server
no ip http server
no ip domain lookup

IP source route is a feature of IP protocol which allows individual packets to specify their own routes. It can be used to attack our firewall (i.e. spoofing). It will be disabled.

No IP classless disables classless routing.

BOOTP server is used to download IOS software from one CISCO router to another CISCO router or routers. If left enabled, an attacker could download our border router's IOS software.

HTTP server allows us to remotely administer the router using a web browser.

We don't want to allow web based administration since it sends critical passwords in plain text. It also requires that users log in using full, level 15 privilege, which could cause potential problems.

No IP domain lookup disables domain name lookups

In the next step we will disable autoloading of CISCO startup and configuration :

no boot network
no service config

Loading configuration from the network is not secure. It should only be used on an isolated network (i.e. lab setup).

Next step will involve disabling all SNMP services :

no snmp-server enable traps
no snmp-server system-shutdown
no snmp-server trap-auth
no snmp server

Simple Network Management Protocol (SNMP) is used for automated monitoring and administration. In most cases the SNMP protocol is considered insecure and could be used by an attacker to collect valuable network and hosts diagnostic information. We are not running SNMP on our network therefore we will disable SNMP services on the router.

Next we will setup our border router to use MD5 password encryption. CISCO IOS comes with 2 kinds of password encryptions :

- type 7, which uses CISCO-defined encryption algorithm and is considered to be weak
- type 5, which uses MD5 hash algorithm and has proven to be much stronger

Based on CISCO's recommendation, we will use type 5 password encryption. To enable MD5 password encryption on our border router we will use the following commands :

```
service password-encryption  
enable secret "password"  
no enable password
```

Service password-encryption command will mask the passwords as they are being displayed on the screen.

Enable secret turns on MD5 password encryption

No enable password explicitly disables the weaker, type 7 password type

We have decided to allow only console access to our border router. The following commands will fulfill this requirement :

```
line con 0  
transport input none  
login local  
exec-timeout 5 0
```

The above commands enforce user login on the console, set 5 minute timeout for inactivity and disallow reverse-telnet access to the console port.

In the next 2 steps we will disable all other access to our border router.

First, we will disable access to the AUX port :

```
line aux 0  
transport input none  
login local  
exec-timeout 0 1  
no exec  
end
```

Second, we will turn off access to the virtual terminal lines :

```
no access-list 90
access-list 90 deny any log
line vty 0 4
    access-class 90 in
    transport input none
    login local
    exec-timeout 0 1
    no exec
end
```

We will enable syslog logging on the router and send syslog data to our central syslog server :

```
logging on
no logging console
logging xxx.yyy.zzz.2
logging facility local6
```

We will use manual clock synchronization on the router. No NTP service will be running.

First we will set proper time zone for our clock :

```
clock timezone EST -5
```

Then we will set the correct time :

```
clock set 15:33:00 2 Nov 2003
```

The clock will be verified on bi-weekly basis with our main NTP server on the DMZ network.

We will also add a warning banner to advise any unauthorized personnel that it would be unlawful to access or attempt to access the router

```
banner /
WARNING: authorized personnel access only
/
```

2.1.2 Ingress and Egress Packet filtering setup on the Border Router

To control network traffic from the Internet to our border router and from our FW/VPN appliance to the router we will use Extended Access Control Lists (ACL's) on both external and internal interfaces of the router. Extended ACL's will allow us to filter out IP traffic more thoroughly than Standard ACL's. Instead of only testing IP source of the incoming packet, using Extended ACL's will add the following testing criteria :

- IP destination
- PROTOCOL, UDP or TCP port, ICMP type
- Flag testing, type of service

2.1.2.1 Ingress packet filtering

The external interface of the router will be setup as follows :

Interface Serial 0

```
ip address xxx.yyy.zzz.150 255.255.255.252
ip access-group 101 in
no ip direct-broadcast
no ip unreachable
no ip redirect
no ip mask-reply
ntp disable
```

no ip direct-broadcast command will prevent direct broadcasts from accessing our router. Direct broadcasts can be used to launch "Smurf" attacks on our network.

no ip unreachable command will prevent our router from providing network information based on ICMP error messages.

no ip redirect and no mask-reply will protect us from DOS attacks

Since our router clock is set manually, we will disable NTP service

```
access-list 101 deny ip host xxx.yyy.zzz.150 any log
```

```
access-list 101 deny ip xxx.yyy.zzz.0 0.0.0.15 any log
```

We will block all packets with source IP addresses of GIAC's internal network coming in from the Internet. If these addresses are coming from the Internet it could be due to misconfiguration or malicious intent.

```
access-list 101 deny ip host xxx.yyy.zzz.150 host xxx.yyy.zzz.150 log
```

This will prevent a "Land attack" against our border router.

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

We will block multicast or engineer network addresses.

access-list 101 deny 127.0.0.0 0.255.255.255 any

We will filter out loopback address. Loopback address should only be used internally on a host.

access-list 101 deny ip 10.0.0.0 0.255.255.255 any

access-list 101 deny ip 172.16.0.0 0.15.255.255 any

access-list 101 deny ip 192.168.0.0 0.0.255.255 any

We will block traffic with source IP addresses coming from private IP address pool. Private IP addresses are of non-routable kind and should not be used as source IP addresses. If we do receive IP packets coming from these ranges it would be either due to misconfiguration or possibly a sign of DOS attack.

access-list 101 deny ip 0.0.0.0 0.255.255.255 any

access-list 101 deny ip 1.0.0.0 0.255.255.255 any

access-list 101 deny ip 2.0.0.0 0.255.255.255 any

access-list 101 deny ip 5.0.0.0 0.255.255.255 any

access-list 101 deny ip 7.0.0.0 0.255.255.255 any

access-list 101 deny ip 23.0.0.0 0.255.255.255 any

access-list 101 deny ip 27.0.0.0 0.255.255.255 any

access-list 101 deny ip 31.0.0.0 0.255.255.255 any

access-list 101 deny ip 36.0.0.0 0.255.255.255 any

access-list 101 deny ip 37.0.0.0 0.255.255.255 any

access-list 101 deny ip 39.0.0.0 0.255.255.255 any

access-list 101 deny ip 41.0.0.0 0.255.255.255 any

access-list 101 deny ip 42.0.0.0 0.255.255.255 any

access-list 101 deny ip 58.0.0.0 0.255.255.255 any

access-list 101 deny ip 59.0.0.0 0.255.255.255 any

..... etc.

We will filter out all unallocated legal IP addresses (based on IANA list - <http://www.iana.org/assignments/ipv4-address-space>). We shouldn't be receiving any packets originating from these IP addresses.

access-list 101 deny ip host 211.239.123.56 any log

access-list 101 deny ip host 61.50.139.141 any log

access-list 101 deny ip host 163.180.51.37 any log

access-list 101 deny ip host 61.231.168.28 any log

access-list 101 deny ip host 81.226.184.28 any log

access-list 101 deny ip host 151.197.192.123 any log

access-list 101 deny ip host 202.175.72.85 any log

access-list 101 deny ip host 203.59.172.23 any log

access-list 101 deny ip host 209.30.95.34 any log

access-list 101 deny ip host 213.67.122.248 any log

Based on <http://www.dshield.org/top10.php> list of the top 10 source ip addresses launching attacks we will block packets coming from these IP addresses.

access-list 101 deny TCP any any range 135 139


```
access-list 101 deny UDP any any range 135 139
access-list 101 deny TCP any any 445
access-list 101 deny UDP any any 445
access-list 101 deny TCP any any 23 log
access-list 101 deny TCP any any range 6000 6255 log
access-list 101 deny UDP any any range 6000 6255 log
access-list 101 deny TCP any any 69 log
access-list 101 deny UDP any any 69 log
access-list 101 deny TCP any any range 512 514 log
access-list 101 deny TCP any any 111 log
access-list 101 deny UDP any any 111 log
access-list 101 deny TCP any any 2049 log
access-list 101 deny UDP any any 2049 log
access-list 101 deny TCP any any range 161 162 log
access-list 101 deny TCP any any range 161 162 log
access-list 101 deny UDP any any 514 log
```

We will block critical services of our internal environment. As we have both Windows and Unix machines running on our network we will be filtering out Windows and Unix specific services. By blocking these ports on our router's external interface we are adding second layer of protection to our setup as our firewall is configured to block these ports as well.

```
access-list 101 permit ip any host xxx.yyy.zzz.2
access-list 101 permit ip any host xxx.yyy.zzz.3
access-list 101 permit ip any host xxx.yyy.zzz.4
access-list 101 permit ip any host xxx.yyy.zzz.5
access-list 101 permit ip any host xxx.yyy.zzz.6
access-list 101 permit ip any host xxx.yyy.zzz.7
```

We will only allow access to the external address of the firewall and 5 public servers located on our DMZ network (external SMTP mail relay server, Web server, external DNS server, Secure reverse proxy server and SSH2 (secure FTP) server)

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

We will deny and log any other traffic.

2.1.2.2 Egress packet filtering

The border router internal interface will be configured as follows :

```
interface Ethernet 0
  ip address xxx.yyy.zzz.1 255.255.255.240
  ip access-group 102 in
  ntp disable
```

As we are not using NTP service on the router, we will disable this service (the router's clock is set manually).

access-list 102 deny TCP any any range 135 139 log-input
access-list 102 deny UDP any any range 135 139 log-input
access-list 102 deny TCP any any 445 log-input
access-list 102 deny UDP any any 445 log-input
access-list 102 deny TCP any any 23 log-input
access-list 102 deny TCP any any range 6000 6255 log
access-list 102 deny UDP any any range 6000 6255 log
access-list 102 deny TCP any any 69 log-input
access-list 102 deny UDP any any 69 log-input
access-list 102 deny TCP any any range 512 514 log-input
access-list 102 deny TCP any any 111 log-input
access-list 102 deny UDP any any 111 log-input
access-list 102 deny TCP any any 2049 log
access-list 102 deny UDP any any 2049 log
access-list 102 deny TCP any any range 161 162 log-input
access-list 102 deny TCP any any range 161 162 log-input
access-list 102 deny UDP any any 514 log-input

We will block critical services from leaving our internal environment in case of internal host(s) compromise. As we have both Windows and Unix machines running on our network we will be filtering out Windows and Unix specific services. The log-input was used for most of the services to allow recording of MAC address of the source. This will help in determining the origin of the attack.

access-list 102 permit ip xxx.yyy.zzz.0 0.0.0.15 any

We will only allow traffic originating from GIAC's network.

access-list 102 deny ip any any log-input

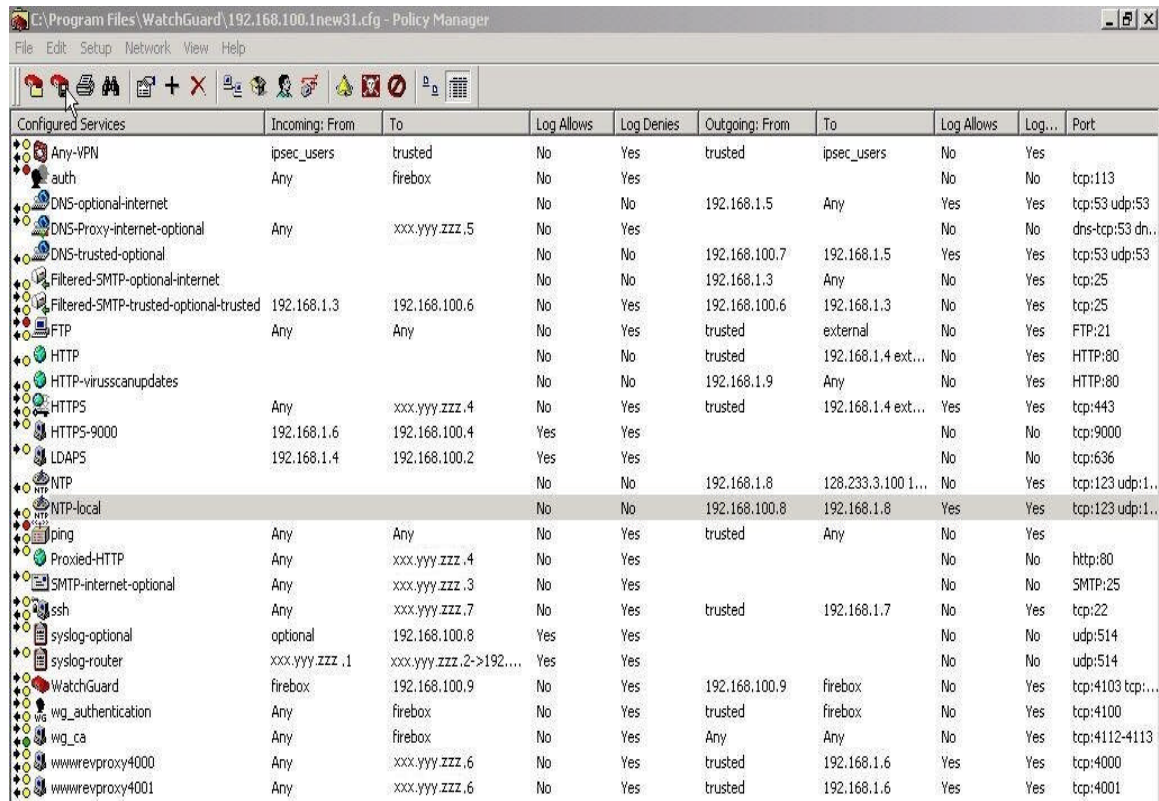
We will deny and log everything else.

ACL's are processed in top down order. When a match is found the processing is stopped. This means that ordering of ACL's is very important.

© SANS Institute 2004. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without the prior written permission of SANS Institute.

2.2 Security Policy for Primary Firewall

The following Firewall policy has been implemented to accommodate all required network traffic :



Configured Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log...	Port
Any-VPN	ipsec_users	trusted	No	Yes	trusted	ipsec_users	No	Yes	
auth	Any	firebox	No	Yes			No	No	tcp:113
DNS-optional-internet			No	No	192.168.1.5	Any	Yes	Yes	tcp:53 udp:53
DNS-Proxy-internet-optional	Any	xxx.yyy.zzz.5	No	Yes			No	No	dns-tcp:53 dn...
DNS-trusted-optional			No	No	192.168.100.7	192.168.1.5	Yes	Yes	tcp:53 udp:53
Filtered-SMTP-optional-internet			No	No	192.168.1.3	Any	No	Yes	tcp:25
Filtered-SMTP-trusted-optional-trusted	192.168.1.3	192.168.100.6	No	Yes	192.168.100.6	192.168.1.3	No	Yes	tcp:25
FTP	Any	Any	No	Yes	trusted	external	No	Yes	FTP:21
HTTP			No	No	trusted	192.168.1.4 ext...	No	Yes	HTTP:80
HTTP-viruscanupdates			No	No	192.168.1.9	Any	No	Yes	HTTP:80
HTTPS	Any	xxx.yyy.zzz.4	No	Yes	trusted	192.168.1.4 ext...	Yes	Yes	tcp:443
HTTPS-9000	192.168.1.6	192.168.100.4	Yes	Yes			No	No	tcp:9000
LDAPs	192.168.1.4	192.168.100.2	Yes	Yes			No	No	tcp:636
NTP			No	No	192.168.1.8	128.233.3.100 1...	No	Yes	tcp:123 udp:1...
NTP-local			No	No	192.168.100.8	192.168.1.8	Yes	Yes	tcp:123 udp:1...
ping	Any	Any	No	Yes	trusted	Any	No	Yes	
Proxied-HTTP	Any	xxx.yyy.zzz.4	No	Yes			No	No	http:80
SMTP-internet-optional	Any	xxx.yyy.zzz.3	No	Yes			No	No	SMTP:25
ssh	Any	xxx.yyy.zzz.7	No	Yes	trusted	192.168.1.7	No	Yes	tcp:22
syslog-optional	optional	192.168.100.8	Yes	Yes			No	No	udp:514
syslog-router	xxx.yyy.zzz.1	xxx.yyy.zzz.2->192...	Yes	Yes			No	No	udp:514
WatchGuard	firebox	192.168.100.9	No	Yes	192.168.100.9	firebox	No	Yes	tcp:4103 tcp:...
wg_authentication	Any	firebox	No	Yes	trusted	firebox	No	Yes	tcp:4100
wg_ca	Any	firebox	No	Yes	Any	Any	No	Yes	tcp:4112-4113
wwwrevproxy4000	Any	xxx.yyy.zzz.6	No	Yes	trusted	192.168.1.6	Yes	Yes	tcp:4000
wwwrevproxy4001	Any	xxx.yyy.zzz.6	No	Yes	trusted	192.168.1.6	Yes	Yes	tcp:4001

Figure 2.2

1. IPSEC users access

Any service (filtered) – Enable Incoming from ipsec_users to Trusted(local) network and Enable Outgoing from Trusted (local network) to ipsec_users
The purpose of this rule is to allow all MUVPN (mobile users with VPN IPsec login) to connect to Trusted(Internal) network. This will permit mobile users (telecommuters and sales force) two-way unrestricted access to GIAC's trusted (Internal) network

WG screenshot rule :

Configured Services	Incoming: Fr...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
Any	ipsec_users	trusted	No	Yes	trusted	ipsec_users	No	Yes	

Figure 2.2.1

2. AUTH/IDENT reject rule for smooth SMTP connections

Auth service TCP port: 113 (filtered) – Enabled and Denied Incoming from Any to the Firebox , Disabled Outgoing

The purpose of this rule is to reject auth/ident service coming from our ISP's SMTP server to our SMTP server. This is used to prevent long negotiation time-

outs. By having this service rejecting auth/ident requests coming from our ISP's SMTP server we should not experience delays in our mail delivery. Watchguard's recommendations for this service are a little different : *"The safest way to handle incoming Auth is to enable requests to the Firebox. The Firebox will respond with a generic user name and the Firebox's External IP address. This allows the service transaction to take place, while preserving the secrecy of your private networks"*.

As we can see, our rule doesn't exactly match Watchguard's guideline. To make sure this service is doing what was intended, we could monitor our Firebox's SMTP logs and determine if there are problems with AUTH/IDENT configuration. WG firewall rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
auth	Any	firebox	No	Yes			No	No	tcp:113

Figure 2.2.2

3. DNS access from our external DNS server to the Internet for zone transfers. TCP (for server-server zone transfers) and UDP (for client-server lookups)
DNS service TCP port: 53, UDP port: 53 (filtered) – Disabled Incoming , Enabled Outgoing from our External DNS server(192.168.1.5) to the Internet
 The purpose of this rule is to allow outgoing traffic from our external DNS server to the Internet (including zone transfers). This service will be responsible for resolving any internet name resolution requests coming from GIAC's network .

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
DNS-optional-internet			No	No	192.168.1.5	Any	Yes	Yes	tcp:53 udp:53

Figure 2.2.3

4. DNS access from the Internet to our External DNS server on the Optional (DMZ) network.

DNS service TCP port: 53, UDP port: 53 (proxied) – Enabled and Allowed Incoming from Any to the External DNS server(xxx.yyy.zzz.5) , Disabled Outgoing

The purpose of this rule is to provide name resolution of our external servers from the Internet. We will be using DNS proxy service for inbound connections from the Internet to our DNS server to protect it from known DNS attacks. This rule will resolve DNS requests for GIAC's external servers coming from the Internet.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
DNS-Proxy-internet-optional	Any	xxx.yyy.zzz.5	No	Yes			No	No	dns-tcp:53 dr

Figure 2.2.4

5. DNS access from our Trusted (Local) network to Optional (DMZ) DNS server
DNS service TCP port: 53, UDP port: 53 (filtered) – Disabled Incoming, Enabled and Allowed Outgoing from our Trusted(local) DNS server(192.168.100.7) to Optional (DMZ) External DNS server (192.168.1.5)

The purpose of this rule is to allow any Internet name resolution requests originating from our local network to be forwarded from our local DNS server to our external DNS server. We have implemented a split DNS setup and this rule allows us to enable users on trusted network to resolve internet names.

WG screenshot rule :

Configure Services	Incoming: Fr...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
DNS-trusted-optional	No	No	192.168.100.7	192.168.1.5	Yes	Yes	tcp:53 udp:53		

Figure 2.2.5

6. SMTP access from our Optional network to the Internet

SMTP service TCP port: 25 (filtered) – Disabled Incoming, Enabled and Allowed Outgoing from our External SMTP Mail Relay Server(192.168.1.3) to the Internet

The purpose of this rule is to allow our External Mail Relay Server to send mail to the Internet. This rule will be responsible for forwarding mail messages from GIAC's network to the Internet

WG screenshot rule :

Configure Services	Incoming: Fr...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
Filtered-SMTP-optional-internet	No	No	192.168.1.3	Any	No	Yes	tcp:25		

Figure 2.2.6

7. SMTP access from Trusted (Local) SMTP server to SMTP Mail Relay Server on Optional (DMZ) network and from SMTP Mail Relay Server to local SMTP server

SMTP service TCP port: 25 (filtered) – Enabled and Allowed Incoming from the External SMTP Mail Relay Server(192.168.1.3) to the Local SMTP server(192.168.100.6) , Enabled and Allowed Outgoing from the Local SMTP server to the External SMTP Mail Relay Server

The purpose of this rule is to allow SMTP traffic between our local and external SMTP servers. This service will be responsible for forwarding mail originating from local SMTP server to GIAC's SMTP relay server located on DMZ network. Also all external mail upon passing through our external mail relay server will be send to our local SMTP server located on Trusted(local) network.

WG screenshot rule :

Configure Services	Incoming: Fr...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
Filtered-SMTP-trusted-optional-trusted	192.168.1.3	192.168.100.6	No	Yes	192.168.100.6	192.168.1.3	No	Yes	tcp:25

Figure 2.2.7

8. FTP access from Trusted to Any

FTP service TCP port: 21 (proxied) – Enabled and Denied Incoming from Any to Any , Enabled and Allowed Outgoing from Trusted to External (Internet)

The purpose of this rule is to allow our local users to FTP to the Internet. We will be using FTP proxy service for outgoing FTP connections. The firewall's FTP-proxy service will address problems arising from using NATted connection to the internet. It will translate the PORT command from the client's direct IP address to

the external IP address and a dynamically negotiate port for the data connection on the firewall itself. We will also log all incoming FTP attempts.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
FTP	Any	Any	No	Yes	trusted	external	No	Yes	FTP:21

Figure 2.2.8

9. HTTP Proxy – Hyper Text Transfer Protocol Proxy

HTTP service TCP port:80 (proxied) – Disabled Incoming , Enabled and Allowed Outgoing from Trusted(Local) network to GIAC's external Web Server(192.168.1.4) and to the Internet

The purpose of this rule is to allow our local users web access to our External Web Server and to the Internet. HTTP proxy will add content type filtering capabilities of the Firebox for better control of web traffic.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
HTTP			No	No	trusted	192.168.1.4 ext...	No	Yes	HTTP:80

Figure 2.2.9

10. HTTP Proxy – Hyper Text Transfer Protocol Proxy

HTTP-virusscanupdates service TCP port: 80 (proxied) – Disabled Incoming , Enabled and Allowed Outgoing from our External Virus Scanning / Backup server(192.168.1.9) to Any

The purpose of this rule is to allow our External Virus Scanning / Backup server to download virus update definitions. We will need to make sure that our Virus Scanning an E-mail scanning servers have the most up to date virus detection files and scanning exngines

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
HTTP-virusscanupdates			No	No	192.168.1.9	Any	No	Yes	HTTP:80

Figure 2.2.10

11. HTTPS (secure HTTP) access to GIAC's External Web server and Trusted (Local) network access to External Web Server and the Internet

HTTPS service TCP port:443 (filtered) – Enabled and Allowed Incoming from Any to External Web Server(xxx.yyy.zzz.4) and Enabled and Allowed Outgoing from Trusted to External Web Server and External (Internet)

The purpose of this rule is to allow incoming HTTPS access to our secure web pages on the External Web Server and to allow our local users access to HTTPS web pages on the External web server and the Internet. All business communication between our customers will be encrypted using SSL 128-bit protocol.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
HTTPS	Any	xxx.yyy.zzz.4	No	Yes	trusted	192.168.1.4 ext...	Yes	Yes	tcp:443

Figure 2.2.11

12. HTTPS on port 9000 - SSL 128bit secured page from our Reverse Proxy Server to our local Notes / Domino web server

HTTPS-9000 service TCP port: 9000 (filtered) - Enabled and Allowed Incoming from the Secure Reverse Proxy Server(192.168.1.6) to the Local Notes / Domino Web server) , Disabled Outgoing

The purpose of this rule is to allow our External Secure Reverse Proxy Server access to our Local Lotus Notes / Domino secure web server page(s). This rule will be responsible for SSL 128 bit secured communication between our secure reverse proxy server and our local Lotus Notes / Domino secure web server page(s). The page(s) will provide direct access to our Lotus Notes database of fortune cookie sayings.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
HTTPS-9000	192.168.1.6	192.168.100.4	Yes	Yes			No	No	tcp:9000

Figure 2.2.12

13. LDAPS – secure LDAP from our External Web Server to our Local LDAP Directory Server

LDAPS service TCP port: 636 (filtered) - Enabled and Allowed Incoming from the External Web Server(192.168.1.4) to our Local LDAP Directory Server(192.168.100.2) , Disabled Outgoing

The purpose of this rule is to allow our External Web Server to access our Local LDAP Directory Server for username registration. This rule will be responsible for accessing our local LDAP server via SSL 128 bit secured link for username registration.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
LDAPS	192.168.1.4	192.168.100.2	No	Yes			No	No	tcp:636

Figure 2.2.13

14. NTP – Network Time Protocol from our external NTP server to 4 Internet NTP stratum servers

NTP service TCP port:123, UDP port: 123 (filtered) - Disabled Incoming , Allowed and Enabled Outgoing from the External NTP server(192.168.1.8) to 128.233.3.100, 128.233.3.101, 128.250.36.2 and 217.153.69.35

The purpose of this rule is to allow time synchronization using outside atomic clock servers with our GIAC network. Time synchronization is very important for proper upkeep of log data. Administrators of GIAC networks require all log generating servers to have synchronized clocks for proper interpretation of log data.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
NTP			No	No	192.168.1.8	128.233.3.100 1...	No	Yes	tcp:123 udp:1

Figure 2.2.14

15. NTP – Network Time Protocol from the Internal NTP Server to the External NTP Server

NTP-local service TCP port: 123, UDP port: 123 (filtered) – Disabled Incoming , Enabled and Allowed Outgoing from the Internal NTP Server(192.168.100.8) to the External NTP Server (192.168.1.8)

The purpose of this rule is to allow local time synchronization using our NTP server on optional network. To protect our trusted (local) network from directly talking to external(Internet) NTP servers we will be using 2nd, local NTP server to synchronize time with GIAC's external NTP server. All local servers will synchronize their time with the local NTP server. Again, the idea is to keep our clocks in sync so the log data will be easier to read and interpret.

