Global Information Assurance Certification Paper

SANS GIAC Certification

GCFW Practical Assignment
Version 1.9

Secure Network Architecture for GIAC Enterprise

By

Agustinus Wibisono

March 17, 2003

Table Of Contents

Abstract

This paper is part of the requirement for obtaining GIAC Certified Firewall Analyst (GCFW). Practical Assignment version 1.9 is used for completion of the paper.

The paper will cover the development of the secure network architecture required by GIAC Enterprise, which comprises of four sections:

- Determining the access requirements for the business operation of the company and designing the network based on those requirements.
- Defining the policy for the perimeter defense systems - border router, firewall and vpn, to provide adequate level of security for the network to support the business operation. Tutorial on configuring the firewall will also be included here.
- Auditing the policy implemented on the firewall to ensure it is performing the task it should do.
- Discussing attack scenarios against other architecture, which are exploiting HTTP Proxy running on the firewall, performing Distributed Denial of Service attack to the network, and attacking web server with Denial of Service exploit.

Assignment 1 – Security Architecture

Introduction

GIAC Enterprise is a startup company with core business in online sale of fortune cookies sayings. The nature of the business will require 24 hours connectivity through Internet and depend on this service, in which system and network security is a very important element that has to be counted in.

As a startup company, GIAC Enterprise management has decided to go by step by step approach in building the network infrastructure, which at first will start with the sufficient requirement to get the operation up and running, but with the adequate security measures in place. As the company grows, upgrades can be done in the future accordingly.

In its business operation, there are few parties communicating with GIAC Enterprise and making use of computer resources of the company:

- Customers
  They need to make online direct purchases of fortunes with GIAC Enterprise.
- Partners
  GIAC Enterprise makes use of partners to translate and resell fortunes, in which they also need to communicate with GIAC Enterprise to purchase fortunes.
- Suppliers
  GIAC Enterprise needs to communicate with them in order to purchase fortunes to be sold to customers or partners.

- Mobile Sales Force and Teleworkers
  These are GIAC Enterprise's employees located outside office which either selling the fortunes on the field or just work remotely with any other functions.
- Employees in the GIAC Enterprise office
  These are employees that located in the GIAC Enterprise office, or in other words, in the internal network.

Access Requirements

In accordance to the defined parties involved in the business operation, each of them will have their access requirements and methods over the resources they require. Most of the methods will make use of Internet as the basis of the communication.

- **Customers**
  They need to connect to GIAC Enterprise to make purchases. To cater for this, a secured web site is provided, where the customer can connect using web connection protected by SSLv3 over the Internet. They can log in using the user name and password provided for them, and make their purchases.

- **Partners**
  With similar requirements as customers, partners are provided similar access, which through web connection with SSLv3 protection.
  They are given different web site for partners, with user name and password to gain the access, and then perform their purchases.

- **Suppliers**
  In communicating with few suppliers, GIAC Enterprise is provided with web access over SSLv3 connection, user names and passwords to make the purchases.
  In this case GIAC Enterprise is the one initiating the communication to the suppliers when they need to do purchases.
  These purchases then need to be appended manually by the GIAC Enterprise purchasing staffs, using the database application, into the database server.

- **Mobile Sales Force and Teleworkers**
  Both of them need to communicate with GIAC Enterprise internal network resources in order to carry out their job. They need to connect to the database server to get or add transactions data, access their emails, or access files saved in the server.
  Both types of employees will be provided with VPN connection from their workstations to connect to the GIAC Enterprise internal network.
  Access control on database, email and file server will determine the rights for each person accordingly.

- **Employees in the GIAC Enterprise office**
  Internal employees will need to access the internal resources, which are the databases, email system, file server and print server. Access control on those systems will determine who are authorized for the access.
  Access to the Internet will also be required for web and ftp, to get information off the Internet.

- **Everybody else**
  Besides the parties involved as defined above, everybody else from the Internet are able to access GIAC Enterprise web site to see the publicly available information and also communicate using email.

Servers Required

Analyzing from the access requirements required by each party, protocols and services needed can be determined, and then further determine software and hardware components need to be provided.