WG screenshot rule :

Configure Services	Incoming: From ...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
NTP-local	No	No		No	192.168.100.8	192.168.1.8	Yes	Yes	tcp:123,udp:1

Figure 2.2.15

16. PING – ICMP echo and echo reply

PING service (filtered) – Enabled and Denied Incoming , Enabled and Allowed outgoing from Trusted(local) network to Any

The purpose of this rule is to allow network testing and troubleshooting from our Trusted (Local) network to our DMZ network as well as the Internet. PING sends ICMP reply request message to a host, expecting an ICMP echo reply to be returned. It is very useful in measuring the round-trip time to the host, giving us some indication of how "far away" that host is. We will also log all ping attempts coming from the Internet.

WG screenshot rule :

Configure Services	Incoming: From...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
Ping	Any	Any	No	Yes	trusted	Any	No	Yes	

Figure 2.2.16

17. Proxied HTTP – Hyper Text Transfer Protocol proxy

HTTP service TCP port: 80 (proxied) – Enabled and Allowed Incoming from Any to the External Web Server (xxx.yyy.zzz.4) , Disabled Outgoing

The purpose of this rule is allow web access to our External Web Server. HTTP proxy will allow us to apply content type filtering capabilities of the Firebox for better control of web traffic. Watchguard recommends this service to be used on not very busy networks (not more than 500 users). If we discover that HTTP access is not fast enough due to network load, we will replace this service with filtered HTTP.

WG screenshot rule :

Configure Services	Incoming: From...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
Proxied-HTTP	Any	xxx.yyy.zzz.4	No	Yes			No	No	http:80

Figure 2.2.17

18. SMTP-internet-optional – Simple Mail Transfer Protocol proxy

SMTP-internet-optional service TCP port: 25 (proxied) – Enabled and Allowed Incoming from Any to the External SMTP server(xxx.yyy.zzz.3) , Disabled Outgoing

The purpose of this rule is to allow SMTP access from the Internet to our SMTP relay server on our optional (DMZ) network. SMTP proxy service will analyze external mail content before sending it off to our internal mail server. It can perform the following tasks : SMTP mail relay protection, mail server profiling prevention, MIME content type filtering, filename content type filtering, buffer overflow exploit prevention, SMTP header syntax checking, SMTP header type filtering, recipient filtering - inbound and outbound, outbound address masquerading, outbound MIME-type masquerading, outbound header filtering, automatic removal of potentially dangerous ESMTP headers. We will utilize only some of the security features mentioned.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
SMTP-internet-optional	Any	xxx.yyy.zzz.3	No	Yes			No	No	SMTP:25

Figure 2.2.18

19. SSH – secure shell access

SSH service TCP port: 22 (filtered) – Enabled and Allowed Incoming from Any to the External SSH2 Server(xxx.yyy.zzz.7) , Enabled and Allowed Outgoing from Trusted to the External SSH2 Server(192.168.1.7)

The purpose of this rule is to allow secure file transfer between our suppliers and our network. SSH secure shell protocol will be responsible for secure communications between our suppliers and our SSH2 server located on our Optional (DMZ) network under IP address xxx.yyy.zzz.7. Our suppliers will deposit their fortune cookie sayings files onto this server using secure ftp. We will also allow our local user to access this server using ssh protocol. As mentioned before local user access will be controlled by TCP wrappers.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
ssh	Any	xxx.yyy.zzz.7	No	Yes	trusted	192.168.1.7	No	Yes	tcp:22

Figure 2.2.19

20. Syslog – log collecting service

Syslog-optional service UDP port: 514 (filtered) – Enabled and Allowed Incoming from the Optional (DMZ) network to the Local Syslog Server (192.168.100.8) , Disabled Outgoing

The purpose of this rule is to allow collection of log data from all the Server on Optional (DMZ) network to a centralized syslog server located on our Trusted (Local) network. We need to be able to analyze log data generated by the servers located on the Optional (DMZ) network. Having a centralized server collecting all log data will make troubleshooting any server / network problems much easier.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
syslog-optional	optional	192.168.100.8	Yes	Yes			No	No	udp:514

Figure 2.2.20

21. Syslog – log collecting service

Syslog-router service UDP port: 514 (filtered) – Enabled and Allowed

Incoming from our border router (xxx.yyy.zzz.1) to the Local Syslog Server (192.168.100.8) , Disabled Outgoing

The purpose of this rule is to allow collection of log data from our border router to a centralized syslog server located on our Trusted (Local) network.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
syslog-router	xxx.yyy.zzz.1	xxx.yyy.zzz.2->192....	Yes	Yes			No	No	udp:514

Figure 2.2.21

22. Watchguard – for firewall appliance management

Watchguard service TCP ports: 4103 and 4105 (filtered) – Enabled and

Allowed Incoming from Firebox to 192.168.100.9 and Enabled and Allowed Outgoing from 192.168.100.9 to Firebox

The purpose of this rule is to allow management and maintenance of our firewall appliance. Watchguard service is used for managing the firewall appliance. It's a 3DES encrypted service. We will only allow access from a dedicated machine on our Trusted(Local) network under IP address 192.168.100.9

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
WatchGuard	firebox	192.168.100.9	No	Yes	192.168.100.9	firebox	No	Yes	tcp:4103 tcp:

Figure 2.2.22

23. wg_authentication – Watchguard authentication service

wg_authentication service TCP ports:4100 (filtered) – Enabled and Allowed

Incoming from Any to Firebox , Enabled and Allowed Outgoing from Trusted to Firebox

The purpose of this rule is to allow External users (in this case it will be used for VPN clients) to authenticate against the Firewall. Also, we will have an option of requiring internal users to authenticate before they can use specific service or services.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
wg_authentication	Any	firebox	No	Yes	trusted	firebox	No	Yes	tcp:4100

Figure 2.2.23

24. wg_ca – watchguard Certificate Authority service

wg_ca service TCP port: 4112-4114 (filtered) – Enabled and Allowed Incoming

from Any to Firebox , Enabled and Allowed Outgoing from Any to Any

The purpose of this rule is to allow access to Firebox's Certificate Authority. This will be used by VPN clients to obtain and renew their client certificates.

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
wg_ca	Any	firebox	No	Yes	Any	Any	No	Yes	tcp:4112-411

Figure 2.2.24

25. wwwrevproxy4000 – secure reverse proxy for Customers

wwwrevproxy4000 service TCP port:4000 (filtered) – Enabled and Allowed Incoming from Any to the External Secure Reverse Proxy Server (xxx.yyy.zzz.6) and Enabled and Allowed Outgoing from Trusted to Secure Reverse Proxy Server (192.168.1.6)

The purpose of this rule is to allow access to our Secure Reverse Proxy Server located on our Optional(DMZ) network, which in turn is used to allow access to our local Lotus Notes / Domino fortune cookie sayings database. For security reasons we have decided to use secure (SSL) reverse proxy to provide access to our local Notes / Domino web server. This will add additional level of protection to our fortune cookie sayings database running on Lotus Notes / Domino on our Trusted(local) network under IP address 192.168.100.4

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
wwwrevproxy4000	Any	xxx.yyy.zzz.6	No	Yes	trusted	192.168.1.6	Yes	Yes	tcp:4000

Figure 2.2.25

26. wwwrevproxy4001 – secure reverse proxy for Partners

wwwrevproxy4001 TCP port:4001 (filtered) – Enabled and Allowed Incoming from Any to External Secure Reverse Proxy Server (xxx.yyy.zzz.6) , Enabled and Allowed Outgoing from Trusted to Secure Reverse Proxy Server (192.168.1.6)

The purpose of this rule is to allow access to our Secure Reverse Proxy Server located on our Optional(DMZ) network, which in turn is used to allow access to our local Lotus Notes / Domino fortune cookie sayings database. For security reasons we have decided to use secure (SSL) reverse proxy to provide access to our local Notes / Domino web server. This will add additional level of protection to our fortune cookie sayings database running on Lotus Notes / Domino on our Trusted(local) network under IP address 192.168.100.4

WG screenshot rule :

Configure Services	Incoming: From	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
wwwrevproxy4001	Any	xxx.yyy.zzz.6	No	Yes	trusted	192.168.1.6	Yes	Yes	tcp:4001

Figure 2.2.25

Service precedence on the Firebox appliance works in the following manner :

- the most specific Incoming and Outgoing rules are processed first
- the least specific Incoming and Outgoing rules are processed last

The only exception to this rule is the Any service. The Any service always has higher precedence when it applies to the IP address/network of a particular packet.

Also the Blocked Site / Ports list takes yet higher priority over the services that are configured.

If two Incoming and Outgoing sections in two different service rules match exactly, then the service which appears first in the services list becomes the rule used for those matching criteria.

2.3 Security Policy for VPN

Full VPN functionality is included with Watchguard Firebox III 1000 firewall appliance.

We will only be using VPN client access functionality of the Watchguard firewall appliance as only GIAC's telecommuters and salesforce will be allowed access to the company's network.

2.3.1 VPN client software

Watchguard provides 2 versions of their mobile user VPN software (MUVPN)– one with ZoneLabs Personal Firewall and one without the firewall software. For added security, we will be using high encryption (128 bit) VPN client software with ZoneLabs Personal Firewall. Use of Personal Firewall is recommended to prevent overtaking of the client machine by a hacker and allowing unauthorized access to our network over VPN channel. The newest version of high encryption MUVPN software at the time of writing was 6.1.2.

2.3.2 VPN type

Watchguard allows us to choose from 2 different types of tunneling protocols : PPTP and IPSec. We have decided to opt for the IPSec solution due to its added security, interoperability and flexibility. Our Firebox III 1000 came with 50 user license for Mobile user VPN software(MUVPN) which uses IPSec tunneling protocol to establish remote connections.

2.3.3 Watchguard Firebox user authentication

Firebox has the following list of available authentication methods :

- Firebox
- NT Server
- RADIUS Server
- CRYPTOCARD Server
- SecureID Server

Because of small number of remote users, VPN clients will be authenticating using Firebox authentication (Watchguard doesn't recommend to use Firebox Authentication if there are more than 100 users to authenticate. Extended Authentication method should be used instead – i.e. RADIUS or SecureID). This will require us to create username and password (shared key) for each remote user on the Firebox itself. The password length will have to have a minimum length of 8 characters and will be known to both Network Administrator and remote user. Each remote user account created will be added to ipsec_users group automatically.

2.3.4 VPN authentication

We can use the following VPN authentication methods :

- pre-shared keys and
- digital certificates

We will utilize digital certificates as means of MUVPN authentication. They will provide us with a stronger and more scalable way of authentication than pre-shared-keys. Digital certificates are issued to clients by a trusted third party called Certificate Authority (CA). We will configure our Watchguard system to function as the CA (CA's are part of a system of key generation, key management and certification called a Public Key Infrastructure (PKI). The PKI provides for certificate and directory services that can generate, distribute, store and revoke certificates). For authenticating by way of Digital Certificates our Firebox appliance must be configured as a DVCP server (Watchguard's proprietary protocol called Dynamic VPN Configuration Protocol) which in turn automatically activates Watchguard's CA.

Upon each MUVPN configuration on the Firebox appliance the following 3 files will be generated :

- *.wgx file containing end user profile (The *.wgx file contains shared key, user identification, IP addresses and settings required to create a secure tunnel between the remote user and the Firebox)
- cacert.pem file containing root certificate and
- *.p12 file containing client certificate

These three files will need to be securely transferred onto every client machine (different set of files for each specific remote user). When a remote user will attempt to connect to GIAC network using their remote system, they will first open the *.wgx file. Before they can successfully open the *.wgx file, they will be prompted for their user password (shared key). If the supplied password is correct, the *.wgx file will open and automatically load root and client certificate files.

2.3.5 IPSec Setup details

Because we have implemented NAT with our IPSec MUVPN setup, we will be using ESP (Encapsulation Security Payload) as our authentication method instead of AH (Authentication Header). This is because NAT changes IP packet's address information thus the packet will fail its data integrity check under AH protocol, which requires every bit in the datagram to remain unchanged. Also, AH only ensures that the data received by a VPN end point has not been tampered with while in transit. It doesn't encrypt the data itself. ESP provides both Encryption and Data Integrity to protect the payload data.

The following 2 encryption algorithms are supported while using ESP:

- DES (less secure, not recommended for sensitive data, faster to compute)
- Triple DES (more secure, slower to compute)

We have chosen TripleDES as our encryption algorithm. Although slower to compute, it will provide us with much greater security than DES.

For Data Integrity, out of 2 options available to us, we have picked 128 bit strength Message Digest 5 (MD5) instead of 160 bit strength Secure Hash Algorithm (SHA). Even though SHA has a greater bit strength and is considered a little more secure than MD5, it places more load on our CPU. The difference in security between MD5 and SHA is minimal and both of them are considered very secure and are used extensively.

2.3.6 Firewall Policy for VPN

We will allow our mobile users (telecommuters and sales force) to use any service on our trusted network. The firewall rule will be as follows :

Configured Services	Incoming: Fr...	To	Log Allows	Log Denies	Outgoing: From	To	Log Allows	Log Denies	Port
 Any	ipsec_users	trusted	No	Yes	trusted	ipsec_users	No	Yes	

Figure 2.3.7

All MUVPN accounts will belong to ipsec_users group (they are added automatically to that group upon creation of their IPSec VPN account).

2.4 Firewall Policy Implementation Tutorial

The easiest way to perform initial Watchguard Firebox III 1000 configuration is through QuickSetup Wizard.



Figure 2.4.1

This initial screen gives a choice of configuring our Firebox in either Drop-In or Routed mode. Drop-in mode is recommend for networks with large number of available public IP addresses. It requires that all of 3 Firebox network interfaces use the same IP address (use of Proxy ARP is necessary for this setup to work). Routed mode, on the other hand, requires that all of Firebox 3 network interfaces reside on 3 different networks. Based on our GIAC network design, we will choose Routed mode for our Firebox.

The final configuration screen of our 3 network interfaces will look like this:

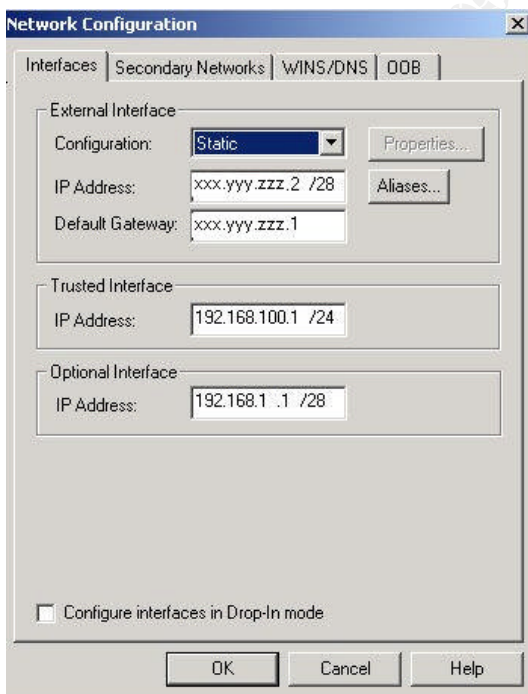


Figure 2.4.2

On our external interface will use a public IP address from a range provided to us by our ISP. Default gateway address here is the internal IP address of the Cisco border router. Trusted and Optional IP addresses have been drawn from private (non-routable) IP addresses range. They will serve as default gateways for systems behind each network address range. For systems behind the Optional (DMZ) interface we will need to configure 1-to-1NAT to map public IP addresses to private IP addresses.

After completing QuickSetup Wizard of our Firebox, the appliance will have a basic set of rules set up. These rules will need to be adjusted or replaced with more strict ones to match GIAC's security policy defined in part one of the document.

The following is the basic set of rules assigned to our Firebox III Appliance after completing our QuickSetup Wizard program.

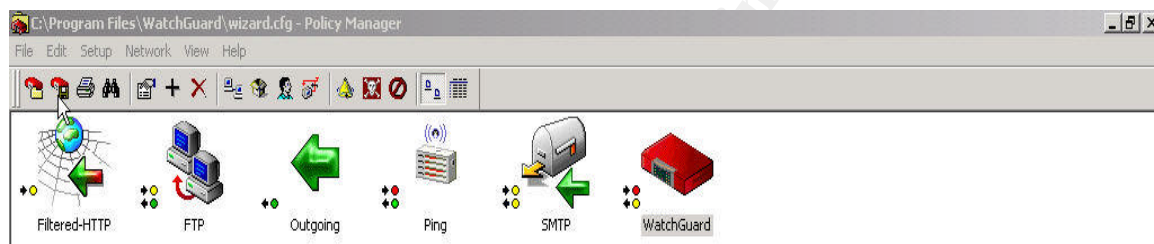


Figure 2.4.3

Before we start adding rules to our Firebox we will go through Firebox Setup and Configuration menu options.

To define the Firebox name click on Setup -> Name :



Figure 2.4.4

Firebox Name window will appear:

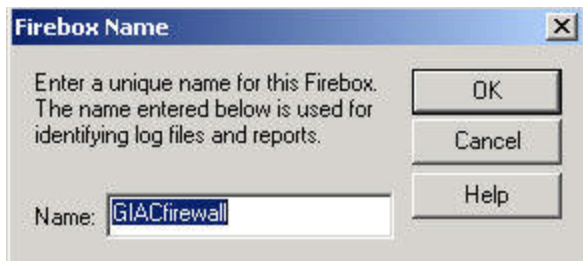


Figure 2.4.5

As stated, this name will be used in log files and reports generated by the Firebox.

Next option in Setup menu is Firebox Model. We will select Firebox model matching our Firebox III appliance model number printed on the front panel of the appliance.



Figure 2.4.6

Next set of options, called Intrusion Prevention will allow us to fine tune how our Firebox deals with outside attacks :

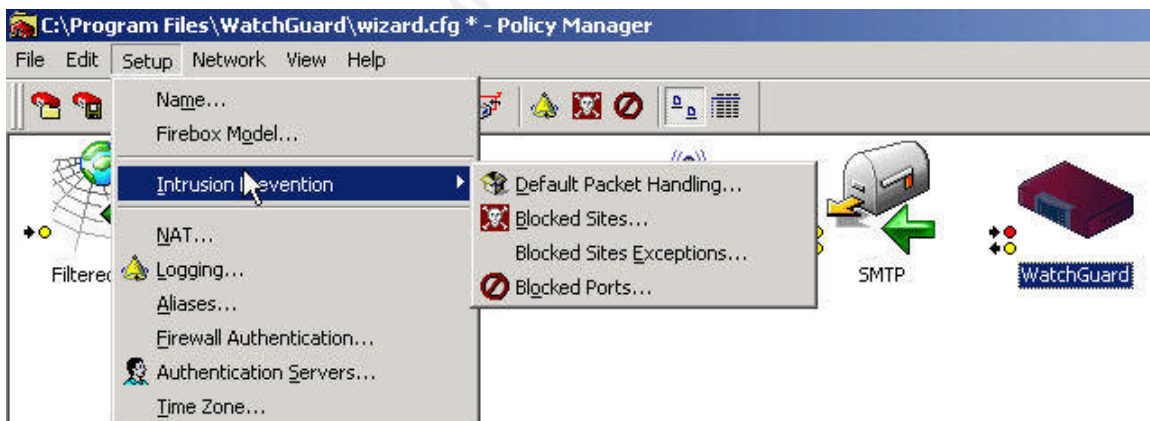


Figure 2.4.7

The following are Firebox's **Default Packet Handling** capabilities:

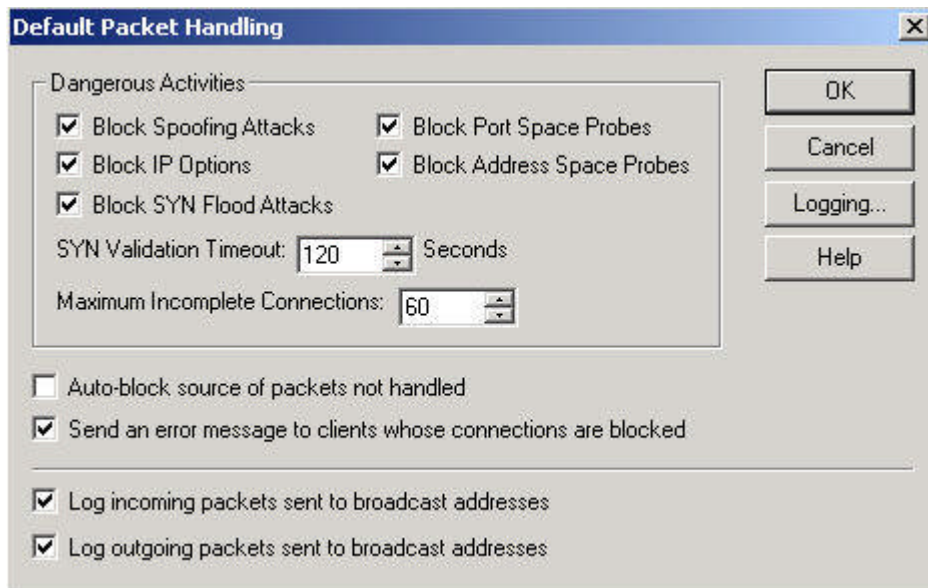


Figure 2.4.8

The following are detailed explanations of each packet handling options.

Block Spoofing Attacks

This option, when enabled, will attempt to block spoofing attacks against our network. The Firebox has a built-in anti-spoofing filter, which will automatically set up rules based on its interface configuration, network routes and IPSec routing policies to prevent spoofing attacks. When a spoofed packet enters the Firebox with a source port that does not belong on the interface in question, that packet will be blocked. The anti-spoofing filter will also block directed broadcasts and broadcasts through the Firebox. Additionally, we can log messages for incoming and outgoing packets sent to broadcast addresses (the last two options).

Block IP Options

If this option is activated, the Firebox will block all packets that contain IP options. IP options are special extensions of the IP protocol that are used for debugging or custom applications. Attackers use them as means to misroute traffic and bypass firewall defenses.

Block Port Space Probes

If this option is checked, the Firebox will automatically block the source IP address of port space probes. Port space probes are used to scan a host to find what services are running on it.

Block Address Space Probes

If this option is selected, the Firebox will automatically block the source IP address of IP space probes. Address space probes are used to scan a range of hosts to check what services are running on specific hosts.

Auto-block source of packets not handled

This option, when enabled, will cause the Firebox to automatically add the source IP address of packets blocked by default to the temporary blocked site list.

Send an error message to clients whose connections are blocked

This option will toggle whether or not the Firebox will send an ICMP destination port unreachable packet in response to a TCP SYN packet.

Blocked sites

This option will allow us to prevent unwanted traffic from known or suspected hostile system. The blocked sites list only applies to External interface. Connections between Optional and Trusted interfaces are not subject to Blocked Sites List. For now, we will keep the default settings:

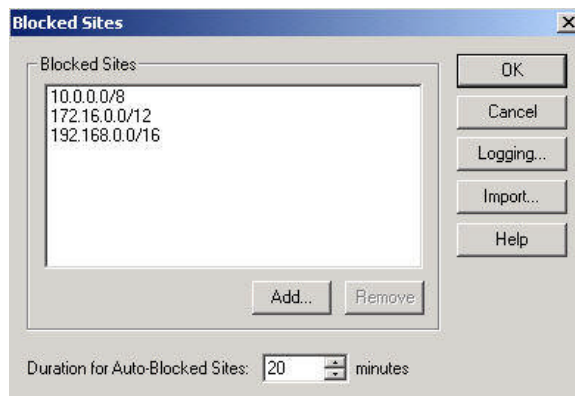


Figure 2.4.9

Note: traffic from the above networks is already being stopped by our border router. This option will add a second line of perimeter defense.

Blocked Sites Exceptions

This option lists host(s) that will not be added to the list of automatically blocked sites regardless of whether it fulfills criteria that would otherwise add it to the list. The site can still be blocked according to the Firebox configuration, but it will not be automatically blocked for any reason.

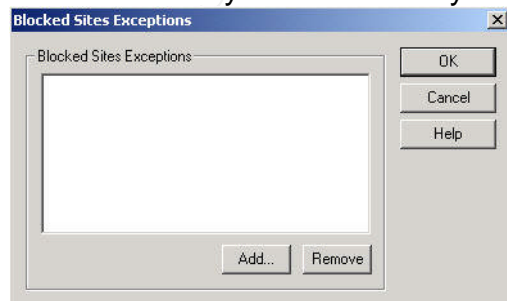


Figure 2.4.10

Blocked ports

This option will allow us to explicitly disable external network services from accessing ports that are vulnerable as entry points to our network. A blocked port setting takes precedence over any of the individual service configuration settings. The Blocked Ports feature will only block packets that enter our network through the External interface. Connections between the Optional and Trusted interfaces are not affected by the Blocked Ports list.

In summary :

- Blocked ports provide an additional layer of protection to our perimeter security by denying access to the most vulnerable ports regardless of firewall services configuration
- attacks against particularly sensitive services can be logged independently
- certain TCP/IP services that use port numbers above 1024 are vulnerable to attacks originating from allowed, well-known services with port numbers below 1024. These connections can be attacked by appearing to be an allowed connection in the opposite direction. This type of attack is preventable by blocking the port numbers of services whose port numbers are under 1024.

By default, the Firebox appliance blocks the following ports:

X Window System (ports 6000-6063)

The X Window System (or X-Windows) is known for its security problems. There are several authentication options available at the X server level (i.e. host or token authentication), but they are not very strong and are easily exploitable. As such, access to X Windows ports is blocked by default.

X Font Server (port 7100)

Many versions of X-Windows support font servers. Font servers are complex programs that run as the super-user on some hosts. Similarly to X Window System ports, X Font server port is blocked by default as well.

NFS (port 2049)

NFS (Network File System) allows us to share file systems over a network. However, current versions have serious authentication and security problems which make providing NFS service over the Internet very dangerous.

OpenWindows (port 2000)

OpenWindows is a windowing system from Sun Microsystems that has similar security risks to X Window.

rlogin, rsh, rcp, syslog (ports 513, 514)

These services provide remote access to other computers and are very insecure when used on the Internet (plain text passwords, automatic logins etc.)

RPC portmapper (port 111)

RPC Services use port 111 to determine which ports are actually used by a given RPC server. Because RPC services themselves are very vulnerable to attack over the Internet, the first step in attacking RPC services is to contact the portmapper to find out which services are available.

Port 0

Port 0 is reserved by IANA, but many programs that scan ports start their search on port 0.

Port 1

Port 1 is for the rarely used TCPmux service. Blocking it is another way to confuse port scanning programs.

Novell IPX over IP (port 213)

If we did use Novell IPX protocol over IP internally, we would want to explicitly block port 213.

NetBIOS services (ports 137 through 139)

We should block these ports as they are very often probed by network scanners. Although those services are blocked implicitly by default packet handling, blocking them here provides additional security.

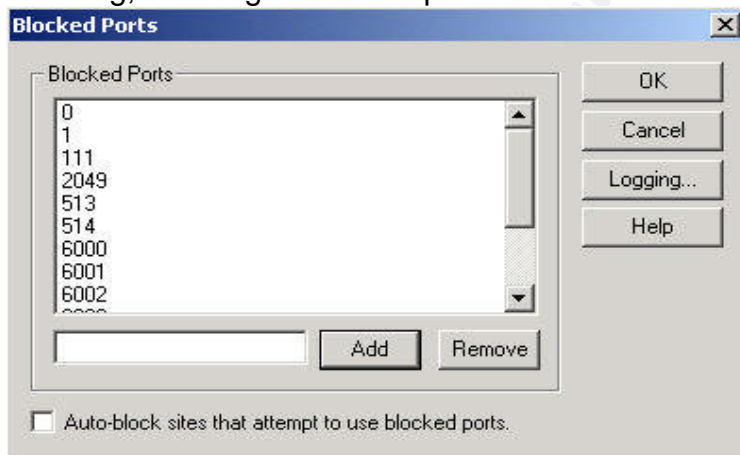


Figure 2.4.11

Note : because we are planning on allowing syslog service to transfer log data from our border router to our local, syslog server, we will need to remove port 514 (used by syslog service) from the default Blocked Ports list.

NAT Setup

We have described NAT settings in our IP addressing scheme part of the document. To allow a better flow through the settings we will touch on this option again.

By default, all private IP address ranges are added to perform dynamic NAT. They apply to both Optional and Trusted Interfaces. We will leave the settings as default (we could remove 172.16.x.x/12 and 10.x.x.x/8 ranges since we don't use them).

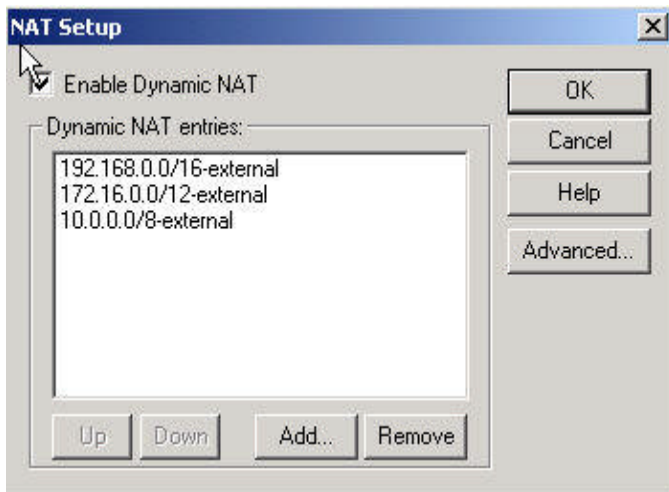


Figure 2.4.12

By clicking on the Advanced tab of NAT setup we will be able to fine tune our NAT configuration.

First option in the Advanced setup is Service-Based NAT.

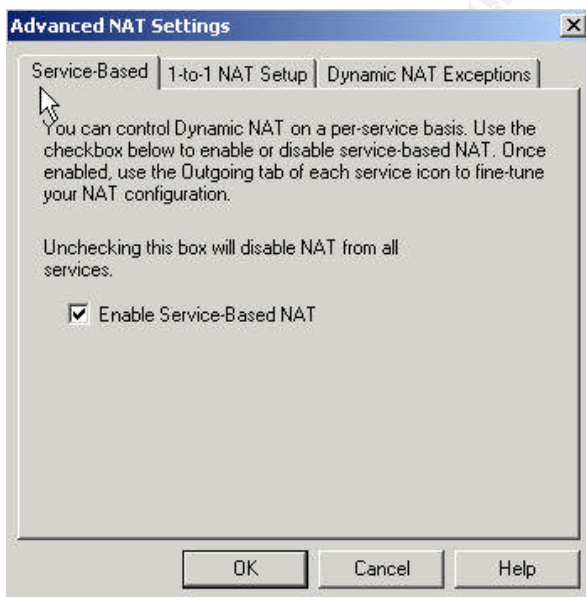


Figure 2.4.13

Second option is 1-to-1 NAT setup. We will use this option to map external IP addresses of our 5 public servers to their real, private IP addresses. First, we will enable 1-to-1 NAT.

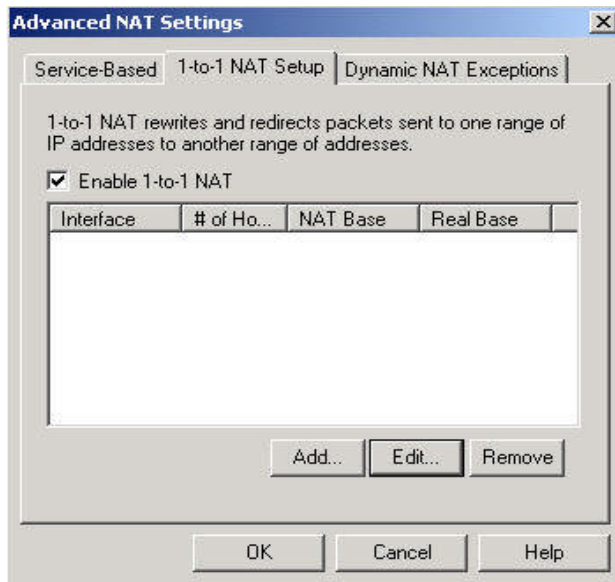


Figure 2.4.14

Then, we will create 1-to-1 NAT mapping range. In our case, we will be translating 5 public IP addresses, starting with xxx.yyy.zzz.3 to 5 private IP addresses starting with 192.168.1.3. This will setup a range of the following mapped IP addresses :

- xxx.yyy.zzz.3 will be mapped to 192.168.1.3 (external SMTP mail relay server)
- xxx.yyy.zzz.4 will be mapped to 192.168.1.4 (public web server)
- xxx.yyy.zzz.5 will be mapped to 192.168.1.5 (external DNS server)
- xxx.yyy.zzz.6 will be mapped to 192.168.1.6 (secure reverse proxy server)
- xxx.yyy.zzz.7 will be mapped to 192.168.1.7 (SSH2 secure ftp server)

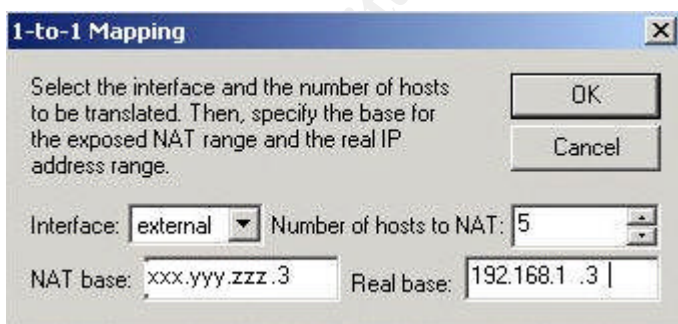


Figure 2.4.15

The final 1-to-1 NAT setup settings will look like this :

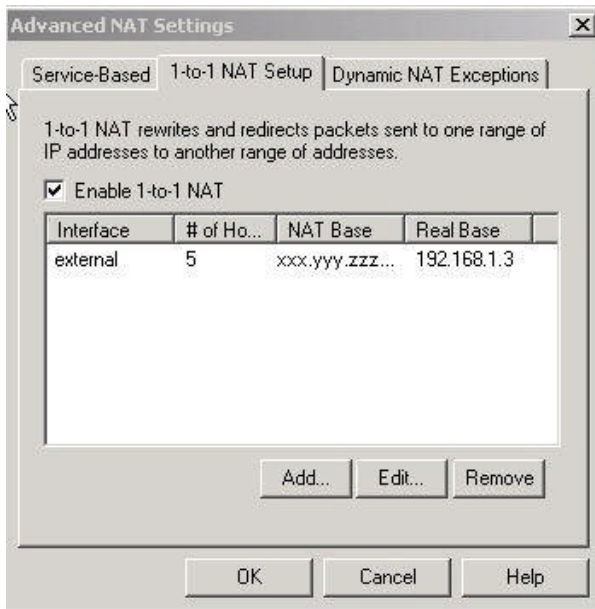


Figure 2.4.16

Because our Firebox operates the 1-to-1 NAT through Proxy-ARP it is imperative that the NATted IP addresses do not match any of the aliases or interfaces on the Firebox.

Keeping this in mind, we will configure Dynamic NAT Exceptions to exclude our 1-to-1 NAT real base address range from being included in the dynamic NAT mappings :

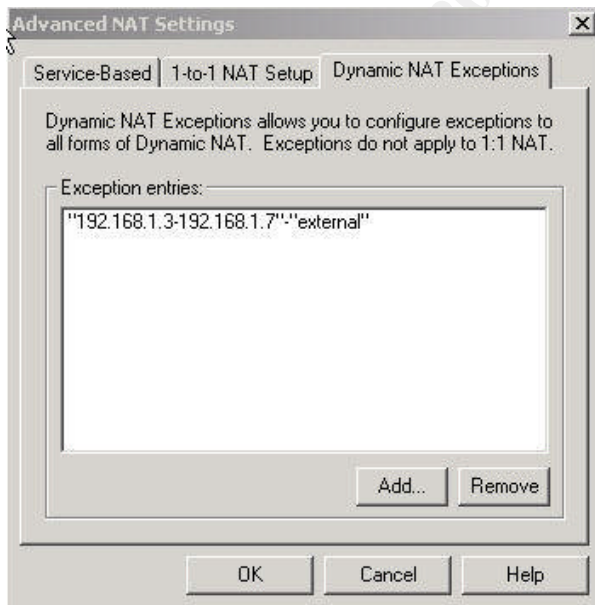


Figure 2.4.17

Next option is **Logging** :

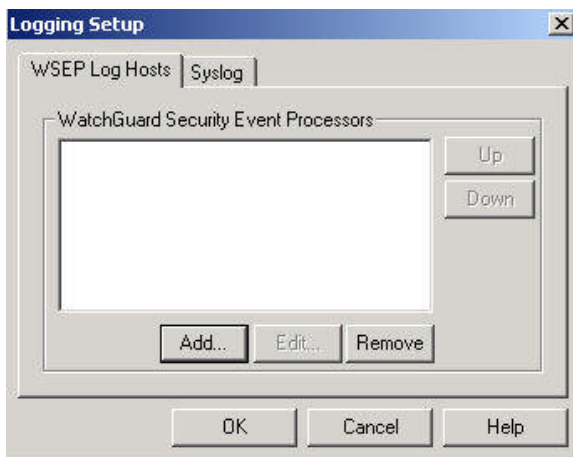


Figure 2.4.18

We will click on Add and specify one internal host IP address and access password to handle our Firebox log data.

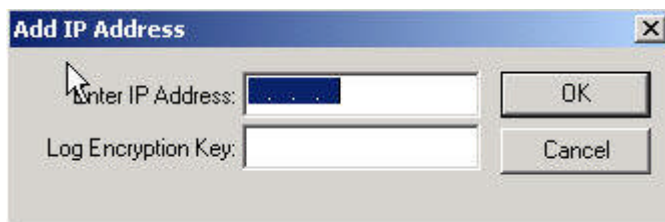


Figure 2.4.19

Our final screen will look like this :

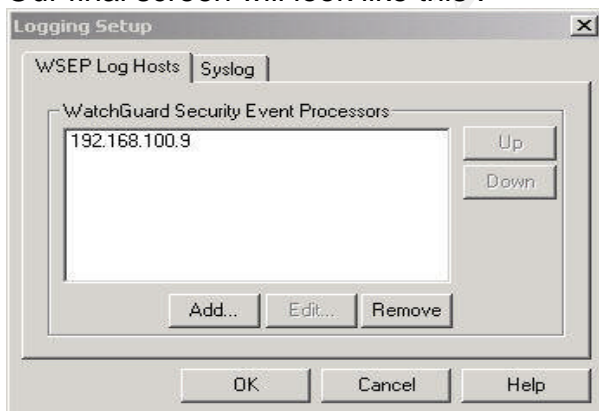


Figure 2.4.20

This option will send all logging data generated by our Firebox appliance to the Watchguard administration host located on Trusted (Local) network.

We also have an option to enable **Syslog** server to collect our Firebox data but we have chosen to use WSEP (Watchguard Security Even Processor) for gathering logging information.

Next option is **Aliases**

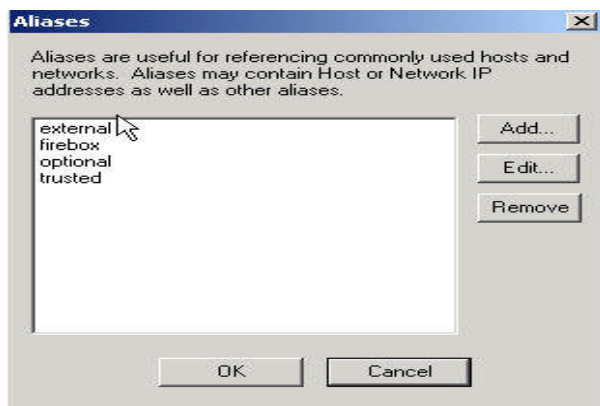


Figure 2.4.21

There are 4 default aliases configured. Here we could add aliases to describe our external and internal servers but we have decided to use IP addresses in our configuration.

Next option is **Firewall Authentication**

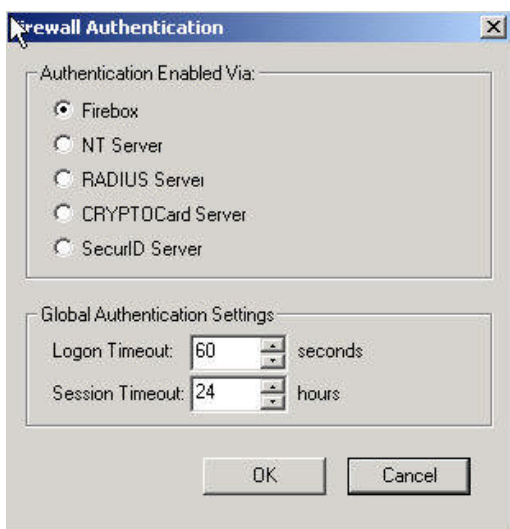


Figure 2.4.22

We will be using Firebox as our Authentication server. In our scenario, our Firebox appliance will be responsible for authenticating our VPN IPSec users. It can also be used to control user access to specific network resources for Incoming and Outgoing connections.

Next option is **Authentication Servers**

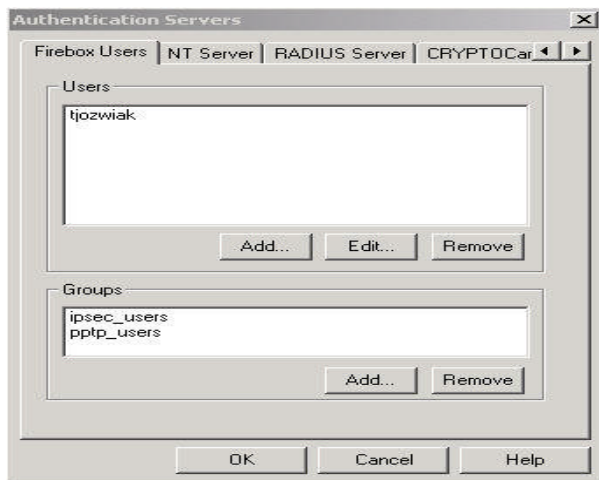


Figure 2.4.23

Under Authentication Servers menu we can configure Firebox user accounts and groups they belong to. These accounts are used for controlling VPN and Incoming / Outgoing access to our network services. We will set up the Firebox device as our Authentication server in the Firewall Authentication menu. We also have 4 other options for user “external” authentication to choose from. They are: NT Server, RADIUS Server, CRYPTOCARD or SecureID.

Next option is **Time Zone**.

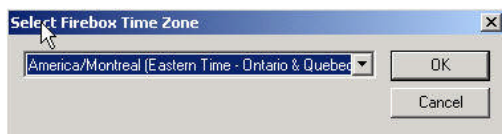


Figure 2.4.24

We have picked our local time zone as our Firebox Time Zone.

To define Network properties of our Firebox we will click on **Network** option :



Figure 2.4.25

Under Configuration, we can confirm IP addresses assigned to Watchguard's 3 network interfaces, default gateway (Cisco router's internal IP address) as well as Configuration mode type (Screenshot 2.4.2)

Next option is **Routes**.

We can define any static routes here. This option is mostly used if we had router(s) behind our Firebox. Our configuration includes 1 external router, which sits between our Firebox appliance and the Internet. No static routes are necessary.

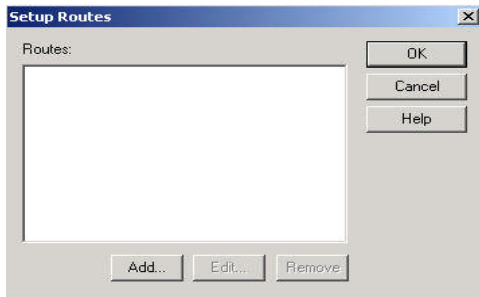


Figure 2.4.26

Next option on the list is **DHCP server**. We will not be using our Firebox as our DHCP server. This option will remain disabled.

Next option is **DVCP client**

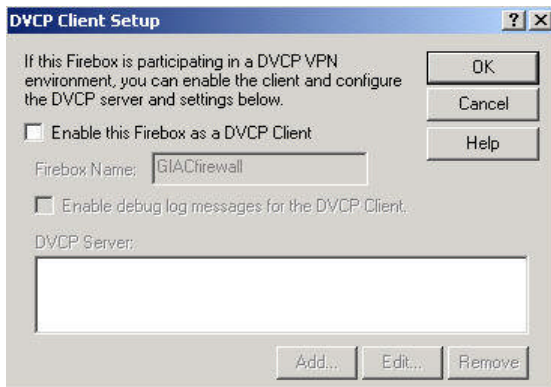


Figure 2.4.27

This option is used when the Watchguard Firebox appliance participates in branch office VPN configuration. We are only using MUVPN setup (client VPN) thus this option will be disabled.

Next option is **DVCP Server Properties**

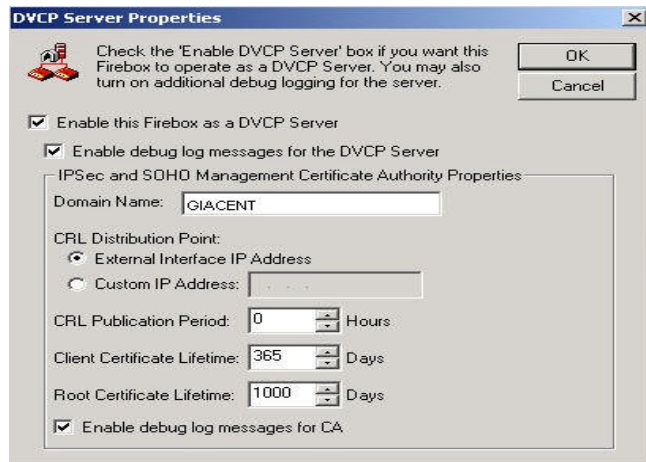


Figure 2.4.28

We will enable DVCP Server option since we will be using our Firebox as our Certificate Authority for issuing client certificates to our IPSec users.

Next option is **Branch Office VPN (BOVPN)**



Figure 2.4.29

We have 2 options under Branch Office VPN: **Basic DVCP Server Configuration** and **Manual IPsec Configuration**. We won't be using these options in our setup, since we are not implementing site-to-site VPN.