- **Web Server** – host name *giac-web*
  Web Server with Microsoft IIS 5.0 running on Windows 2000 Server, Service Pack 3 is used to provide both HTTP and HTTPS services.
  HTTP is used for publicly available web site, while HTTPS is used for web sites for customers and partners to access.
  This Web Server will also initiate communication with database server, to retrieve or save information from and to the database. These accesses to the database are required for customers' and partners' transactions.
  The web server is installed as stand alone, not as part of the Windows domain. This will separate user accounts information from those in the domain, which make it more secure so if there is compromise on the user account, it will only affected this server.

- **Mail Server** – host name *giac-mail*
  Mail Server with Microsoft Exchange 2000 Server, Service Pack 2, running on Windows 2000 Server, Service Pack 3, is used to provide external and internal email communication.
  SMTP is used for email transfer with other mail servers in the Internet, while Microsoft RPC protocol is used for internal email communication with the email clients. All of the users will be using Microsoft Outlook 2000 as their email client.
  Microsoft Exchange 2000 Server must be installed on Windows 2000 Server that is a member of the Windows domain running Active Directory.
  There are few ports being used by this server to communicate with the domain controllers. Reference for these ports is taken from Microsoft Knowledge Base article, Exchange 2000 Windows 2000 Connectivity Through Firewalls[1].

[1] http://support.microsoft.com/default.aspx?scid=KB;en-us;q280132

The following table explained the ports used:

Port	Transport	Description
53	TCP/UDP	DNS
88	TCP/UDP	Kerberos authentication
123	UDP	Windows Time Synchronization Protocol (NTP)
135	TCP	EndPoint Mapper
389	TCP/UDP	Lightweight Directory Access Protocol (LDAP)
445	TCP	Server Message Block (SMB)
3268	TCP	LDAP to Global Catalog Server
1025	TCP/UDP	Customized port for Active Directory logon and directory replication interface, following the instruction in the reference

In accepting connection from the Microsoft Outlook 2000 as the client, the server is using Microsoft RPC protocol, with some additional configured ports, referring to Microsoft Knowledge Base article, Exchange 2000 Static Port Mappings[2].

.

Port	Transport	Description
135	TCP	EndPoint Mapper
1026	TCP	Microsoft Exchange SA RFR Interface
1027	TCP	Microsoft Exchange Directory NSPI Proxy Interface
1028	TCP	Microsoft Exchange Information Store Interface

TCP ports 1026, 1027 and 1028 from the table above are customized ports.

- **Database Server** – host name *giac-db*
  Database Server with Microsoft SQL Server 2000 running on Windows 2000 Server, Service Pack 3, is used for hosting the transactions data.
  SQL Server protocol, which running over TCP port 1433 is used for the communication with this server.
  Database Server will accept connections in two forms, by which both are using SQL Server protocol:
  - Connections from Web Server, for transactions occur through web interface, which are from customers and partners.
  - Connections from Database Applications, for transactions from internal employees, including transactions done for purchases to suppliers, inserted manually using the application, as well as transactions by mobile employees and teleworkers through VPN connection.

  Similar as the Web Server, since there is no necessity for this Database Server to be the member of the Windows domain, it is installed as stand alone server. User accounts in this server will be separated from the rest of the machines.

[2] http://support.microsoft.com/default.aspx?scid=kb;en-us;270836

Authentication and authorization of users accessing the database will be done by the database application.

- **Internal Servers** – host names *giac-svr1* and *giac-svr2*
  There are two Windows 2000 Server, Service Pack 3, as Internal Servers, both as Domain Controllers running Active Directory. This will provide redundancy, since every workstation will be configured as member of the Windows domain, which will rely on the availability of the Domain Controller.
  Since they are configured as Domain Controllers, both machines are required to run DNS Servers. Every member of the Windows domain will be configured to point to these DNS Servers. Global Catalog Server is configured for both servers, to provide redundancy.
  Domain controllers which hosting Global Catalog Server, will require additional configuration to allow Microsoft Outlook connection to them over static port, with reference from Microsoft Knowledge Base article, How to Configure a Global Catalog Server to Use a Specific Port When Servicing MAPI Clients[3].

Port	Transport	Description
1029	TCP	Name Service Provider Interface (NSPI)

The port listed in the table is customized port after editing the registry.

All of the workstations, which are using Windows 2000 Professional, as members of the Windows domain, will need to connect to these two domain controllers, includes those which connecting through VPN tunnel.
Few ports are required on these domain controllers, for domain connections, as described in the Microsoft Knowledge Base article, How to Configure a Firewall for Domains and Trusts[4].