The last option in Configuration Menu is **Remote User Setup**. Remote user setup is divided into 3 categories:

Mobile User VPN setup

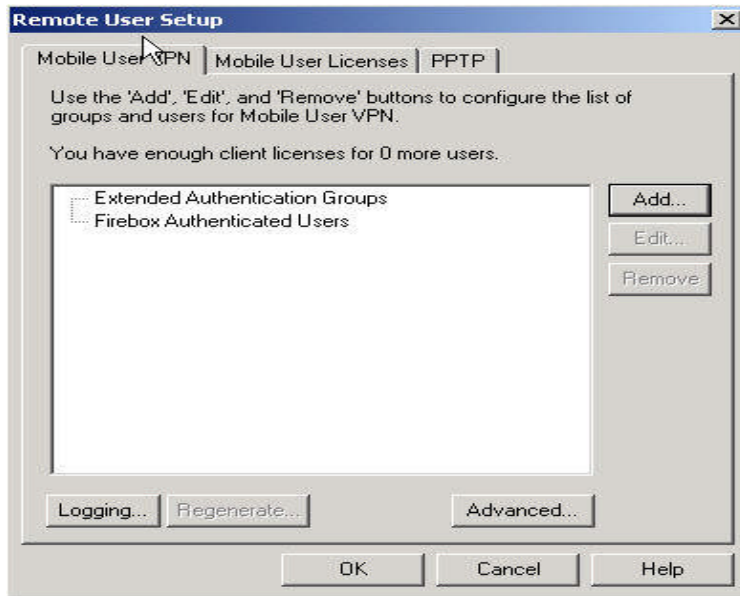


Figure 2.4.30

In here we can add, edit and remove VPN users based on their authentication method

Mobile User Licenses

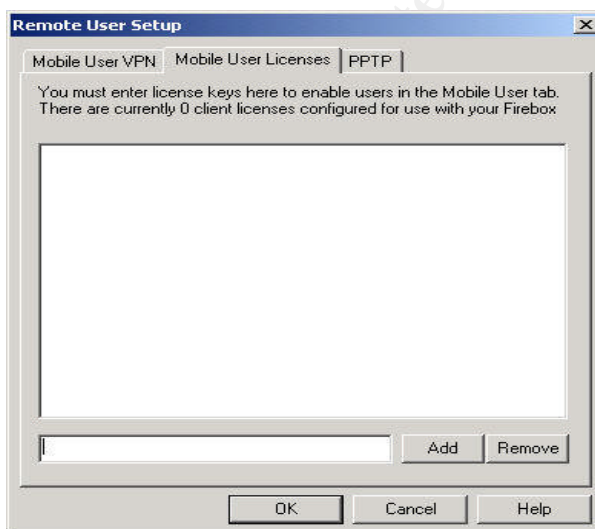


Figure 2.4.31

Under Mobile User Licenses we can add licenses for MUVPN access, which are required to use IPSec protocol.

PPTP setup

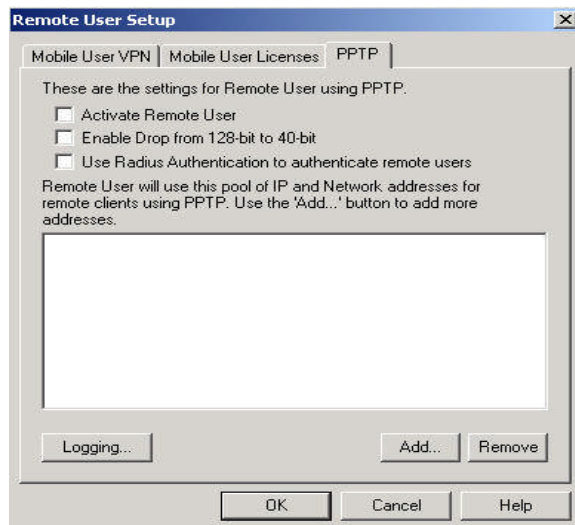


Figure 2.4.32

Should we decide to use PPTP access instead of (or in tandem with) MUVPN IPSec, the above options are available to us. There are no licenses required for PPTP as it doesn't use IPSec protocol. PPTP option may come useful for remote systems with slow or very slow internet access since it is faster than MUVPN with IPSec. We will not be using PPTP at this point, but should the need to provide remote access to clients with very slow internet connection arise, we will add these users as required.

Services configuration.

After completing Firebox configuration we can start adding Services to our Firewall security Policy. We will click on Edit option on the main menu, and then on Add Service:



Figure 2.4.33

In the Add Service option we will be presented with 3 sets of services :

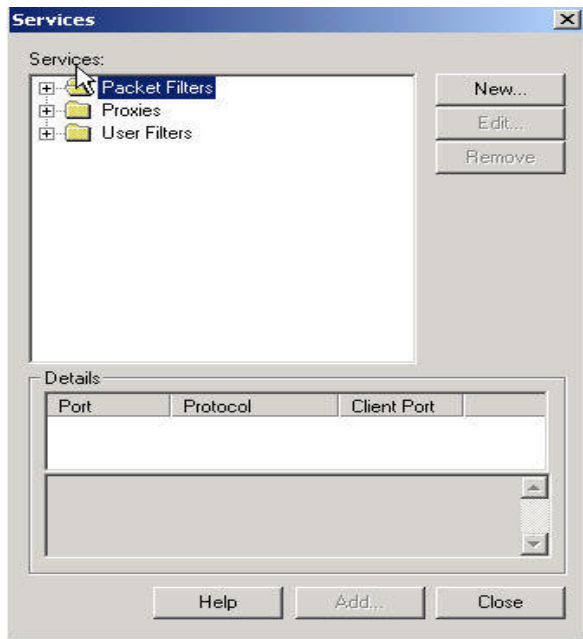


Figure 2.4.34

By default, we can choose from Watchguard list of pre-configured **Packet Filters** and **Proxies**. The **User Filters** folder will contain any custom (user) defined services.

When we expand **Packet Filters**, a built-in list of packet filters will open:

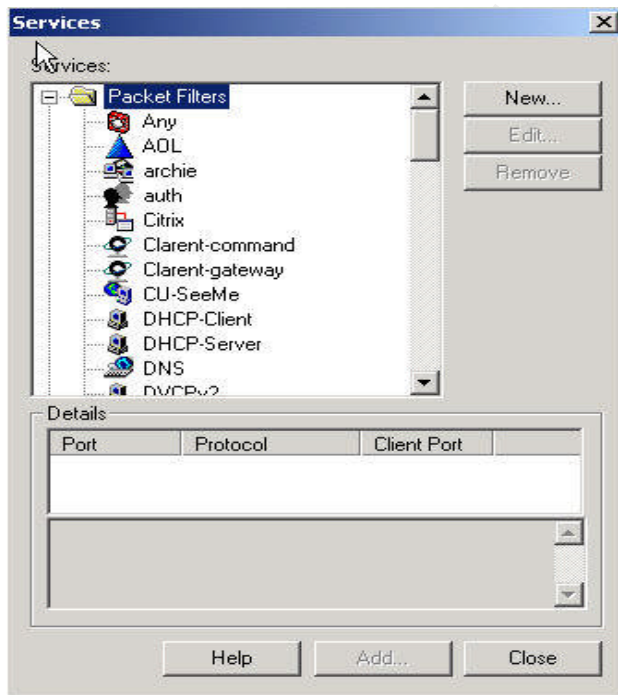


Figure 2.4.35

As we can see, we have an extensive list of pre-defined packet filtering services available to us.

The next services group available to us is **Proxies** :

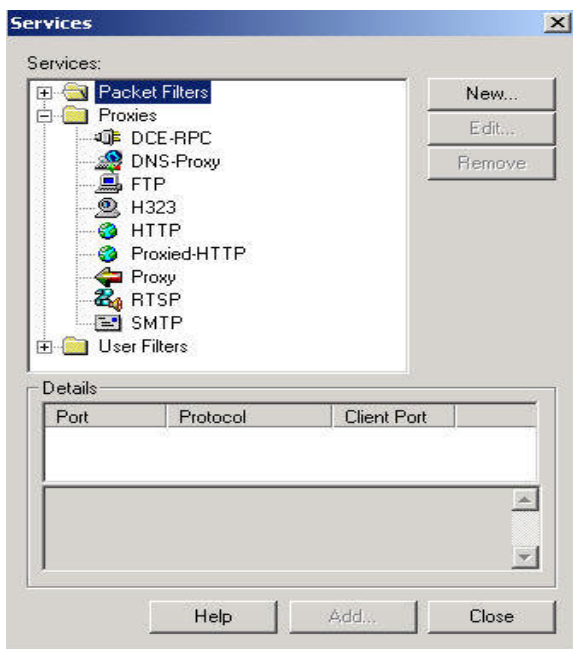


Figure 2.4.36

Watchguard Firebox III 1000 also comes with a rich list of pre-configured proxy services. We will utilize 4 of them.

The last group called **User Filters**, contains custom packet filters defined to allow access to custom ports and/or services.

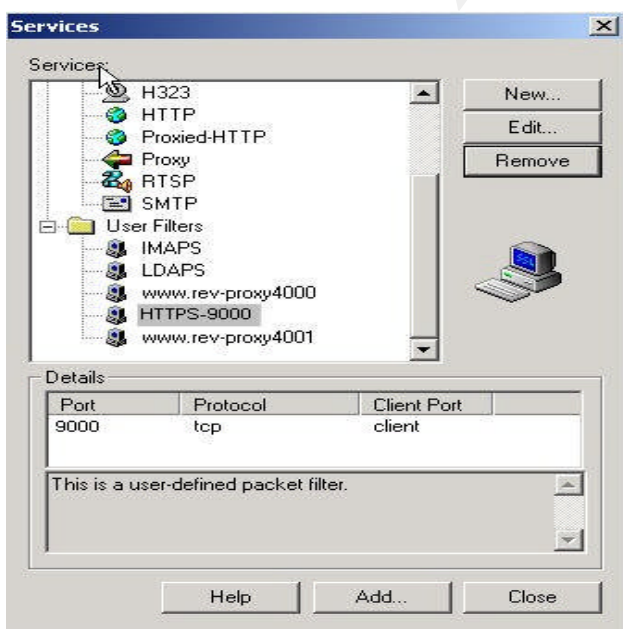


Figure 2.4.37

For the purpose of this document, I will demonstrate how to add **Proxy** and **User (custom) filter** services to the firewall security policy. The procedures to add **Packet filters**, as required, are the same.

Firebox's Proxy Services configuration

The Watchguard Firebox System comes with several proxies. The most commonly used are those for email (SMTP), DNS, FTP, and Web traffic (Proxied HTTP and HTTP). By requiring the Firebox to analyze each packet more closely, we can use proxies to create additional rules and restrictions on traffic using those ports and protocols. A firewall proxy goes beyond packet filtering capabilities. It examines not just the IP header information but also the contents. Because proxies examine every part of the packet, they are both more secure but also consume more CPU resources than a simple packet filters. We will utilize the following 4 Firebox proxies in our configuration : HTTP, SMTP, FTP and DNS.

Configuring HTTP proxy

In our main Firewall Policy window we will select Edit -> Add Service -> Proxies -> Proxied HTTP -> Add -> Proxy Name (leave as default) -> Click OK

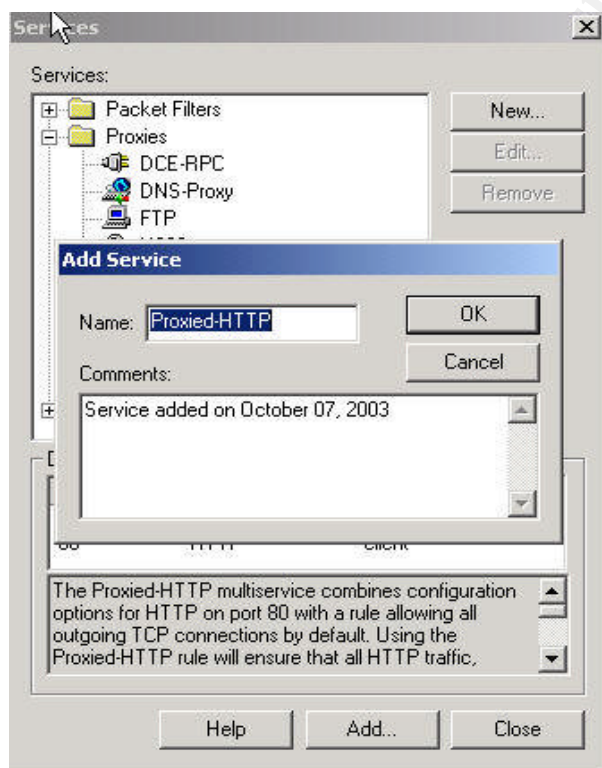


Figure 2.4.38

By default, Incoming Connections are Enabled and Denied. From drop down menu we will select Enabled and Allowed :

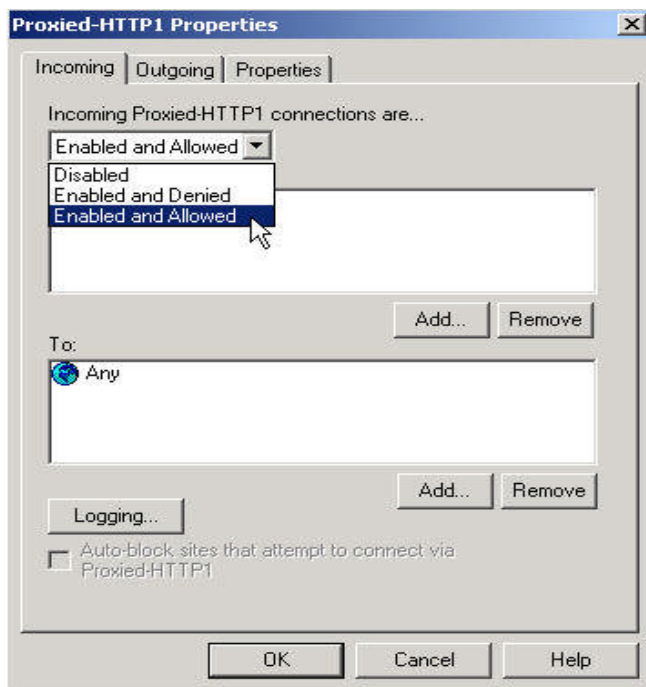


Figure 2.4.39

We'll leave **Incoming** -> From -> Any as is. We will need to change **Incoming To** from Any to the public IP address of our external Web Server – xxx.yyy.zzz.4. To add the IP address of our external web server for the Incoming To we'll click on Add -> Add Other, Choose Type – Host IP address. In Value field we'll type in xxx.yyy.zzz.4 then click OK. Then we'll click OK again in the Add Address Window.

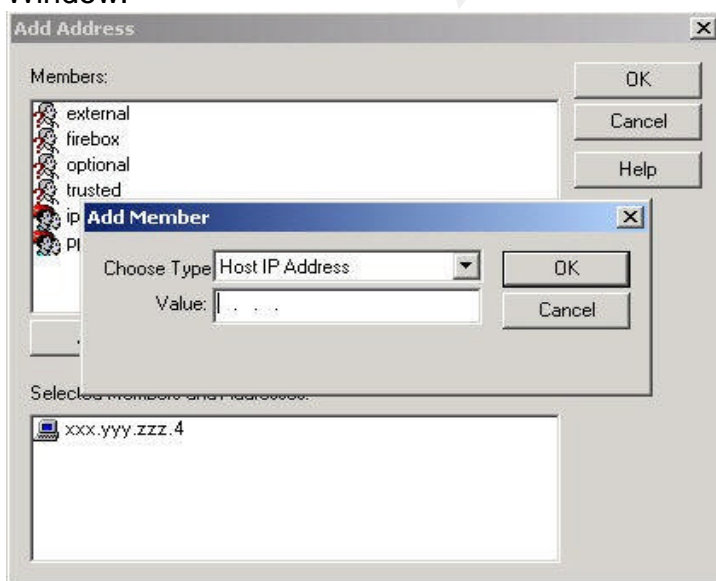


Figure 2.4.40

Our Incoming traffic configuration will look like this:

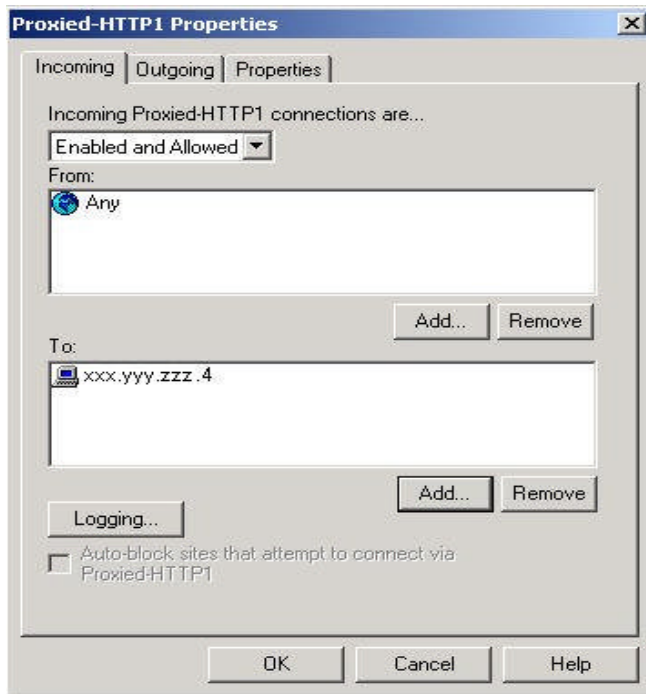


Figure 2.4.41

For Logging, we will leave the default settings, which will log only denied Incoming and Outgoing packets in our log data:

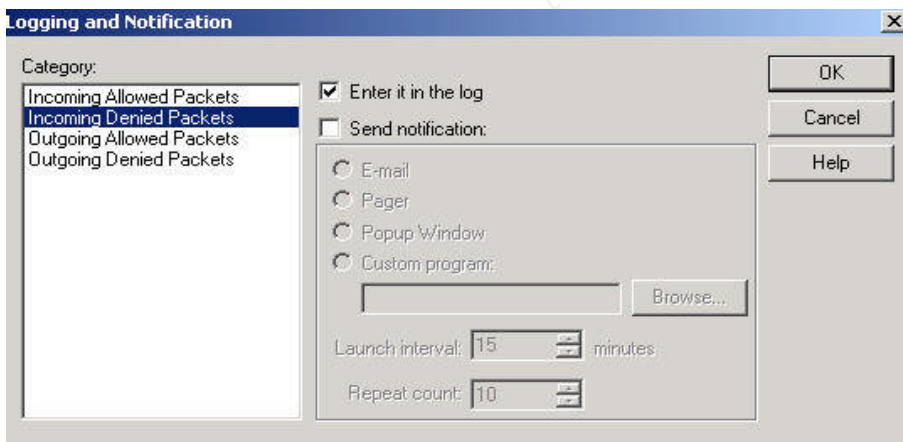


Figure 2.4.42

For the Outgoing traffic we will select Disabled. Originally, we have selected Enabled and Allowed From Trusted (Local) network to the Internet as well as to GIAC's external Web server. But since this HTTP Proxy service allows Outgoing HTTP traffic on ALL available TCP ports with no restrictions at all, this option did not comply with GIAC's security policy. To allow Outgoing HTTP traffic from Trusted (Local Network) to the Internet as well as to GIAC's external Web server only on port 80, we have selected another HTTP proxy from available proxies called HTTP.

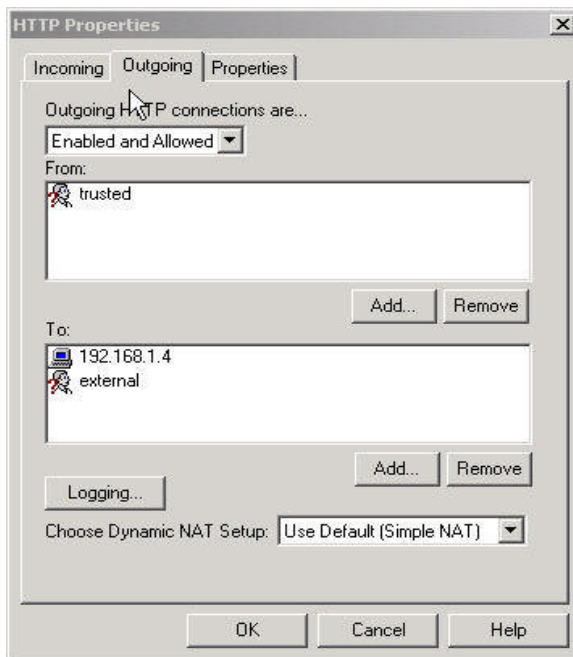


Figure 2.4.43

In the Properties Window, we'll be able to view our HTTP proxy service properties :

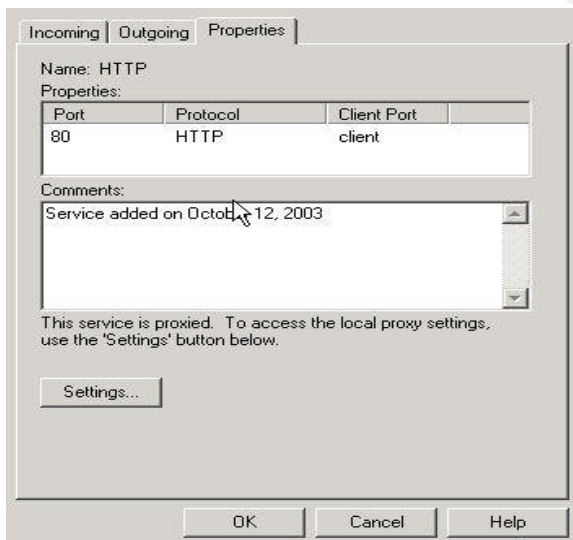


Figure 2.4.44

By clicking on the Settings button we'll be presented with HTTP proxy Settings:

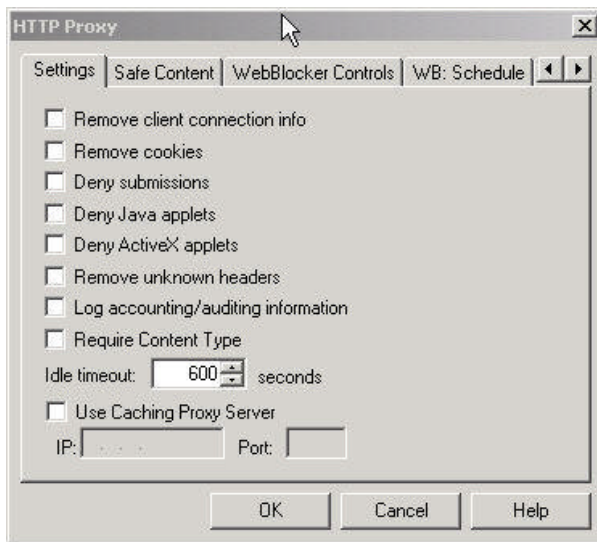


Figure 2.4.45

- Remove client connection info option will block sensitive client network information from leaking out to the Internet (e-mail address, operating system, browser type etc.). This information is sent out by default upon initial HTTP GET conversation
- Remove cookies option will prevent profiling of our systems Internet activity (spyware)
- Deny submissions option, when enabled, will deny filling in web pages (forms) by our internal users.
- Deny Java applets option will stop java applets from being executed while browsing the Internet. Also, as another security measure, this option will not allow HTTP downloads of ZIP files due to possibility of automatic execution of those files without proper virus / worm protection.
- Deny ActiveX applets option works using similar techniques as Deny Java applets
- The Remove unknown headers option will deny HTTP response headers from Web servers that are not defined in RFC 2616 (<http://www.ietf.org/rfc/rfc2616.txt?number=2616>). This is yet another HTTP proxy security measure preventing malformed HTTP responses from entering our network
- Log accounting/auditing information will add detailed accounting and auditing information to the log files. It will increase the amount of log data being stored in Firebox's Historical Reports module for detail auditing information
- Require content type option will require remote web servers to include MIME content type header in the HTTP message. If they don't, the pages won't be displayed
- Idle Time out option controls how long the Firebox HTTP proxy will wait for the Web client, after initiating the TCP connection, to request something from the outside Web server. It also controls how long the Firebox HTTP

- proxy will wait for the Web server to send the Web page that was requested. The default is 600 seconds (10 minutes).
- Use Caching Proxy Server option will enable the Firebox to forward HTTP requests to a caching proxy server (i.e. Squid or SUN ONE proxy servers) for faster internet browsing

Safe Content tab - Allow only safe content types:

In here we can specify what type of MIME content we are allowed to view. The below list of allowed MIME types is very restrictive. If we leave this option enabled, we will, most likely, need to add more permitted MIME types to allow for proper web access functionality.

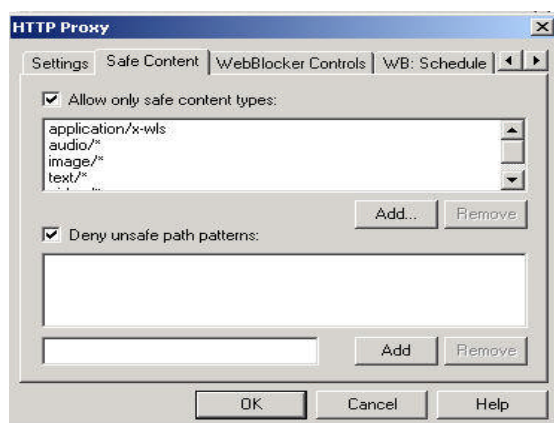


Figure 2.4.46

Web Blocker Tab Options - WebBlocker is WatchGuard's answer to filtering of objectionable Internet content. We will leave WebBlocker disabled.

Next Proxy filter we will configure will be **SMTP proxy**. SMTP proxy will inspect incoming and outgoing e-mail messages for harmful content. It will examine the SMTP headers, message recipients, message senders, message content and attachments and based on the configured criteria either deny or allow the e-mail message through. The criteria could be setup to strip certain SMTP headers, filter attachments by filename and content type, or deny e-mail messages based on their address pattern(s). The SMTP proxy service will be transparent to GIAC's internal users and mail servers.

To add SMTP Proxy service to our Policy, on our main Policy Editor menu, we will click on Edit -> Add Service -> Proxies -> SMTP -> Add -> Fill in proxy name or leave as default -> OK

In the Incoming Tab, from the drop down menu we'll select Enabled and Allowed. We will leave From Any as is. Incoming To we will change to our SMTP mail relay external IP address – xxx.yyy.zzz.3. The screen will look like this:

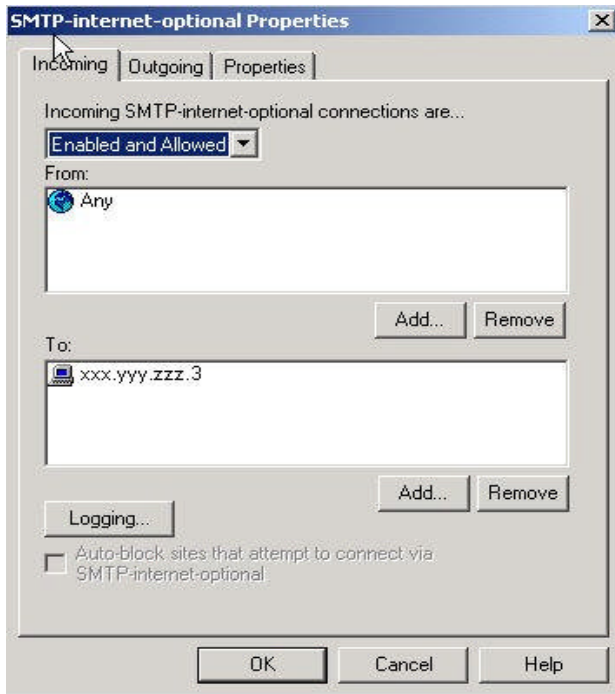


Figure 2.4.47

Outgoing SMTP proxy will be disabled (Outgoing ESMTP is not yet supported as of this writing). For Outgoing SMTP traffic we will use Filtered SMTP service from Packet Filters folder.

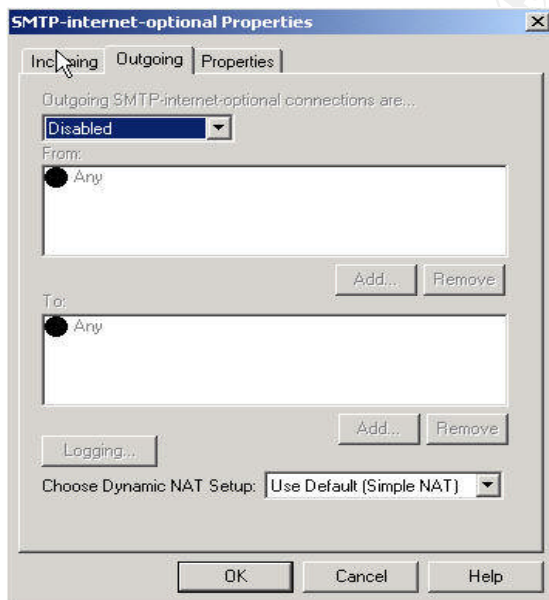


Figure 2.4.48

We will fine tune our Incoming SMTP connection by clicking on Properties Tab:

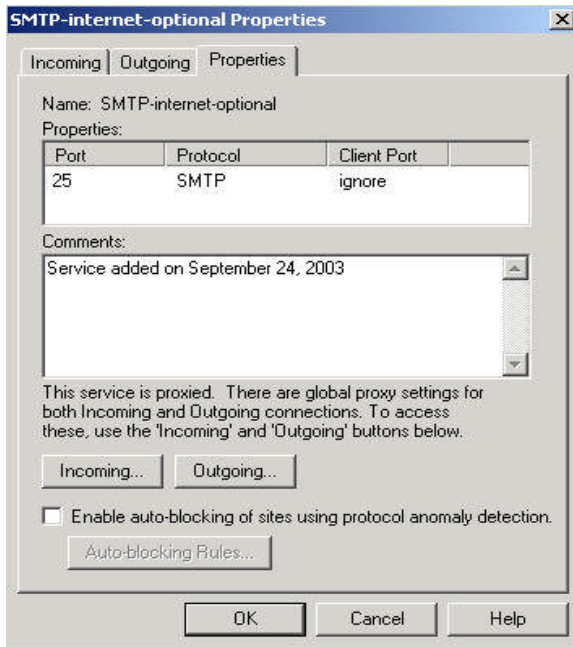


Figure 2.4.49

We will click on Incoming button to get into Incoming SMTP proxy settings:

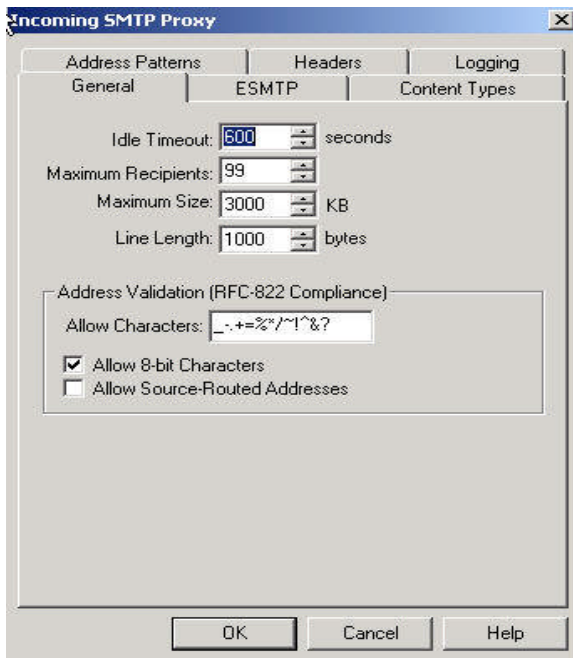


Figure 2.4.50

Idle Timeout

This option will allow us to configure the amount of time that the SMTP proxy will wait for the SMTP sender to send the mail before terminating the connection. By default, the SMTP proxy will wait for 600 seconds (10 minutes).

Maximum recipients

Using this option we can configure the maximum number of recipients per message. This parameter can be useful in limiting mass mailing of e-mail messages (spam). At this point, we will leave at 99 allowed recipients per message.

Maximum Size

Here we can configure the maximum message size (including any attachments). This can be anywhere between 0 and 50 megabytes, and is a good way of reducing the load on our mail server. We will leave it at 3MB's for now. Of course we can also control total mailbox sizes (quotas) internally, on our mail server.

Line Length

This option will allow us to limit the maximum line length in SMTP message.

For **Address Validation** rules, we have the following options:

Allow Characters

This option will add a capability to configure special characters allowed in the email addresses in the MAIL FROM and RCPT TO fields, besides letters and numbers. The default settings are the characters suggested by RFC 822 (<http://www.ietf.org/rfc/rfc0822.txt?number=822>)

Allow 8-bit characters

This option will allow 8-bit ASCII characters, which means all special characters will be sent without being MIME encoded. Most mail servers will only allow 7-bit, MIME encoded characters through, so if we leave this option enabled, we should closely monitor our SMTP traffic for dropped messages and based on our findings decide if this option should be left enabled or if we should disable it.

Allow Source Routed Addresses

This option will allow us to reject mail sent to us, which has a %(percent) sign in the MAIL FROM: field. The % sign in the e-mail address indicates a source-routed address. A source-routed address is an email address, which relays itself through another host. By default, this setting is disabled.

Next Menu Tab is **ESMTP**

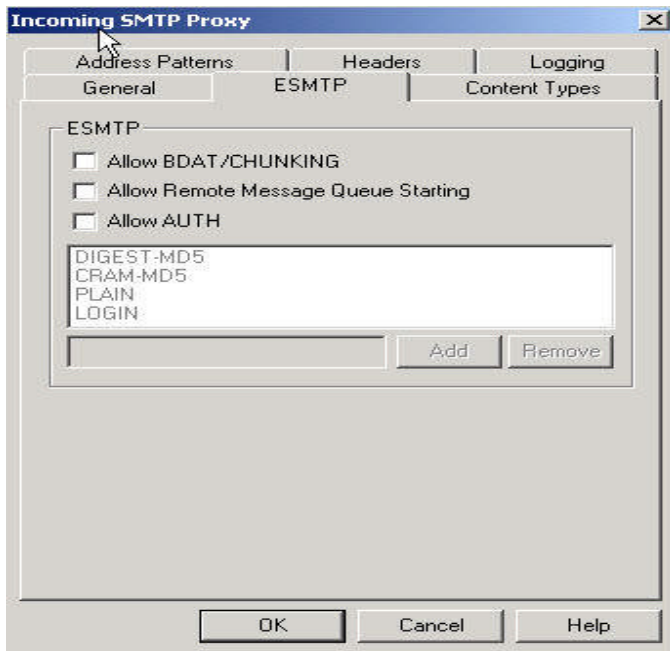


Figure 2.4.51

In here we can specify AUTH authentication types, which specify various ways of authenticating to SMTP server. We can also enable support for ESMTP extensions (keywords). These settings will allow us to fine tune how our SMTP mail relay server will communicate with other SMTP servers. We will leave the options disabled for now. By monitoring Firebox's logs we will be able to see how smoothly our SMTP traffic is flowing and adjust the above settings should there be a problem.

Next tab is **Content Types**

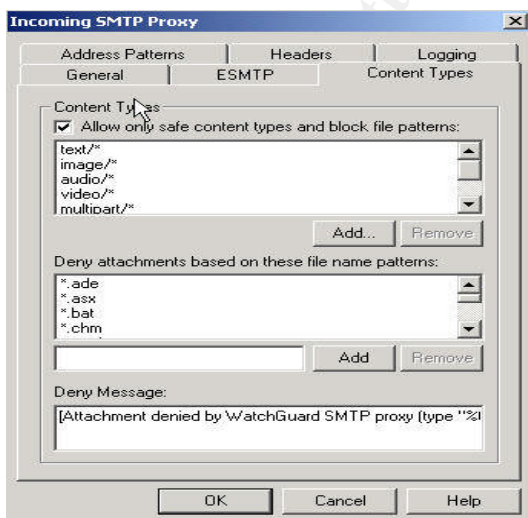


Figure 2.4.52

This option allows us to specify what MIME content types we will allow through our SMTP proxy service. By reading the MIME headers contained in an incoming email message, the Firebox can admit only the types listed and disallow all others. If we leave this option enabled, we will need to monitor the Firewall logs to determine if the SMTP proxy service isn't stripping valid e-mail messages due to MIME type(s) it simply doesn't know about yet. Should this be the case, we will need to add new MIME types to this list.

Next tab is **Address Patterns**

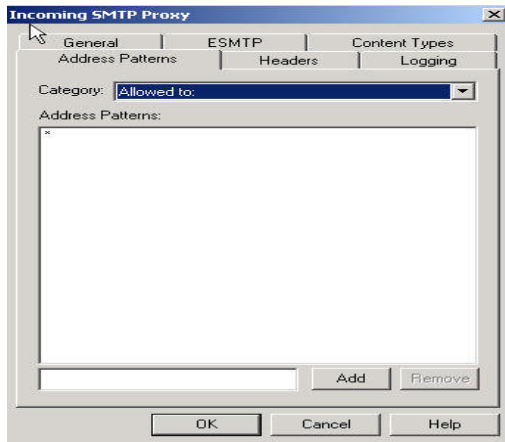


Figure 2.4.53

The Firebox is capable of limited, relay protection in the form of receiving address filtration. The SMTP proxy will allow us to configure incoming wildcard-based address patterns that are allowed or denied.

Along with the relay protection, we can configure the SMTP proxy to allow and deny message recipients and senders. (i.e. if we do not wish to receive messages from anyone at hostiledomain.com, we could put this in the Denied from: category "*hostiledomain.com", and all mail from that domain would be denied). Based on our domain name (i.e. giacent.com) in Category -> Allowed to option we can specify *giacent.com and e-mails addressed only to our domain name will be allowed. The SMTP proxy will check the RCPT TO: line in the SMTP conversation to determine the message recipient and apply the Allowed To policy to allow or deny the message.

Next option is **Headers**

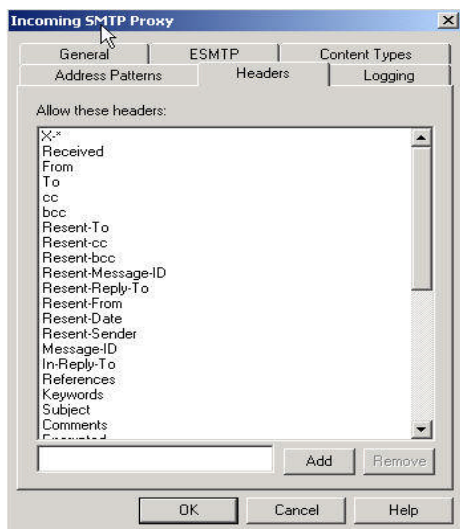


Figure 2.4.54

The Firebox will analyze incoming messages' SMTP headers and won't allow any of them through to GIAC's external mail server that it does not recognize. The Firebox also strictly enforces the RFC 821 1000 byte line-length limits (<http://www.ietf.org/rfc/rfc0821.txt?number=821>) thus preventing any possible hostile buffer overflow exploits. The SMTP headers that are allowed are user-configurable.

Next and last option in our Incoming SMTP proxy menu is **Logging**

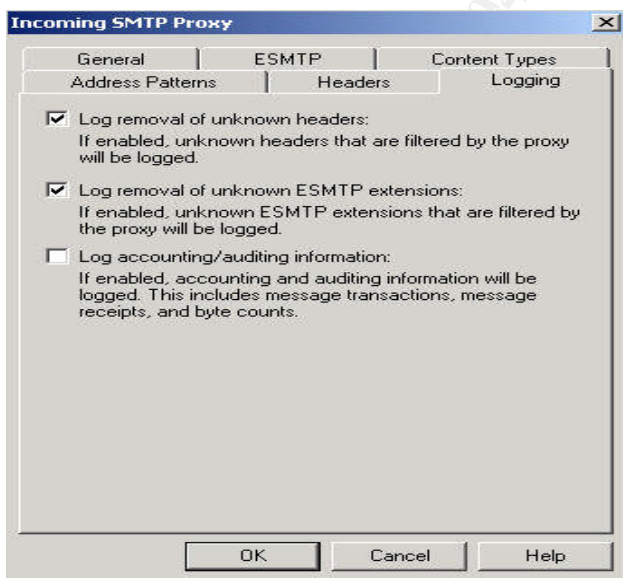


Figure 2.4.55

By enabling the first 2 logging options we will be able to monitor our SMTP traffic in our Firebox's log data. This will allow us to make adjustments to our SMTP proxy settings should there be any problems with receiving external e-mails (i.e. unknown headers etc.).

Since we left our Outgoing SMTP proxy service disabled we will leave Outgoing SMTP proxy options alone.

Mail server profiling protection

This option will allow us to limit our SMTP server version exposure. The less information our SMTP system reveals about itself, the smaller the chance of an attacker being able to quickly determine its vulnerabilities.

Without the SMTP proxy:

220 www.mydomain.com ESMTP Sendmail 8.11.0/8.11.0; Tue, 29 May 2001 18:59:02 -0700

And with the SMTP proxy:

220 SMTP service ready

In the first server greeting, the mail server identified the version, the system time, the local hostname, and the time zone. This type of information could be useful to a potential attacker. In the second greeting, all of that information was filtered out by the SMTP proxy on the Firebox, eliminating the extra information. The Firebox also adds a few seconds delay into the response, making response-time profiling impossible. These two things can prevent most types of automated server profiling attempts, because the only important information that the SMTP server sends out is the status numbers, for example, 220 for ready, 550 for user OK.

Next Proxy Service we will add to our Firewall Policy is **FTP**. The steps to add the service are the same as in 2 previous proxy services. We will Allow and Deny Incoming FTP service to be able to log attempted FTP requests coming into our network..

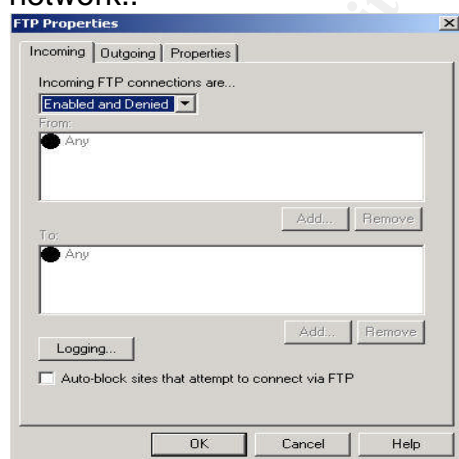


Figure 2.4.56

We will Enable and Allow Outgoing FTP from our Trusted (Local) network to Any.

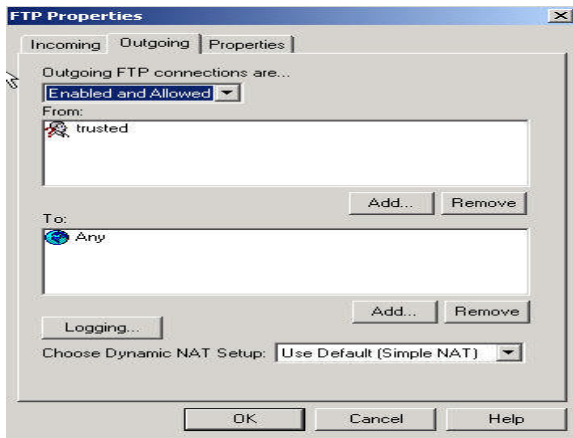


Figure 2.4.57

In Properties Tab, we will be able to adjust our incoming and outgoing FTP behavior

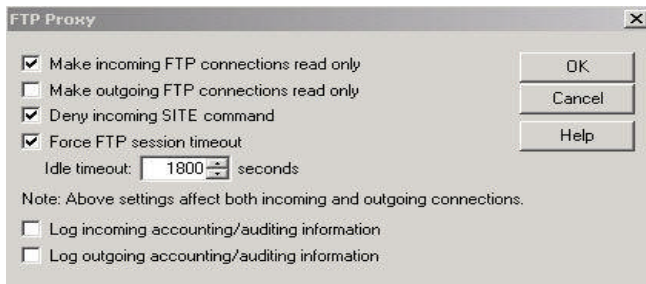


Figure 2.4.58

As we are not allowing incoming FTP connections, we will leave Make incoming FTP connections read only option enabled. We will leave the other FTP proxy settings as they are.

Last proxy service we have decided to enable is DNS. The DNS Proxy will validate all DNS traffic and will block any DNS packets that are illegally formed or that don't match a basic list of allowable transactions.

To add this proxy service we will follow the same steps as in prior examples. We will Enable and Allow Incoming from Any to our external DNS server – xxx.yyy.zzz.5

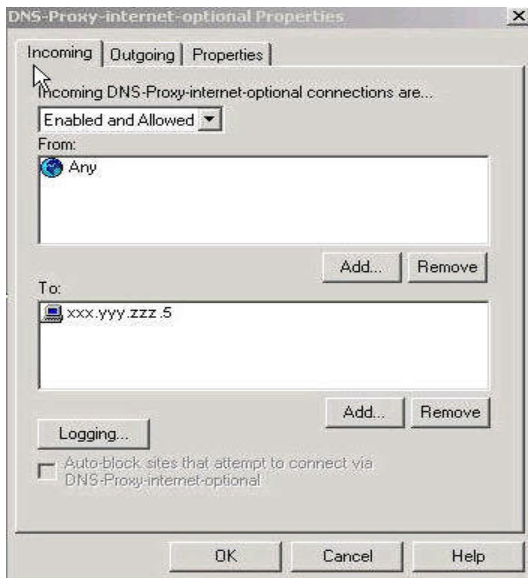


Figure 2.4.59

The Outgoing DNS proxy will be Disabled. We will use DNS service from Packet filters list for Outgoing DNS (as recommended by Watchguard).

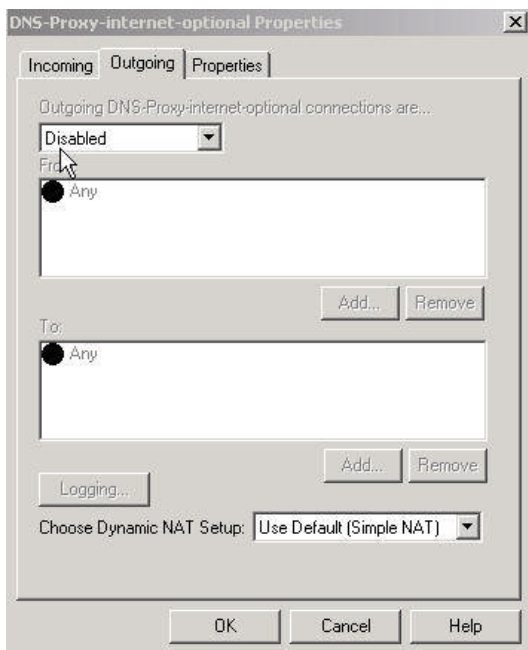


Figure 2.4.60

In Properties Tab, we'll confirm our DNS proxy service settings.