Port	Transport	Description
53	TCP/UDP	DNS
88	TCP/UDP	Kerberos authentication
123	UDP	Windows Time Synchronization Protocol
135	TCP	EndPoint Mapper
389	TCP/UDP	Lightweight Directory Access Protocol (LDAP)
445	TCP	Server Message Block (SMB)
3268	TCP	LDAP for Global Catalog Server

Windows Time Protocol, which is using UDP port 123 is used to synchronized time of the domain members to the domain controllers.
Both domain controllers are also configured to run DHCP to assigned IP addresses to workstations in the internal network.

[3] http://support.microsoft.com/default.aspx?scid=kb;EN-US;298369
[4] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q179442&gssnb=1

Both also will be used as a file server and print server, communicating using SMB over TCP/IP using TCP port 445. Users will be able to save, retrieve and share files in this server, as well as send printing jobs.

Besides the main services above, several other services are required as complementary.

- **DNS Service**
  Although both domain controllers in the internal network are running DNS servers, they are only to be used for internal communication with the Windows domain members.
  If there are requests for external Internet names, these DNS servers will forward the request to another DNS Server.
  Split DNS Servers available in the firewall will be used to receive the forwarded requests from the domain controllers.
  This Split DNS will have two parts, Internal and External. DNS servers on the domain controllers will forward their request to the Internal part of Split DNS. It will then forward to the External part for non-authoritative queries. The External part will be the one who communicate with other DNS servers in the Internet to get the results.
  To increase the performance of getting the query results, External DNS will be configured to point to ISP DNS Servers as forwarders.
  The External part of Split DNS will act as Primary External DNS Server, which hosting the GIAC Enterprise domain, *giac.com*. There is a Secondary External DNS Server hosted at the ISP, which perform zone transfer to the Primary.
  The use of Split DNS on the firewall will increase the level of security for DNS infrastructure. This is because it sits on the firewall host, which has a better security than normal servers.

- **VPN Service**
  This service will also be run by the firewall, which has VPN functionality integrated with it.
  It is using IPSec based VPN to encapsulate the data, to be used by mobile employees and teleworkers. Protocols used for the VPN are Internet Key Exchange (IKE) for key exchange (UDP port 500) and Encapsulating Security Payload (ESP) protocol of IPSec for data encryption (IP protocol 50).
  These users will need to install VPN clients in their workstations, then connecting to the firewall using VPN tunnel to get into the internal network. CyberGuard VPN Client will be used for this purpose.
  Access to the database, email, files and Windows domain are required for them.

- **Anti Virus Server** – host name *giac-avs*
  To protect the network from virus, an Anti Virus protection is implemented at the gateway (firewall). Network traffic, which are HTTP, FTP and SMTP, passing the firewall will be directed for virus scanning first before they allowed to leave or to enter the network.

F-Secure Anti Virus for Firewall is used for this purpose, installed on Windows 2000 Server, Service Pack 3.
It will communicate with firewall using Generic CVP (Content Vectoring Protocol). TCP port 18181 is used for this communication.

- **Log Server** – host name *giac-log*
  This server is used to consolidate logs from router and firewall. It is running Kiwi Syslog server to gather logs from both of the devices through Syslog protocol on UDP port 514. The server is running on Windows 2000 Server, Service Pack 3, which is installed as stand alone server.

Protocols required

The tables below summarize the access requirements of the network with protocols involved.

Outbound to Internet

Service		Usage	Direction	Description
80	TCP	HTTP	Internal users to Internet	Web access
443	TCP	HTTPS	Internal users to Internet	Web access, SSL secured connections
21	TCP	FTP	Internal users to Internet	FTP command port
20	TCP	FTP	Internal users to Internet	FTP data port
25	TCP	SMTP	giac-mail to Internet	SMTP transfer to other mail servers in the Internet
53	UDP	DNS	External DNS server (on the firewall) to Internet	DNS queries to other DNS servers in the Internet
53	TCP	DNS	External DNS server (on the firewall) to Internet	DNS queries, large queries, to other DNS servers in the Internet
80	TCP	HTTP	giac-avs to Internet	giac-avs to get virus signature update from Internet