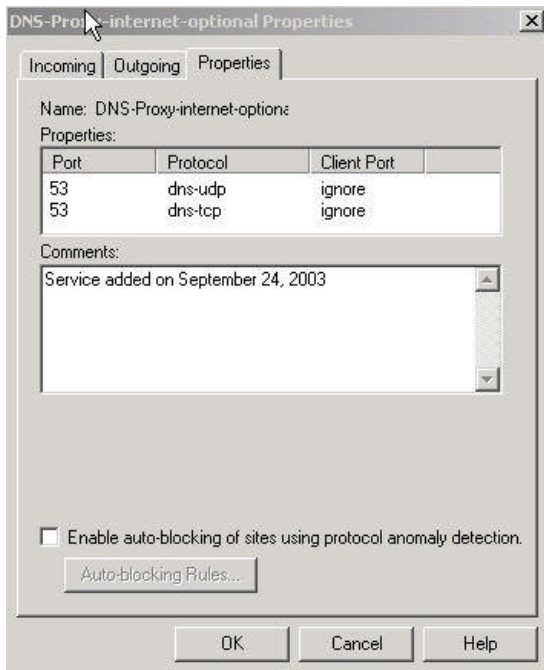


Figure 2.4.61

We have added 4 custom filter services to our Firebox to accommodate our network access requirements : LDAPS (secure LDAP), wwwrevproxy4000 (secure reverse proxy on port 4000), wwwrevproxy4001 (secure reverse proxy on port 4001) and HTTPS-9000 (secure access to Lotus / Domino web server). To add a custom service, from the main menu we need to click on Edit -> Add Service -> New -> Name of service

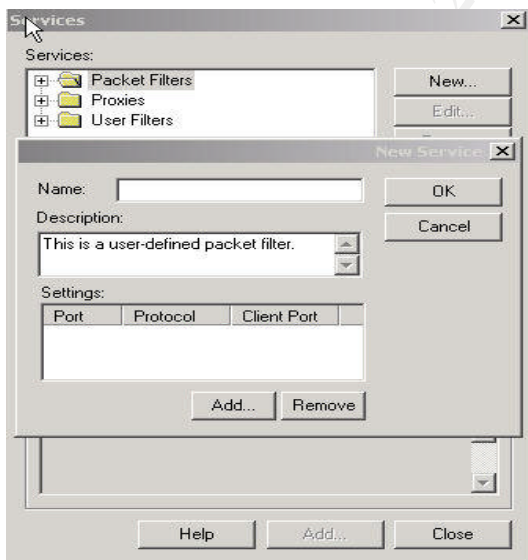


Figure 2.4.62

After defining new name for our custom service, we will click on Add

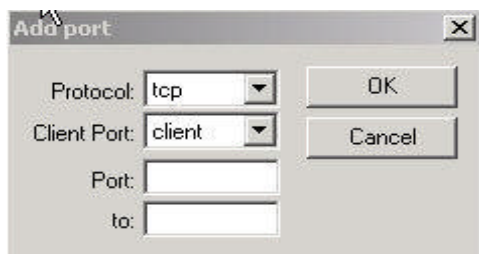


Figure 2.4.63

In here we specify Protocol, Client Port, Port or Port range

In Protocol drop down menu box we have 4 options :

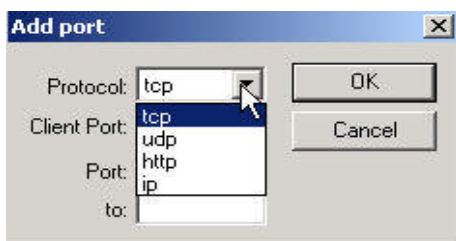


Figure 2.4.64

Generally, this will be TCP or UDP. IP refers to IP Protocol numbers. HTTP means that this is a custom service that will use the Firebox's HTTP-Proxy on the port we choose.

For all of our custom services we will choose TCP.

In Client Port drop down menu box we have the following options :

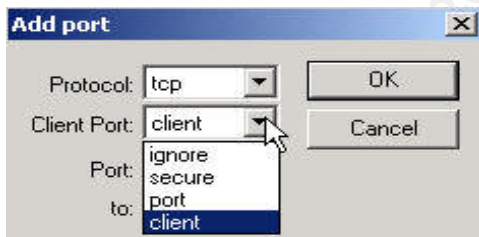


Figure 2.4.65

Client - Source port must be >1023.

Port - Source port must be equal to the destination port.

Secure - Source port must be < 1024.

Ignore - Source port doesn't matter.

For all of our custom services we will pick client.

We will specify single port for the 4 services we will define:

LDAPS – 636

HTTPS-9000 - 9000

wwwrevproxy4000 – 4000

wwwrevproxy4001 – 4001

Upon completion, all of our new custom services will be listed in User Filters folder.

To add the new custom service to our Firewall policy we'll follow the same steps as we did while adding proxy services.

3. Assignment 3 – Verify the Firewall Policy

Planning the validation of Firewall Policy

To verify that GIAC Firewall policy has been implemented properly, we will need to validate all of its configured rules. This is a very important step in Firewall implementation. It will allow us to compare the firewall audit results with expectations set in our overall network design. This way we will be able to address any discrepancies between the two.

3.1 Technical approach to our firewall assessment

We will use Lance Spitzner's "Auditing Your Firewall Setup – <http://www.spitzner.net/audit.net> as a reference document in performing our firewall assessment. Lance recommends dividing the firewall audit into 2 parts :

- testing the firewall itself
- testing the rule base

3.1.1 Firewall Test

The firewall test will ensure that no one from the outside or the inside can modify or access our firewall except for authorized personnel. This includes physical access to our firewall device as well as firewall administration and monitoring software access.

The physical location of our firewall device will be in a lock controlled room with only authorized, network administrators' access. This will be monitored, by enforcing all technical staff sign-in and sign-out in GIAC's log book before entering and after leaving the room. For software access we will have to make sure that the operating system our firewall runs on is secure. Since we are using a firewall appliance, we have put our trust in the manufacture's ability to harden the operating system. In Firebox's case, the OS is based on Linux kernel. The only processes running are the ones required for the firewall to function. Also, we will need to perform a port scan of our firewall from the Internet, Trusted and Optional networks. This will help us to identify any open ICMP, UDP and TCP ports on our firewall.

3.1.2 Firewall Rule Base Test

Firewall rule base test will ensure that the firewall is enforcing GIAC security policy for accessing company's networks. For this test, Lance Spitzner recommends scanning every network segment from every other network segment defined in our firewall configuration policy. Basically, we will need to place a scanning host on one side of the firewall to scan systems on the other 2 sides of the firewall. We will rotate the scanning host through all of our network segments to exhaust all possibilities. This will determine what packets can and cannot get through. To audit our rule base we will perform icmp (ping), udp and tcp scans using nmap and tcpdump utilities. Nmap will be used to scan the ports and tcpdump will confirm which packets came through. We will also use netcat utility to simulate services on scanned hosts.

The following is a list of firewall and rulebase scans performed from all three of our network segments :

3.1.2.1 Scanning from the Internet.

We will place our scanning host in place of our external, border router. We will use the external router's internal IP address for our scanning host.

1. Scan the external interface of the firewall
 - verify any open ports
 - verify if icmp echo requests (ping) were successful
2. Scan Optional(DMZ) network
 - verify open ports on external SMTP server. The only open port should be TCP:25
 - verify open ports on the external Web server (there should only be HTTP/HTTPS ports open 80 and 443 respectively)
 - verify open ports on external DNS server (the only ports open should be TCP/UDP 53)
 - verify open ports on secure reverse proxy server. The only ports open should be TCP:4000 and TCP:4001
 - verify open ports on ssh server. The only open port should be TCP:22
 - verify open ports on NTP, Backup / Virus scanning and IDS servers. Nmap should not be able to scan these servers. Their addresses are not accessible from the Internet.
3. Scan Trusted network
 - verify open ports on Certificate/LDAP, IDS, Lotus Notes/Domino, Virus Scanner, Internal SMTP, Internal DNS and file/printsharing, Central Syslog and local NTP servers, Firebox management and internal host workstations. Nmap scan should not be able to access servers on Trusted (Internal) network. They are all using private IP addresses (192.168.100.x/24) and are not accessible from the Internet.

3.1.2.2 Scanning from the Optional (DMZ) network

We will place our scanning host inside of our DMZ network.

1. Scan the Optional Interface of the firewall

- verify any open ports
- verify if icmp echo requests (ping) were successful (they should fail)

To properly scan access from our Optional(DMZ) network we will replace each of the servers with our scanning host and verify network access from each of them. This will simulate a situation when one of our DMZ servers has been compromised by an outside attacker.

2. Replace the external SMTP relay server with the scanning host

- verify it can access our internal SMTP server only on port 25. Access to any other port or server on the Trusted network should not be allowed
- verify it can send outgoing SMTP traffic on port 25 to the Internet. No other traffic should be allowed

3. Replace the external Web server with the scanning host

- verify it can only access our internal LDAP server
- verify it can not access any other host on the Trusted network or the Internet

4. Replace the External DNS server with our scanning host

- verify it can only access the Internet on ports TCP/UDP 53. All other Internet traffic should be disallowed
- verify it can not access any host on the Trusted network

5. Replace the Secure Reverse Proxy Server with our scanning host

- verify it can only access our Internal Lotus Notes / Domino database server
- verify it cannot access any other host on the Trusted Network or the Internet

6. Replace the SSH2 server with our scanning host

- verify it can not access any host on the Trusted Network or the Internet

7. Replace the External NTP server with our scanning host

- verify it can only access specified stratum servers on the Internet on port TCP/UDP 123. All other Internet traffic should be disallowed
- verify it can not access any host on the Trusted Network

8. Replace the External Backup and Virus Scanning server with our scanning host

- verify it can access the Internet on port 80 (HTTP). This is required to perform virus definition updates

9. Replace the External IDS server with our scanning host

- verify it cannot access any host on the Trusted Network or the Internet

10. Verify all servers on Optional (DMZ) network can send syslog data to server located on Trusted(Internal) network

3.1.2.3 Scanning from the Trusted (Internal) network

We will place our scanning host inside our Trusted(Internal) network. We will replace all servers (one by one) on Trusted(Internal) network with the scanning host.

1. Scan the Trusted(Internal) IP address of the firewall
 - verify any open ports
2. Verify the only traffic let through to the Internet from any internal host is : HTTP, HTTPS, and FTP.
3. Verify that access to the Secure Reverse Proxy server on ports 4000 and 4001 is allowed from any host on the Trusted network
4. Verify ssh access from any host on the Trusted network to SSH2 server is allowed
5. Verify Internal PC used for Watchguard firewall management can access the firewall for maintenance and monitoring purposes
6. Verify internal SMTP server can access external SMTP mail relay server
7. Verify internal DNS server can access external DNS server
8. Verify internal NTP server can access external NTP server for time synchronization purpose
9. Verify internal hosts can ping the firewall, DMZ and the Internet (for troubleshooting purposes)

3.1.3 Audit date consideration

To minimize impact on GIAC network resources and allow for network servers downtime, we will perform our Firewall audit during 2 weekends period. We will ask our management staff for written authorization to give us 3 day window to perform the Firewall audit : from Friday 6:00pm to Monday 6:00am. This should give us enough time to address any problems caused by the scan (server reboots, network downtime, firewall policy adjustments etc.) before the work week begins. We will also inform our partners and suppliers of the audit schedules to allow them to plan for it. GIAC's main web site will be updated accordingly with Downtime messages so GIAC's customers are aware of the outage.

3.1.4 Estimate costs and level of effort

We have given ourselves 2 weekend time frame to prepare for and test our firewall policy.

The first weekend period designated for the audit of our firewall will be spent on planning and preparing for the actual verification of GIAC's firewall policy. Good preparation is the key in this case. Second weekend will be used to run all the tests against the firewall. Upon completion of the audit the results will be evaluated and appropriate steps will be taken to address any possible problems.

The estimated time for planning and preparation to perform the test : 24hrs

As for the actual audit, Lance Spitzner's in his "Auditing the firewall" document estimates that each scan should take between 30-60 minutes. This will of course depend on network performance, firewall and scanned systems behavior as well as types of network scan tools used. We will estimate each scan to take approx. 30min.

We will perform the following scans :

- 4 scans to the Firewall (1 from the Internet, 1 from the DMZ and 2 from the internal systems – 1 from Watchguard's admin workstation and 1 from any of the other internal hosts). Total time – 2hrs.
- 5 scans from the Internet to DMZ servers. Total time 2.5hrs.
- 8 scans from DMZ to the Internet. Total time 4 hrs.
- 11 scans from DMZ to Local hosts (full set of scans from 1 server, unique scan from all of the other servers). Total time 5.5hrs
- 1 scan from Local to the Internet. Total time .5hrs
- 12 scans from Local to DMZ (full set of scans from 1 servers, 4 unique scans from all of the other servers). Total time 6 hrs

The estimated time to perform the above scan is : 21 hrs (rounding up).

We will also need to take under consideration possible system crashes, shutdowns and network performance degradation. The estimated time to deal with and address those issues : 6hrs.

The total estimated time to perform GIAC's firewall audit is : 27hrs.

GIAC will assign 2 of its system administrators to perform the audit.

They will be paid overtime rate of 1.5 times of their regular pay.

Their regular hourly rate is \$45.

3.1.5 Risks associated with performing the firewall audit

As with any major firewall audit main risks associated with it are :

- causing scanned system to crash. In best case, this will only require a reboot. In other cases we can discover that certain components of the systems may need patching up and / or upgrading to bring them back up
- raising red flags in our log systems due to volume of incoming data

3.2 Validation of Firewall Policy

3.2.1 Audit of the Firewall

We will utilize the following network tools : nmap and ping.

The audit of the firewall will consist of 3 scans :

- ping and nmap scan from the Internet

- ping and nmap scan from Optional (DMZ) network
- ping and nmap scan from Trusted (Internal) network

For the scan from the Internet we will replace our border router with the scanning host.

For the scan from the Optional (DMZ) network we will replace one of our DMZ servers with the scanning host.

For the scan from the Trusted (Internal) network we will replace one of the internal servers with the scanning host.

The following nmap command will be used :

- for TCP scan - `nmap -v -sS -sR -P0 -O -n -p1-65535 "firewall external IP address"`
- for UDP scan - `nmap -v -sU -sR -P0 -O -n -p1-65535 "firewall external IP address"`

Description of the nmap options used :

- v – verbose
- sS – SYN stealth scan
- sU – UDP scan
- sR – RPC scan
- P0 – don't ping the scanned host
- O – attempt to determine Operating System firewall is running on
- n – don't resolve IP address to host name
- p1-65535 – scan for all ports

Note: Most of the nmap scans show all closed ports as filtered. This is due to most of the rules dropping the packets instead of rejecting them – no RST (Disabled vs. Enabled and Denied in Watchguard's case).

1. Output of firewall TCP scan from the Internet :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -O -P0 -p1-65535 -n xxx.yyy.zzz.2
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 12:57 Eastern
Daylight Time
Host xxx.yyy.zzz.2 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.2 at 12:57
Adding open port 4110/tcp
Adding open port 4100/tcp
Adding open port 4113/tcp
Adding open port 4112/tcp
The SYN Stealth Scan took 248 seconds to scan 65535 ports.
Initiating RPCGrind Scan against xxx.yyy.zzz.2 at 13:01
The RPCGrind Scan took 3 seconds to scan 4 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
For OSScan assuming that port 4100 is open and port 33748 is closed and neither are firewalled
For OSScan assuming that port 4100 is open and port 40991 is closed and neither are firewalled
For OSScan assuming that port 4100 is open and port 33189 is closed and neither are firewalled
Interesting ports on xxx.yyy.zzz.2:
(The 65531 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
4100/tcp  open  unknown
4110/tcp  open  unknown
4112/tcp  open  unknown
4113/tcp  open  unknown
Device type: general purpose router
Running (JUST GUESSING) : Linux 2.0.X (95%), IBM embedded (85%)
Aggressive OS guesses: Linux 2.0.32-34 (95%), Linux 2.0.34-38 (90%), IBM 2210 Router MRS 2.x on Token Ring interface (85%), Linux 2.0.27 - 2.0.30 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Class=truly random
                        Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 268.577 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.1.1

The SYN stealth scan shows 4 open ports on our firewall :

- 4100 is used for Firebox Authorization service
- 4110 is used by Watchguard's Dynamic VPN Configuration protocol.
Since we have decided to use certificate for validation our VPN users we had to enable DVCP server. There was a problem with having this port opened in Firebox firmware 5.x.x. An attacker could crash DVCP service by using anywhere between 1 and 400 packets of tab characters, followed by CRLF. After the attack, the firewall needed a reboot for the DVCP service to work again. This problem was addressed in Firebox firmware v.6.0.b1140. Since we are using the newest firmware – 7.x.x. this problem should not affect us
- 4112 and 4113 are used by Watchguard's Certificate Authority. The service – wg_ca has been created automatically after enabling DVCP server. Watchguard recommends leaving it unchanged.

2. Output of firewall UDP scan from the Internet :

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -O -P0 -pi-65535 -n xxx.yyy.zzz.2
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 13:05 Eastern
Daylight Time
Host xxx.yyy.zzz.2 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.2 at 13:05
The UDP Scan took 180 seconds to scan 65535 ports.
Adding open port 514/udp
Adding open port 4500/udp
Adding open port 500/udp
Initiating RPCGrind Scan against xxx.yyy.zzz.2 at 13:08
The RPCGrind Scan took 3 seconds to scan 3 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
Interesting ports on xxx.yyy.zzz.2:
(The 65532 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
500/udp   open  isakmp
514/udp   open  syslog
4500/udp  open  sae-urn
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
$Info(U=3.45%P=i686-pc-windows-windows%D=10/12%Time=3F898A96%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=Y%DF=N%TOS=0%IPLen=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 197.244 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.1.2

The UDP scan of our Firebox shows 3 ports open :

- 500 is used by IPSec negotiations
- 514 is used by syslog service. Since we have replaced our border router with the scanning host, this port shows up in the scan as open. We are allowing syslog data to go from our router through the firewall to our local syslog server. Port forwarding on the firewall has been implemented to allow this connection. Scanning from any other external host would not show this port as opened.
- 4500 is used by NAT – T (NAT traversal). This is used for IPSec connections. It has been added to version 7 of the Firebox software.

3. Output of ping command to the firewall from the Internet :

```
C:\nmap\nmap-3.45>PING xxx.yyy.zzz.2
Pinging xxx.yyy.zzz.2 with 32 bytes of data:

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

Ping statistics for xxx.yyy.zzz.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\nmap\nmap-3.45>
```

Figure 3.2.1.3

As expected, pinging the firewall did not work.

4. Output of firewall TCP scan from Optional (DMZ) network :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -O -p1-65535 -n 192.168.1.1

Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-12 13:16 Eastern
Daylight Time
Host 192.168.1.1 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.1.1 at 13:16
Adding open port 4113/tcp
Adding open port 4100/tcp
Adding open port 4112/tcp
The SYN Stealth Scan took 206 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.1.1 at 13:19
The RPCGrind Scan took 3 seconds to scan 3 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
For OSScan assuming that port 4100 is open and port 30220 is closed and neither are firewalled
For OSScan assuming that port 4100 is open and port 35837 is closed and neither are firewalled
For OSScan assuming that port 4100 is open and port 30756 is closed and neither are firewalled
Interesting ports on 192.168.1.1:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
4100/tcp  open  unknown
4112/tcp  open  unknown
4113/tcp  open  unknown
Device type: general purpose router
Running (JUST GUESSING) : Linux 2.0.X (95%), IBM embedded (85%)
Aggressive OS guesses: Linux 2.0.32-34 (95%), Linux 2.0.34-38 (90%), IBM 2210 Router MRS 2.x on Token Ring interface (85%), Linux 2.0.27 - 2.0.30 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Class=truly random
                        Difficulty=99999999 <Good luck!>
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address <1 host up> scanned in 225.518 seconds
```

Figure 3.2.1.4

5. Output of firewall UDP scan from Optional (DMZ) network :

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -O -p1-65535 -n 192.168.1.1

Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-12 14:02 Eastern
Daylight Time
Host 192.168.1.1 appears to be up ... good.
Initiating UDP Scan against 192.168.1.1 at 14:02
The UDP Scan took 56 seconds to scan 65535 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on 192.168.1.1 are: closed
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo<U=3.45%P=i686-pc-windows-windows%D=10/12%Time=3F899768%O=-1%C=-1>
T5<Resp=N>
T6<Resp=N>
T7<Resp=N>
PU<Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E>

Nmap run completed -- 1 IP address <1 host up> scanned in 73.480 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.1.5

6. Output of ping command to the firewall form host on Optional(DMZ) network :

```
C:\nmap\nmap-3.45>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\nmap\nmap-3.45>
```

Figure 3.2.1.6

As expected, pinging the firewall didn't work.

7. Output of firewall TCP scan from Trusted (Internal) network :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -O -n -p1-65535 192.168.100.1
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 15:02 Eastern
Daylight Time
Host 192.168.100.1 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.1 at 15:02
Adding open port 4100/tcp
Adding open port 4112/tcp
Adding open port 4113/tcp
The SYN Stealth Scan took 259 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.100.1 at 15:06
The RPCGrind Scan took 2 seconds to scan 3 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
For OSScan assuming that port 4100 is open and port 34498 is closed and neither are firewalled
For OSScan assuming that port 4100 is open and port 39503 is closed and neither are firewalled
For OSScan assuming that port 4100 is open and port 30902 is closed and neither are firewalled
Interesting ports on 192.168.100.1:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
4100/tcp  open  unknown
4112/tcp  open  unknown
4113/tcp  open  unknown
Device type: general purpose router
Running (JUST GUESSING): Linux 2.0.X (95%), IBM embedded (85%)
Aggressive OS guesses: Linux 2.0.32-34 (95%), Linux 2.0.34-38 (90%), IBM 2210 Router MRS 2.x on Token Ring interface (85%), Linux 2.0.27 - 2.0.30 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Class=truly random
                        Difficulty=99999999 <Good luck!>
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 278.049 seconds

C:\nmap\nmap-3.45>
```

Figure 3.2.1.7

8. Output of firewall UDP scan from Trusted(Internal) network :

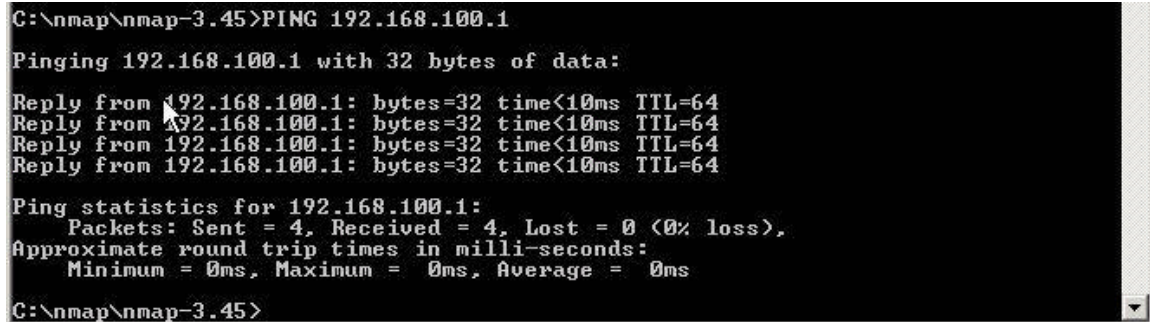
```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -O -n -p1-65535 192.168.100.1
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 15:07 Eastern
Daylight Time
Host 192.168.100.1 appears to be up ... good.
Initiating UDP Scan against 192.168.100.1 at 15:07
The UDP Scan took 93 seconds to scan 65535 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 65535 scanned ports on 192.168.100.1 are: closed
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(U=3.45%P=1686-pc-windows-windows%D=10/12%Time=3F89A6D8%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 107.813 seconds

C:\nmap\nmap-3.45>
```

Figure 3.2.1.8

9. Output of ping command from internal host to firewall :



```
C:\nmap\nmap-3.45>PING 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time<10ms TTL=64
Reply from 192.168.100.1: bytes=32 time<10ms TTL=64
Reply from 192.168.100.1: bytes=32 time<10ms TTL=64
Reply from 192.168.100.1: bytes=32 time<10ms TTL=64

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\nmap\nmap-3.45>
```

Figure 3.2.1.9

We are allowing all of our internal hosts to ping the firewall and the Internet for testing purposes.

3.2.2 Audit of the Firewall Rulebase

Next step in our audit will be to test our **Firewall's Rulebase**. This will ensure that only expected traffic is let through the firewall and the rest is either denied or dropped.

As described earlier, we will perform the scan from every network segment. We will use nmap, netcat, windump and ping utilities.

netcat will allow us to listen on specific TCP and UDP ports to simulate network services.

windump will confirm that the packet actually made it through.

The following nmap and netcat commands will be used :

For nmap SYN TCP scan :

nmap -v -sS -sR -P0 -n -p1-65535 "ip address of scanned host"

For nmap UDP scan :

nmap -v -sU -sR -P0 -n -p1-65535 "ip address of scanned host"

For netcat to listen on specific port :

nc -v -l -p"service port number" (i.e. nc -v -l -p80 will listen on port 80)

-v – verbose

-l – listen on any port (UDP, TCP)

-p – port number

First we will test access to our Optional (DMZ) servers from the internet :

1. Output of external SMTP server TCP scan from the Internet :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -p1-65535 xxx.yyy.zzz.3
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-11 12:46 Eastern
Daylight Time
Host xxx.yyy.zzz.3 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.3 at 12:46
Adding open port 25/tcp
The SYN Stealth Scan took 246 seconds to scan 65535 ports.
Initiating RPCGrind Scan against xxx.yyy.zzz.3 at 12:50
The RPCGrind Scan took 1 second to scan 1 ports.
Interesting ports on xxx.yyy.zzz.3:
<The 65534 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
25/tcp    open  smtp
Nmap run completed -- 1 IP address (1 host up) scanned in 251.572 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.1

As expected, only SMTP port 25 is open.

2. Output of external SMTP server UDP scan from the Internet :

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -p1-65535 xxx.yyy.zzz.3
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-11 12:53 Eastern
Daylight Time
Host xxx.yyy.zzz.3 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.3 at 12:53
The UDP Scan took 65 seconds to scan 65535 ports.
All 65535 scanned ports on xxx.yyy.zzz.3 are: closed
Nmap run completed -- 1 IP address (1 host up) scanned in 70.481 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.2

3. Output of external Web server TCP scan from the internet :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -p1-65535 xxx.yyy.zzz.4
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-11 12:56 Eastern
Daylight Time
Host xxx.yyy.zzz.4 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.4 at 12:56
Adding open port 443/tcp
Adding open port 80/tcp
The SYN Stealth Scan took 243 seconds to scan 65535 ports.
Initiating RPCGrind Scan against xxx.yyy.zzz.4 at 13:00
The RPCGrind Scan took 3 seconds to scan 2 ports.
Interesting ports on xxx.yyy.zzz.4:
<The 65533 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
80/tcp    open  http
443/tcp   open  https
Nmap run completed -- 1 IP address (1 host up) scanned in 251.151 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.3

As expected, only HTTP port 80 and HTTPS port 443 access is allowed from the internet to our external Web server.

4. Output of external Web server UDP scan from the internet :

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -p1-65535 xxx.yyy.zzz.4
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-11 13:28 Eastern
Daylight Time
Host xxx.yyy.zzz.4 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.4 at 13:28
The UDP Scan took 66 seconds to scan 65535 ports.
All 65535 scanned ports on xxx.yyy.zzz.4 are: closed
Nmap run completed -- 1 IP address (1 host up) scanned in 70.842 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.4

As expected, no UDP ports are opened on the external Web server.

The following is tcpdump output while scanning our external Web server. It shows that both HTTP and HTTPS packets made it through the firewall :

```
13:33:27.490950 IP xxx.yyy.zzz.1.57796 > pc2.80: S 1132282420:1132282420(0) win 1024
13:33:27.491098 IP pc2.80 > xxx.yyy.zzz.1.57796: S 709857670:709857670(0) ack 1132282421 win 16616 <mss 1460> (DF)
13:33:27.492504 IP xxx.yyy.zzz.1.57796 > pc2.80: R 1132282421:1132282421(0) win 0
13:34:24.358112 IP xxx.yyy.zzz.1.1048 > pc2.80: S 3573296091:3573296091(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
13:34:24.358257 IP pc2.80 > xxx.yyy.zzz.1.1048: S 724092764:724092764(0) ack 3573296092 win 17520 <mss 1460,nop,nop,sackOK> (DF)
13:34:24.358985 IP xxx.yyy.zzz.1.1048 > pc2.80: . ack 1 win 64240 (DF)
13:34:24.358998 IP xxx.yyy.zzz.1.1048 > pc2.80: P 1:45(44) ack 1 win 64240 (DF)
13:34:24.536515 IP pc2.80 > xxx.yyy.zzz.1.1048: . ack 45 win 17476 (DF)
13:34:24.537985 IP xxx.yyy.zzz.1.1048 > pc2.80: P 45:89(44) ack 1 win 64240 (DF)
13:34:24.736791 IP pc2.80 > xxx.yyy.zzz.1.1048: . ack 89 win 17432 (DF)
13:34:24.738223 IP xxx.yyy.zzz.1.1048 > pc2.80: P 89:177(88) ack 1 win 64240 (DF)
13:34:24.937084 IP pc2.80 > xxx.yyy.zzz.1.1048: . ack 177 win 17344 (DF)
13:34:25.257212 IP xxx.yyy.zzz.1.1048 > pc2.80: P 177:221(44) ack 1 win 64240 (DF)
13:34:25.437810 IP pc2.80 > xxx.yyy.zzz.1.1048: . ack 221 win 17300 (DF)
13:34:25.439190 IP xxx.yyy.zzz.1.1048 > pc2.80: P 221:265(44) ack 1 win 64240 (DF)
13:34:25.638115 IP pc2.80 > xxx.yyy.zzz.1.1048: . ack 265 win 17256 (DF)
13:34:25.858404 IP xxx.yyy.zzz.1.1048 > pc2.80: P 265:265(0) ack 1 win 64240 (DF)
13:34:25.858520 IP pc2.80 > xxx.yyy.zzz.1.1048: . ack 266 win 17256 (DF)
13:34:25.858846 IP pc2.80 > xxx.yyy.zzz.1.1048: F 1:1(0) ack 266 win 17256 (DF)
13:34:25.859514 IP xxx.yyy.zzz.1.1048 > pc2.80: . ack 2 win 64240 (DF)
13:34:25.859561 IP xxx.yyy.zzz.1.1049 > pc2.443: S 3573718243:3573718243(0) win 64240 <mss 1460,nop,nop,sackOK> (DF)
13:34:25.859675 IP pc2.443 > xxx.yyy.zzz.1.1049: S 724515765:724515765(0) ack 3573718244 win 17520 <mss 1460,nop,nop,sackOK> (DF)
13:34:25.861055 IP xxx.yyy.zzz.1.1049 > pc2.443: . ack 1 win 64240 (DF)
13:34:25.861071 IP xxx.yyy.zzz.1.1049 > pc2.443: P 1:45(44) ack 1 win 64240 (DF)
13:34:25.880771 IP pc2.443 > xxx.yyy.zzz.1.1049: F 1:1(0) ack 45 win 17476 (DF)
13:34:25.882166 IP xxx.yyy.zzz.1.1049 > pc2.443: P 45:89(44) ack 2 win 64240 (DF)
13:34:25.882281 IP pc2.443 > xxx.yyy.zzz.1.1049: R 724515767:724515767(0) win 0 (DF)
```

Figure 3.2.2.4.1

Note : pc2 is a host name of our external Web server. It maps to IP address : 192.168.1.3

5. Output of external DNS server TCP scan from the Internet :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -pi-65535 xxx.yyy.zzz.5
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-11 13:39 Eastern Daylight Time
Host xxx.yyy.zzz.5 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.5 at 13:40
Adding open port 53/tcp
The SYN Stealth Scan took 248 seconds to scan 65535 ports.
Initiating RPCGrind Scan against xxx.yyy.zzz.5 at 13:44
The RPCGrind Scan took 0 seconds to scan 1 ports.
Interesting ports on xxx.yyy.zzz.5:
(The 65534 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
53/tcp    open  domain

Nmap run completed -- 1 IP address (1 host up) scanned in 253.034 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.5

6. Output of external DNS server UDP scan from the internet :

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -p1-65535 xxx.yyy.zzz.5
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-11 13:46 Eastern Daylight Time
Host xxx.yyy.zzz.5 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.5 at 13:46
The UDP Scan took 81 seconds to scan 65535 ports.
Adding open port 53/udp
Initiating RPCGrind Scan against xxx.yyy.zzz.5 at 13:47
The RPCGrind Scan took 1 second to scan 1 ports.
Interesting ports on xxx.yyy.zzz.5:
<The 65534 ports scanned but not shown below are in state: closed>
PORT      STATE SERVICE VERSION
53/udp    open  domain
Nmap run completed -- 1 IP address <1 host up> scanned in 87.816 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.6

As expected, both TCP and UDP ports are open for DNS communications on port 53.

7. Output of Secure Reverse Proxy server TCP scan from the internet :

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -p1-65535 199.100.100.6
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-11 14:20 Eastern Daylight Time
Host 199.100.100.6 appears to be up ... good.
Initiating UDP Scan against 199.100.100.6 at 14:20
The UDP Scan took 65 seconds to scan 65535 ports.
All 65535 scanned ports on 199.100.100.6 are: closed
Nmap run completed -- 1 IP address <1 host up> scanned in 69.881 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.7

We have implemented Secure reverse proxy server on our DMZ network to proxy traffic between our Lotus Notes / Domino server and the Internet. We are using 2 custom ports for these connections.

8. Output of Secure Reverse Proxy server UDP scan from the internet :

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -p1-65535 xxx.yyy.zzz.6
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-11 14:20 Eastern Daylight Time
Host xxx.yyy.zzz.6 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.6 at 14:20
The UDP Scan took 65 seconds to scan 65535 ports.
All 65535 scanned ports on xxx.yyy.zzz.6 are: closed
Nmap run completed -- 1 IP address <1 host up> scanned in 69.881 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.8

The scan showed no open UDP ports on our secure reverse proxy server

9. Output of SSH2 server TCP scan from the Internet :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -p1-65535 xxx.yyy.zzz.7

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-11 14:23 Eastern
Daylight Time
Host xxx.yyy.zzz.7 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.7 at 14:23
Adding open port 22/tcp
The SYN Stealth Scan took 239 seconds to scan 65535 ports.
Initiating RPCGrind Scan against xxx.yyy.zzz.7 at 14:27
The RPCGrind Scan took 1 second to scan 1 ports.
Interesting ports on xxx.yyy.zzz.7:
<The 65534 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
22/tcp    open  ssh

```

Nmap run completed -- 1 IP address (1 host up) scanned in 245.463 seconds

C:\nmap\nmap-3.45>

Figure 3.2.2.9

10. Output of SSH2 server UDP scan from the Internet :

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -p1-65535 xxx.yyy.zzz.7

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-11 14:28 Eastern
Daylight Time
Host xxx.yyy.zzz.7 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.7 at 14:28
The UDP Scan took 66 seconds to scan 65535 ports.
All 65535 scanned ports on xxx.yyy.zzz.7 are: closed

```

Nmap run completed -- 1 IP address (1 host up) scanned in 70.522 seconds

C:\nmap\nmap-3.45>

Figure 3.2.2.10

11. pinging to any of the above servers didn't work

Secondly we will test traffic from our Optional (DMZ) servers to the Internet as well as to our Trusted (Local) network.

1. Scanning from external SMTP server to Internet and all servers on Trusted (Internal) network
 - to Internet using TCP and UDP scans :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 xxx.yyy.zzz.1

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:41 Eastern
Daylight Time
Host xxx.yyy.zzz.1 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.1 at 16:41
Adding open port 25/tcp
The SYN Stealth Scan took 369 seconds to scan 65535 ports.
Initiating RPCGrind Scan against xxx.yyy.zzz.1 at 16:47
The RPCGrind Scan took 3 seconds to scan 1 ports.
Interesting ports on xxx.yyy.zzz.1:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
25/tcp    open  smtp
4112/tcp  closed unknown
4113/tcp  closed unknown

```

Nmap run completed -- 1 IP address (1 host up) scanned in 373.208 seconds

C:\nmap\nmap-3.45>

Figure 3.2.2.11

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 xxx.yyy.zzz.1

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:49 Eastern
Daylight Time
Host xxx.yyy.zzz.1 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.1 at 16:49
The UDP Scan took 208 seconds to scan 65535 ports.
All 65535 scanned ports on xxx.yyy.zzz.1 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 210.235 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.12

As expected, only SMTP port 25 was allowed to the Internet.

- to local LDAP and Certificate server using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.2

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:42 Eastern
Daylight Time
Host 192.168.100.2 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.2 at 16:42
The SYN Stealth Scan took 422 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.2 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 425.727 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.13

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.2

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:50 Eastern
Daylight Time
Host 192.168.100.2 appears to be up ... good.
Initiating UDP Scan against 192.168.100.2 at 16:50
The UDP Scan took 179 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.2 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 180.210 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.14

No Incoming TCP and UDP traffic allowed from our SMTP server to our LDAP server located on Trusted (Internal) network – as expected.

- to local IDS server using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.3

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:43 Eastern
Daylight Time
Host 192.168.100.3 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.3 at 16:43
The SYN Stealth Scan took 487 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.3 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 490.344 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.15

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.3
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:53 Eastern
Daylight Time
Host 192.168.100.3 appears to be up ... good.
Initiating UDP Scan against 192.168.100.3 at 16:53
The UDP Scan took 181 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.3 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 182.333 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.16

- to local Lotus Notes/Domino Server using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.4
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:54 Eastern
Daylight Time
Host 192.168.100.4 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.4 at 16:54
The SYN Stealth Scan took 239 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.4 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 239.539 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.17

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.4
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 17:03 Eastern
Daylight Time
Host 192.168.100.4 appears to be up ... good.
Initiating UDP Scan against 192.168.100.4 at 17:04
The UDP Scan took 565 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.4 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 566.289 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.18

- to local Lotus Notes/Domino virus scanning and Network backup server using TCP and UDP scans

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.5
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:57 Eastern
Daylight Time
Host 192.168.100.5 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.5 at 16:57
The SYN Stealth Scan took 441 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.5 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 443.004 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.19

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.5

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 17:05 Eastern
Daylight Time
Host 192.168.100.5 appears to be up ... good.
Initiating UDP Scan against 192.168.100.5 at 17:05
The UDP Scan took 252 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.5 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 253.640 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.20

- to local SMTP server using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.6

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 16:56 Eastern
Daylight Time
Host 192.168.100.6 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.6 at 16:56
Adding open port 25/tcp
The SYN Stealth Scan took 270 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.100.6 at 17:01
The RPCGrind Scan took 0 seconds to scan 1 ports.
Interesting ports on 192.168.100.6:
(The 65534 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp

```

Figure 3.2.2.21

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.6

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 17:03 Eastern
Daylight Time
Host 192.168.100.6 appears to be up ... good.
Initiating UDP Scan against 192.168.100.6 at 17:03
The UDP Scan took 599 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.6 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 599.729 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.22

TCP scan shows, that SMTP port 25 traffic is allowed from our external SMTP server to our internal SMTP server. This is with accordance to our rule base.

- to local DNS and file and printsharing server using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.7

Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 17:43 Eastern
Daylight Time
Host 192.168.100.7 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.7 at 17:43
The SYN Stealth Scan took 390 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.7 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 391.626 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.23


```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.7
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 12:41 Eastern
Daylight Time
Host 192.168.100.7 appears to be up ... good.
Initiating UDP Scan against 192.168.100.7 at 12:41
The UDP Scan took 59 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.7 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 60.270 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.24

- to local syslog and NTP server using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.8
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-12 17:43 Eastern
Daylight Time
Host 192.168.100.8 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.8 at 17:43
The SYN Stealth Scan took 565 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.8 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 565.637 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.25

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.8
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-12 17:55 Eastern
Daylight Time
Host 192.168.100.8 appears to be up ... good.
Initiating UDP Scan against 192.168.100.8 at 17:55
The UDP Scan took 247 seconds to scan 65535 ports.
Interesting ports on 192.168.100.8:
<The 65534 ports scanned but not shown below are in state: closed>
PORT      STATE      SERVICE VERSION
514/udp   filtered  syslog
Nmap run completed -- 1 IP address (1 host up) scanned in 248.732 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.26

All servers on GIAC's Optional(DMZ) network are setup to send their syslog data to the internal syslog server. The above UDP scan demonstrates that the syslog UDP port 514 is allowed through.

- to local Watchguard Firebox management workstation using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.9
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-12 17:43 Eastern
Daylight Time
Host 192.168.100.9 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.9 at 17:43
The SYN Stealth Scan took 577 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.9 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 578.337 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.27

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.9
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 17:54 Eastern
Daylight Time
Host 192.168.100.9 appears to be up ... good.
Initiating UDP Scan against 192.168.100.9 at 17:54
The UDP Scan took 243 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.9 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 244.295 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.28

Only our Firebox is allowed to communicate with our dedicated Watchguard administration workstation.

- to local PC with IP address 192.168.100.10 using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.10
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-13 12:51 Eastern
Daylight Time
Host 192.168.100.10 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.10 at 12:51
The SYN Stealth Scan took 210 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.10 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 211.708 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.29

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.10
Starting nmap 3.45 ( http://www.insecure.org/nmap ) at 2003-10-12 17:58 Eastern
Daylight Time
Host 192.168.100.10 appears to be up ... good.
Initiating UDP Scan against 192.168.100.10 at 17:58
The UDP Scan took 87 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.10 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 88.773 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.30

For the scans of our 7 remaining DMZ servers, we will only show the ones which produced unique results compared to the complete list of scans of our external SMTP server in section 1.

2. From external Web server :

- to local LDAP Certificate server using TCP scan :

```

C:\nmap\nmap-3.45>nmap -v -sS -P0 -p1-65535 192.168.100.2

Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 11:42 Eastern
Daylight Time
Host 192.168.100.2 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.2 at 11:42
Adding open port 636/tcp
The SYN Stealth Scan took 212 seconds to scan 65535 ports.
Interesting ports on 192.168.100.2:
<The 65534 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE
636/tcp   open  ldapssl

Nmap run completed -- 1 IP address <1 host up> scanned in 218.224 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.31

Our external Web server needs to communicate with GIAC's local LDAP server for user account creation. The communication is only allowed using SSL thus LDAPS on port 636.

3. From external DNS server :

- to Internet using TCP and UDP scans :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 xxx.yyy.zzz.1

Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 10:33 Eastern
Daylight Time
Host xxx.yyy.zzz.1 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.1 at 10:33
The SYN Stealth Scan took 206 seconds to scan 65535 ports.
Interesting ports on xxx.yyy.zzz.1:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
53/tcp    closed domain
4112/tcp  closed unknown
4113/tcp  closed unknown

Nmap run completed -- 1 IP address <1 host up> scanned in 206.447 seconds

C:\nmap\nmap-3.45>

```

Figure 3.2.2.32

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 xxx.yyy.zzz.1

Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 10:51 Eastern
Daylight Time
Host xxx.yyy.zzz.1 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.1 at 10:51
The UDP Scan took 59 seconds to scan 65535 ports.
All 65535 scanned ports on xxx.yyy.zzz.1 are: closed

Nmap run completed -- 1 IP address <1 host up> scanned in 59.806 seconds

```

Figure 3.2.2.33

Our nmap scan showed no open UDP ports, but from the firewall log it shows that port 53 UDP did make it through :

```

10/13/03 10:52 firewallld[104]: allow out eth2 28 udp 20 52 192.168.1.5 xxx.yyy.zzz.1 35907 53 (DNS-optional-internet)
10/13/03 10:54 firewallld[104]: allow out eth2 28 udp 20 41 192.168.1.5 xxx.yyy.zzz.1 53 53 (DNS-optional-internet)

```

Figure 3.2.2.34

4. From Secure Reverse Proxy server :

- to local Lotus Notes/Domino server using TCP scan :

```
C:\nmap\nmap-3.45>nmap -v -sS -P0 -p1-65535 192.168.100.4
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 11:57 Eastern
Daylight Time
Host 192.168.100.4 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.4 at 11:57
Adding open port 9000/tcp
The SYN Stealth Scan took 218 seconds to scan 65535 ports.
Interesting ports on 192.168.100.4:
<The 65534 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE
9000/tcp  open  unknown
Nmap run completed -- 1 IP address <1 host up> scanned in 224.122 seconds
```

Figure 3.2.2.35

Firewall log also confirms communication on this port has made it through :

```
10/13/03 11:13 firewalld[104]: allow in eth2 40 tcp 20 40 192.168.1.6 192.168.100.4 39405 9000 syn (HTTPS-9000)
10/13/03 11:13 firewalld[104]: allow in eth2 40 tcp 20 40 192.168.1.6 192.168.100.4 39406 9000 syn (HTTPS-9000)
```

Figure 3.2.2.36

5. Our SSH2 server has no Outgoing access.

6. Our external NTP server can only communicate with the specified stratum servers to synchronize its time.

7. From Backup and Virus Scanning server :

- to Internet using TCP scan :

```
C:\nmap\nmap-3.45>nmap -v -sS -P0 -p1-65535 xxx.yyy.zzz.1
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 13:57 Eastern
Daylight Time
Host xxx.yyy.zzz.1 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.1 at 13:57
Adding open port 80/tcp
The SYN Stealth Scan took 212 seconds to scan 65535 ports.
Interesting ports on xxx.yyy.zzz.1:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE
80/tcp    open  http
4112/tcp  closed unknown
4113/tcp  closed unknown
Nmap run completed -- 1 IP address <1 host up> scanned in 218.304 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.37

We have allowed Outgoing HTTP port 80 from our external Virus scanning server to the Internet to permit virus definition updates.

8. IDS server (Snort) no Outgoing traffic allowed.

Thirdly we will test traffic from our local servers to the Internet as well as to our Optional (DMZ) network.

1. From LDAP and Certificate server

- to Internet using TCP and UDP scans :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 xxx.yyy.zzz.1

Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 14:14 Eastern
Daylight Time
Host xxx.yyy.zzz.1 appears to be up ... good.
Initiating SYN Stealth Scan against xxx.yyy.zzz.1 at 14:14
Adding open port 80/tcp
Adding open port 443/tcp
Adding open port 21/tcp
The SYN Stealth Scan took 210 seconds to scan 65535 ports.
Initiating RPCGrind Scan against xxx.yyy.zzz.1 at 14:17
The RPCGrind Scan took 2 seconds to scan 3 ports.
Interesting ports on xxx.yyy.zzz.1:
<The 65530 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
4112/tcp  closed unknown
4113/tcp  closed unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 212.411 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.38

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 xxx.yyy.zzz.1

Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 14:36 Eastern
Daylight Time
Host xxx.yyy.zzz.1 appears to be up ... good.
Initiating UDP Scan against xxx.yyy.zzz.1 at 14:36
The UDP Scan took 60 seconds to scan 65535 ports.
All 65535 scanned ports on xxx.yyy.zzz.1 are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 60.551 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.39

The above scan produced the same results for all of the systems on our Trusted (Local) network. They are only allowed access to the Internet on ports : FTP port 21, HTTP port 80 and HTTPS port 443. This is with compliance with GIAC's security policy.

- to Web server on DMZ network using TCP scan :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.1.4
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:04 Eastern Daylight Time
Host 192.168.1.4 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.1.4 at 15:04
Adding open port 443/tcp
Adding open port 80/tcp
The SYN Stealth Scan took 210 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.1.4 at 15:07
The RPCGrind Scan took 2 seconds to scan 2 ports.
Interesting ports on 192.168.1.4:
<The 65531 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
80/tcp    open  http
443/tcp    open  https
4112/tcp   closed unknown
4113/tcp   closed unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 213.061 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.40

All systems on our Trusted (Local) network are allowed access to our External web server : HTTP and HTTPS.

- to Secure Reverse Proxy server using TCP scan :

```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.1.6
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 14:51 Eastern Daylight Time
Host 192.168.1.6 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.1.6 at 14:51
Adding open port 4001/tcp
Adding open port 4000/tcp
The SYN Stealth Scan took 210 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.1.6 at 14:55
The RPCGrind Scan took 2 seconds to scan 2 ports.
Interesting ports on 192.168.1.6:
<The 65531 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
4000/tcp   open  remoteanything
4001/tcp   open  unknown
4112/tcp   closed unknown
4113/tcp   closed unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 212.070 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.41

All systems on our Trusted(Local) network are allowed access to our Secure Reverse Proxy server on ports HTTPS 4000 and HTTPS 4001.

No other access from LDAP server to our DMZ network servers is allowed.

2. From IDS server. IDS server has the same Outgoing access privileges as our LDAP server.
3. Internal Lotus Notes / Domino server has the same Outgoing access privileges as our LDAP server
4. Internal Backup and Virus Scanning server has the same Outgoing access privileges as our LDAP server
5. Internal SMTP e-mail server has the same Outgoing access privileges as our LDAP server and additionally it can access GIAC's external SMTP mail relay server :

- to external SMTP server using TCP scan :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.1.3
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:21 Eastern
Daylight Time
Host 192.168.1.3 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.1.3 at 15:21
Adding open port 25/tcp
The SYN Stealth Scan took 210 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.1.3 at 15:25
The RPCGrind Scan took 0 seconds to scan 1 ports.
Interesting ports on 192.168.1.3:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
25/tcp    open  smtp
4112/tcp  closed unknown
4113/tcp  closed unknown
Nmap run completed -- 1 IP address <1 host up> scanned in 211.669 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.42

6. Internal DNS server has the same Outgoing access privileges as our LDAP server. Additionally it can access GIAC's external DNS server :

- to external DNS server using TCP and UDP scans :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.1.5
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:11 Eastern
Daylight Time
Host 192.168.1.5 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.1.5 at 15:11
Adding open port 53/tcp
The SYN Stealth Scan took 209 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.1.5 at 15:14
The RPCGrind Scan took 1 second to scan 1 ports.
Interesting ports on 192.168.1.5:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
53/tcp    open  domain
4112/tcp  closed unknown
4113/tcp  closed unknown
Nmap run completed -- 1 IP address <1 host up> scanned in 210.798 seconds
```

Figure 3.2.2.43

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.1.5
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:15 Eastern
Daylight Time
Host 192.168.1.5 appears to be up ... good.
Initiating UDP Scan against 192.168.1.5 at 15:15
The UDP Scan took 60 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.1.5 are: closed
Nmap run completed -- 1 IP address <1 host up> scanned in 61.413 seconds
```

Figure 3.2.2.44

```
10/13/03 15:18 firewalld[104]: allow out eth1 28 udp 20 53 192.168.100.7 192.168.1.5 53 53 (DNS-trusted-optional)
```

Figure 3.2.2.45

Although our DNS UDP scan didn't show any open UDP ports, our firewall log showed the DNS UDP packet made it through to our external DNS server.

7. Internal NTP server has the same Outgoing access privileges as our LDAP server. Additionally it can access GIAC's external NTP server :

- to External NTP server using TCP and UDP scans :

```
C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.1.8
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:31 Eastern
Daylight Time
Host 192.168.1.8 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.1.8 at 15:31
Adding open port 123/tcp
The SYN Stealth Scan took 211 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.1.8 at 15:35
The RPCGrind Scan took 1 second to scan 1 ports.
Interesting ports on 192.168.1.8:
<The 65532 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
123/tcp   open  ntp
4112/tcp  closed unknown
4113/tcp  closed unknown

Nmap run completed -- 1 IP address <1 host up> scanned in 213.031 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.46

```
C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.1.8
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:37 Eastern
Daylight Time
Host 192.168.1.8 appears to be up ... good.
Initiating UDP Scan against 192.168.1.8 at 15:37
The UDP Scan took 54 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.1.8 are: closed

Nmap run completed -- 1 IP address <1 host up> scanned in 54.763 seconds
C:\nmap\nmap-3.45>
```

Figure 3.2.2.47

```
10/13/03 15:38 firewalld[104]: allow out eth1 28 udp 20 38 192.168.100.8 192.168.1.8 43089 123 (NTP-local)
```

Figure 3.2.2.48

The UDP scan of our external NTP server didn't show any open UDP ports. But by closely examining our firewall logs NTP UDP packet on UDP port 123 made it through the firewall.

8. Firebox administration workstation has the same Outgoing access privileges as our LDAP server. Additionally it can access Firebox appliance for administration and monitoring purposes :

- to Firewall from Firebox administration workstation using TCP and UDP scans :


```

C:\nmap\nmap-3.45>nmap -v -sS -sR -P0 -n -p1-65535 192.168.100.1
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:42 Eastern Daylight Time
Host 192.168.100.1 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.100.1 at 15:42
Adding open port 4113/tcp
Adding open port 4105/tcp
Adding open port 4100/tcp
Adding open port 4112/tcp
The SYN Stealth Scan took 191 seconds to scan 65535 ports.
Initiating RPCGrind Scan against 192.168.100.1 at 15:45
The RPCGrind Scan took 3 seconds to scan 4 ports.
Interesting ports on 192.168.100.1:
<The 65530 ports scanned but not shown below are in state: filtered>
PORT      STATE SERVICE VERSION
4100/tcp  open  unknown
4103/tcp  closed unknown
4105/tcp  open  unknown
4112/tcp  open  unknown
4113/tcp  open  unknown

Nmap run completed -- 1 IP address <1 host up> scanned in 195.511 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.49

```

C:\nmap\nmap-3.45>nmap -v -sU -sR -P0 -n -p1-65535 192.168.100.1
Starting nmap 3.45 < http://www.insecure.org/nmap > at 2003-10-13 15:48 Eastern Daylight Time
Host 192.168.100.1 appears to be up ... good.
Initiating UDP Scan against 192.168.100.1 at 15:48
The UDP Scan took 52 seconds to scan 65535 ports.
All 65535 scanned ports on 192.168.100.1 are: closed

Nmap run completed -- 1 IP address <1 host up> scanned in 54.338 seconds
C:\nmap\nmap-3.45>

```

Figure 3.2.2.50

The scan shows port 4105 open. This port is used for Watchguard firebox service. As expected, only our local Workstation with IP address 192.168.100.9 can communicate with the firewall on this port.

9. Any other host on Trusted local network can access the Internet on ports HTTP:80, HTTPS:443 and FTP:21. It can also access Secure Reverse proxy and Web servers on GIAC's Optional(DMZ) network.

10. pinging from any host to Firewall and Internet was successful.

As we have noticed from our scan we are allowing DNS access to our external DNS server on both UDP port: 53 and TCP port: 53. We could limit this to only UDP port: 53 as there should not be any replies from our external DNS systems larger than 492 bytes. We would need to configure "User Defined" service in Watchguard's "Add Service" menu to implement this change.

We have a PING rule to allow Internal users to ping to any hosts on the DMZ network as well as on the Internet. We could limit this service to only allow pinging to our Firebox (for testing and / or troubleshooting purposes) or disable pinging altogether.

VPN rule which allows VPN IPSec users to use Any service on GIAC's internal network may prove to be too lenient. We may be required to limit access to certain services for VPN users based on their privileges.

Also, we could add another Watchguard firewall appliance as hot spare(stand by) to allow for uninterrupted network uptime due to hardware failures.

4. Assignment 4 – Design under Fire

In this part of the document we will focus on evaluating network security of GCFW practical assignment by Lesa Ludwig. Her practical can be found at : http://www.giac.org/practical/GCFW/Lesa_Ludwig_GCFW.pdf

We will divide our attacks into 3 segments :

- attack against the firewall itself
- distributed denial of service attack (DDoS)
- attack plan to compromise an internal system

Lesla Ludwig's network diagram is shown below :

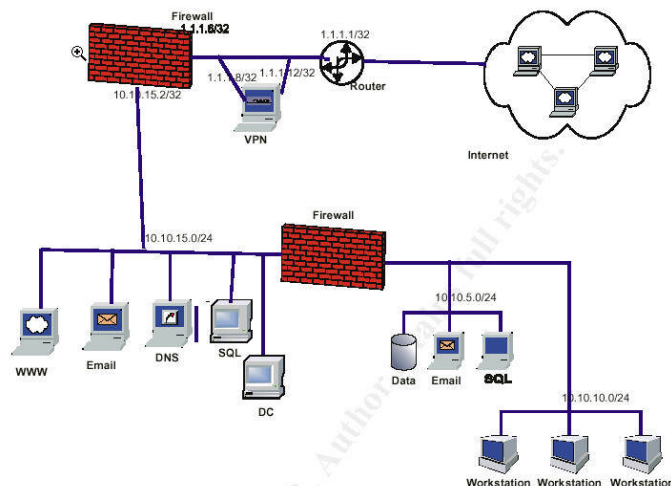


Figure 4.0

4.1 Attack against the firewall

Lesla is using IPCop 1.3.0 Linux based firewall. The firewall runs on a hardened version of Linux operating system with kernel release 2.4.20. First, we will spend some time on researching any vulnerabilities of the firewall system and ways to exploit them.

By checking IPCop distribution and support web site - www.ipcop.org we have found the following advisory :

- <http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopAdvisories>
Kernel Network DoS - "If there was an FTP or IRC session open, it was possible to remotely crash the machine by sending a special packet. It was not possible to gain access to the IPCop machine".

The advisory states that the original version of IPCop 1.3 Linux kernel (2.4.20) has ip_nat_ftp and ip_nat_irc modules enabled by default. Lesla has not specified if she disabled those 2 options of the kernel and if she applied the patch addressing this problem.

After extensive searches on <http://xforce.iss.net/xforce/xfdb/12806> , <http://www.securityfocus.com/bid/8330> and <http://www.netfilter.org/security/2003-08-01-nat-sack.html> sites I could not find any examples of “specially crafted” packets which I could send to the firewall to exploit this vulnerability and crash the firewall.

To be able to narrow my search for IPCop 1.3 firewall vulnerabilities, I decided to install a copy of the software on one of my machines and take note of service versions running on it :

Iptables – 1.2.7a

Apache http server – 1.3.27

OpenSSL – 0.9.6b

Syslogd – 1.4.1

Linux kernel version – 2.4.20

Note: all these versions apply to unpatched IPCop 1.3 firewall configuration.

At this point I could try to exploit OpenSSL 0.9.6b vulnerability in Apache web server mod_ssl module (CERT Advisory CA-2002-27 Apache/mod_ssl Worm). This vulnerability is known as Linux Slapper Worm. The code uses the OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow vulnerability to propagate. A sample of the exploit code can be found under

<http://packetstoresecurity.org/0209-exploits/bugtraqworm.tgz>.

The worm will try to connect to GIAC’s firewall server on port 80 and send a simple "GET /" request to check if the server runs an Apache version :

GET / HTTP/1.1\r\n\r\n

This is an invalid HTTP 1.1 request, since it doesn’t contain the *Host:* parameter. After receiving the request, Apache web server will generate the following response :

HTTP/1.1 400 Bad Request

Date: Fri, 13 Sep 2002 10:24:13 GMT

Server: Apache/1.3.23 (Unix) (Red-Hat/Linux)

Connection: close

Transfer-Encoding: chunked

Content-Type: text/html; charset=iso-8859-1

Next, the worm will check if the specific Apache version reported in the HTTP *Server:* response line matches any of the versions it knows to infect. In our case, an Apache server version would be unknown to the worm (1.3.27). In this situation, the worm is setup to assume Apache version 1.3.26 running on Red Hat Linux operating system. At this stage, the worm will attempt to exploit the SSL2 vulnerability by communicating with the SSL server on port 443. If the exploit was successful, it will uuencode copy of its source, upload it through the hacked connection into the GIAC firewall server, compile it using gcc compiler

and execute it. The whole process will create the following 3 files under /tmp directory on the victim's server :

```
/tmp/.uubugtraq  
/tmp/.bugtraq.c  
/tmp/.bugtraq
```

The whole command syntax run by the worm is as follows :

```
/usr/bin/uudecode -o /tmp/.bugtraq.c /tmp/.uubugtraq;gcc -o /tmp/.bugtraq  
/tmp/.bugtraq.c -lcrypto;/tmp/.bugtraq %s;exit;\n
```

As soon as the worm is executed, there will be a process called .bugtraq running in the process table. The Linux Slapper worm will, by default, listen on UDP port 2002 for peer-to-peer connections. This will allow me launch all sorts of attacks against the compromised GIAC firewall server: flooding it with UDP, TCP, DNS or RAW packets (DOS), running local commands, downloading a binary from a remote machine via HTTP and running it, sending mails, to name a few.

4.1.1 Countermeasures

Most likely I would not be able to exploit Lesa's IP Cop 1.3 firewall system using the Linux Slapper worm. She is not allowing any external IP addresses to communicate with the firewall's web server. Only a dedicated Windows 2000 Professional machine running on internal network is permitted access to the Firewall system (for administrative purposes). The IPCop 1.3 firewall's admin server is also only accepting HTTP requests on port 81 instead of 80. Moreover, the firewall doesn't come with gcc compiler thus the virus would not be able to compile and execute its source.

Although Lesa's IpCop 1.3 system is relatively secure "out of the box" I would recommend applying the newest patches for it (one of them includes OpenSSL patch). They can be found on IPCop web site <http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopDownload>.

4.2 Distributed denial of service attack (DDoS).

In this part of the assignment we will attempt to accomplish the following :

- compromise 50 cable / DSL connected systems
- perform a DDoS attack using the above compromised systems
- outline countermeasures to mitigate the DDoS attack

4.2.1. Compromise of 50 cable / DSL connected systems

The first task on the list is to find 50 cable / DSL internet connected systems, break into them and plant our DDoS tool(s). We will begin with finding 50 IP addresses belonging to cable / DSL Internet connected systems. This can be accomplished by researching on-line gaming, peer-to-peer or IRC (internet relay chat) servers and checking for DSL / cable users. We will look for specific domain names of known cable / DSL Internet service providers as well as latency in response times. Once we will find a host, whose fully qualified domain name contains known cable / DSL ISP domain name and response time falls within a range of fast cable / DSL system, we will try to resolve that name to an IP address using nslookup utility. We will use <http://www.sampade.org> site to perform the resolution to minimize our exposure. If the resolution is successful, we will attempt to scan a range of host names close to the one we found until we end up with 50 IP addresses.

In the next step we will scan those 50 systems looking for vulnerabilities. The tool of choice here will be NESSUS (<http://www.nessus.org>). Depending on what vulnerabilities NESSUS will find (if any), we will either continue with gathering as much information about our “victims” as possible (using nmap and other tools) or keep searching for more cable / DSL hosts.

An example of nmap command we could use against one of the 50 system would be :

nmap -O “ip address”

This command will try to determine version of the operating system running on the specific host. Knowing the type and version of our victim’s OS would make the task of compromising it much easier.

Once we are able to determine that we have successfully found 50 cable / DSL systems suitable for planting our DDoS tools on, we will proceed with our distributed denial of service attack against Lesa Ludwig design. We will choose TFN2K utility by Mixter, downloadable from

<http://packetstormsecurity.org/distributed/tfn2k.tgz> to perform the attack.

The reason for choosing TFN2K utility to perform our DDoS attack is that the tool is widely available, it is free and it is considered to be one of the most effective. The TFN2k tool consists of 2 components:

- master machine running a client program
- agent systems running daemon processes

The master machine with its command-driven client program initiates attacks by sending instructions to the clients to unleash flood of packets against the target machine(s). The target machine(s) get overwhelmed by the amount of received packets, which results in service disruptions and in worst cases, their complete shutdown or crash. What makes TFN2k different from other DDoS tools is that master to agent communications are encrypted using a key-based CAST-256 algorithm. Moreover, the agent machine doesn’t acknowledge any commands it receives from the master system. The master relies on probability that at least 1 command out of 20 it sends to the agent’s daemon will be received. All of this makes tracing and fighting against this DDoS tool very difficult.

4.2.2. Denial of Service attack

At this point we were able to successfully install TFN2k daemons on all of the 50 compromised cable / DSL Internet connected systems. The master machine running the client program will be one of our own systems with spoofed IP address.

TFN2k tool can perform the following list of attacks :

- TCP / SYN
- UDP
- ICMP / PING
- Broadcast PING (Smurf) packet flood

We will instruct our agents to run all of the above kinds of attacks against Lesa's network. To avoid any patterns we will also randomly alternate between the 4 types of attacks.

We will SYN flood ports 80 and 443 to the external Web server and port 25 to the external SMTP relay mail server. This attack will bring the Web and SMTP server to their knees. The servers won't be able to process requests on time due to overwhelmingly high number of packets hitting them.

We will UDP flood port 53 to external DNS server. This attack should make any name lookup requests coming from the Internet to GIAC's external DNS server fail.

And finally we will instruct our agents to also ICMP / PING and Broadcast PING flood the entire network. This attack will cause degradation in GIAC's network performance as well as limit access bandwidth to the Internet.

4.2.3. Countermeasures

- use of an IDS server. Lesa's design doesn't include any IDS (Intrusion Detection Systems). Having an IDS system between the border router and DMZ network would help in alerting local administrators of suspicious network traffic. IPCop ver 1.3 has a built in IDS system (Snort) but Lesa chose to leave it disabled.
- use of service specific proxies. There are no service proxies implemented for incoming HTTP, SMTP and DNS traffic. The HTTP service proxy would prevent SYN floods to ports 80(HTTP) and 443(HTTPS). The SMTP and DNS service proxies would also protect us from the TFN2k tool initiated SYN and UDP flood attacks on ports 25 and 53 respectively.

By closely analyzing GIAC's External firewall's iptables configuration file, we have noticed that Lesa implemented 10sec packet limit to reduce SYN flood attacks. This option will time out initiated SYN, half-opened, connections faster therefore freeing up TCP buffer space.

Lesa is also already blocking unnecessary ICMP traffic on the border router. This will limit the exposure to ICMP / PING and Broadcast PING attacks.

- filter all non-routable and unassigned IP addresses. Lesa is already doing this on the border router
- keep good relationship with the ISP. Good internet service providers will attempt to stop spoofed IP address from entering the Internet. Of course we can not fully rely on our ISP to help us fight against all of the DDoS attacks but any assistance from their side will help us in addressing the problem.

4.3 Compromising an internal system

To be able to compromise any of the internal systems in Lesa's network design we will need to break through the main perimeter defenses (border router and primary firewall) as well as her second line of defense – internal firewall.

I will attempt to compromise Lesa's e-mail servers. The external e-mail server is a Microsoft Windows 2000 Server machine with service pack 4 applied. It has been hardened using Microsoft and NSA security guidelines. The system uses Clearswift Mail Sweeper 4.3 for SMTP to filter out unwanted e-mail messages based on their content. Accepted e-mails are then relayed to GIAC's internal e-mail server, which runs Microsoft Exchange 2000.

I have found a new exploit for Clearswift Mail Sweeper 4.3 for SMTP on <http://www.secunia.com/advisories/10148/> site:

"A vulnerability has been identified in MAILsweeper for SMTP 4.3, which can be exploited by malicious people to bypass the virus detection.

The vulnerability is caused due to an error when checking certain malformed Zip archives (eg. those generated by some Mimap worm variants). This can be exploited to send a virus through the MAILsweeper without it being detected."

The first step in attempting to exploit this vulnerability would be to find a list of valid e-mail addresses to send the exploit code to. I will try to obtain it from GIAC's main web site. By clicking on Contact US button, I will look for marketing / management e-mail contact addresses. Employees belonging to either of the two categories are usually the most vulnerable to outside attacks. Once armed with valid e-mail addresses list I will send a file called message.zip containing MIMAIL worm to each member of the list hoping that at least one of them will open it. The message.zip file contains a specially crafted MHTML file named "message.html". The email message body will look similar to the following:

From: admin@<your domain>

Subject: <your account> [random text]

Hello there,

I would like to inform you about important information regarding your email address. This email address will be expiring.

Please read attachment for details

Best regards, Administrator

[random text]

As soon as any of my potential victims opens the e-mail and views the 'message.html' file, the malicious code will be installed and executed. It will run as run as %windowsroot%\videodrv.exe. The worm will search for new victims (recipients) by scanning files in C:\Documents and Settings\{current_user}\ , C:\Program Files\ and C:\%windowsroot%\Fonts\ looking for the pattern %s@%s. All picked up e-mail addresses will be stored under %windowsroot% directory in eml.tmp file. At this point the virus will re-distribute itself to newly found e-mail addresses and attempt a DDoS attack most popular spam blocking sites. One thing of note: What is actually allowing the automatic execution of the e-mail attachment, once it successfully passes through Mail Sweeper and Anti-Virus defenses, is a Microsoft Outlook Express and Internet Explorer vulnerability described in Microsoft security bulletin MS03-014. The above is a 1 example of exploitation of this vulnerability. I used MIMAIL virus method to bypass MAILsweeper defenses and infect internal machine(s). I could send my own, specially crafted zip file, with much more malicious content to attack GIAC's internal systems.

4.3.1 Countermeasures

As stated on <http://www.secunia.com/advisories/10148/> page, to prevent exploitation of this vulnerability MailSweeper 4.3 for SMTP will need to be patched to version 4.3.10 with technology update ver. 1.4_9 or above. Also, to stop automatic execution of the e-mail attachment, Microsoft patch number 330994 will need to be applied to all of the internal systems. I am not certain if this exploit would work on Lesa's network. She has a Norton Antivirus Enterprise running on all servers (including e-mail systems) and virus definitions are updated daily. It is to be seen if the MIMAIL virus malformed zip file attachment would be able to sneak pass the virus scanning software due to MAILSweeper 4.3 vulnerability.

5. References

1. SANS Institute, Track 2 – Firewall, Perimeter Protection and VPN's – 2.1 TCP/IP, 2003
2. SANS Institute, Track 2 - Firewall, Perimeter Protection and VPN's – 2.2 Packet Filters, 2003
3. SANS Institute, Track 2 - Firewall, Perimeter Protection and VPN's – 2.3 Firewalls, 2003
4. SANS Institute, Track 2 - Firewall, Perimeter Protection and VPN's – 2.4 Defense in Depth, 2003
5. SANS Institute, Track 2 - Firewall, Perimeter Protection and VPN's – 2.5 VPN's, 2003

6. SANS Institute, Track 2 - Firewall, Perimeter Protection and VPN's – 2.6 Network Design and Assessment, 2003
7. NSA/SNAC Router Security Configuration Guide ver. 1.1
<http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf>, September 27, 2003
8. Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks
<http://www.cisco.com/warp/public/707/newsflash.html>, Apr 29, 2003
9. Distributed Intrusion Detection System, Top 10 most wanted
<http://www.dshield.org/top10.php>, Jan 19, 2004
10. IANA Internet Protocol v4 address space
<http://www.iana.org/assignments/ipv4-address-space>, Nov. 14, 2003
11. Watchguard Firebox III ver 6.2 User Guide
<http://www.watchguard.com/help/docs/v62UserGuide.pdf>
12. Watchguard Firebox III ver 6.2 VPN Guide
<http://www.watchguard.com/help/docs/v62VPNGuide.pdf>
13. Watchguard Firebox III ver. 6.1 Mobile User Administrator Guide
<http://www.watchguard.com/help/docs/v611MUVPNAdministratorGuide.pdf>
14. Watchguard Firebox III ver.6.2 Reference Guide
<http://www.watchguard.com/help/docs/v62ReferenceGuide.pdf>
15. Request for comments RFC
<http://www.ietf.org/rfc/rfc0821.txt?number=821>,
<http://www.ietf.org/rfc/rfc0822.txt?number=822>,
<http://www.ietf.org/rfc/rfc2616.txt?number=2616>
16. Lance Spitzner, Auditing Your Firewall Setup
<http://www.spitzner.net/audit.net>
17. Fyodor, Nmap port scanning utility <http://www.insecure.org>
18. Chris Wysopal, Netcat utility ver.02.08.98
http://www.atstake.com/research/tools/network_utilities
19. Windump utility ver. 3.8 alpha <http://windump.polito.it>, July 18, 2003
20. Lesa Ludwig, Attack against a firewall ver. 2.0

- http://www.giac.org/practical/GCFW/Lesa_Ludwig_GCFW.pdf, October 2003
21. System vulnerabilities research sites : <http://www.securityfocus.com>, <http://xforce.iss.net>, <http://www.netfilter.org/security/2003-08-01-nat-sack.html> , <http://www.bugtraq.org> , <http://www.ipcop.org/cgi-bin/twiki/view/IPCop/IPCopAdvisories>
 22. CERT Advisory CA-2002-27 Apache/mod_ssl Worm
<http://www.cert.org/advisories/CA-2002-27.html> , October 11, 2002
 23. Security Focus, Linux Slapper Worm description
Bartek Kostanecki, Mario Van Velzen, Marc Fossi, Jensenne Roculan,
http://analyzer.securityfocus.com/alerts/020913-Alert-Apache-mod_ssl-Exploit.pdf, September 14, 2002,
KasperskyLab, <http://www.avp.ch/avpve/worms/linux/slapper.stm>
 24. Packetstorm Security, Linux Slapper Worm code
<http://packetstormsecurity.org/0209-exploits/bugtraqworm.tgz>
 25. Samspade Web based network analyzer <http://samspade.org>
 26. Renaud Deraison, Nessus utility ver. 2.0.9
http://www.nessus.org/nessus_2_0.html
 27. Jason Barlow and Woody Thrower, TFN2k – An Analysis by Jason Barlow and Woody Thrower
http://packetstormsecurity.nl/distributed/TFN2k_Analysis-1.3.txt, March 7, 2000
 28. Mixer, TFN2k DDoS attack tool
<http://packetstormsecurity.org/distributed/tfn2k.tgz>
 29. Secunia, MAILsweeper Malformed Zip Archive Virus Detection Bypass vulnerability <http://www.secunia.com/advisories/10148/> , Nov. 26, 2003
 30. Sophos, MIMAIL.A virus description
<http://www.sophos.com/virusinfo/analyses/w32mimaila.html>, August 2003
 31. Microsoft, Microsoft Security Bulletin MS03-014
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-014.asp> , August 22, 2003
 32. Microsoft, Microsoft patch number 330994 download page
<http://www.microsoft.com/windows/ie/downloads/critical/330994/default.asp>, April , 2003