Inbound from Internet

Service		Usage	Direction	Description
80	TCP	HTTP	Internet to giac-web	Web access
443	TCP	HTTPS	Internet to giac-web	Web access, SSL secured connections, for registered users (customers and partners)
25	TCP	SMTP	Internet to giac-mail	SMTP transfer from other mail servers in the Internet

53	UDP	DNS	Internet to External DNS server (on the firewall)	DNS queries for giac.com
53	TCP	DNS	Internet to External DNS server (on the firewall)	DNS queries, large queries, for giac.com
53	TCP	DNS	Secondary DNS server to External DNS server (on the firewall)	Zone transfer from Secondary DNS server in the ISP

Inbound from VPN tunnel

Service		Usage	Direction	Description
1433	TCP	SQL Server	VPN users to giac-db	Database application connection
135	TCP	RPC	VPN users to giac-mail	Microsoft Outlook connection to the Microsoft Exchange Server
1026	TCP	RPC		
1027	TCP	RPC		
1028	TCP	RPC		
1029	TCP	Global Catalog	VPN users to Domain Controllers (giac-svr1 and giac-svr2)	
53	TCP	DNS	VPN users to Domain Controllers (giac-svr1 and giac-svr2)	Connection to domain controllers, including authentication and file sharing
53	UDP	DNS		
88	TCP	Kerberos		
88	UDP	Kerberos		
123	UDP	Time Protocol		
135	TCP	RPC		
389	TCP	LDAP		
389	UDP	LDAP		
445	TCP	SMB		
3268	TCP	Global Catalog		

Internal traffic – Internal users to servers

Service		Usage	Direction	Description
80	TCP	HTTP	Internal users to giac-web	Web connection
443	TCP	HTTPS		
1433	TCP	SQL Server	Internal users to giac-db	Database application connection
135	TCP	RPC	Internal users to giac-mail	Microsoft Outlook connection to the Microsoft Exchange Server
1026	TCP	RPC		
1027	TCP	RPC		

1028	TCP	RPC		
1029	TCP	Global Catalog	Internal users to Domain Controllers (giac-svr1 and giac-svr2)	
53	TCP	DNS	Internal users to Domain Controllers (giac-svr1 and giac-svr2)	Connection to domain controllers, including authentication and file sharing
53	UDP	DNS		
88	TCP	Kerberos		
88	UDP	Kerberos		
123	UDP	Time Protocol		
135	TCP	RPC		
389	TCP	LDAP		
389	UDP	LDAP		
445	TCP	SMB		
3268	TCP	Global Catalog		

Internal traffic – Servers to servers

Service		Usage	Direction	Description
53	TCP	DNS	giac-mail to Domain Controllers (giac-svr1 and giac-svr2)	Required connections for Microsoft Exchange 2000 to Domain Controllers
53	UDP	DNS		
88	TCP	Kerberos		
88	UDP	Kerberos		
123	UDP	Time Protocol		
135	TCP	RPC		
389	TCP	LDAP		
389	UDP	LDAP		
445	TCP	SMB		
3268	TCP	Global Catalog		
1025	TCP	Active Directory Logon		
1433	TCP	SQL Server	giac-web to giac-db	Web server save and retrieve transaction to and from Database server
53	TCP	DNS	Domain Controllers (giac-svr1 and giac-svr2) to firewall	Request forwarding to DNS Server running in the firewall
53	UDP	DNS		
18181	TCP	CVP	Firewall to giac-avs	CVP communication between Firewall and Anti Virus Server

514	UDP	Syslog	Firewall and Router to giac-log	Firewall and Router sending logs to giac-log

VPN traffic

Service		Usage	Direction	Description
500	UDP	IKE	VPN Hosts to VPN Gateway (on the firewall)	VPN clients connecting to the VPN Gateway
50	IP	ESP		
500	UDP	IKE	VPN Gateway (on the firewall) to VPN Hosts	VPN clients connecting to the VPN Gateway
50	IP	ESP		

Perimeter Defenses

The design of the network is making use of two main components for perimeter defense, border router and firewall/vpn.

Border Router

This border router will serve as the outer gateway between GIAC Enterprise network and Internet.

Cisco 1720 series router, running Cisco IOS 12.2 will be used for this purpose. This router is an entry class router, which should be sufficient enough to be used as a start. Performance will need to be monitored as the company grow and getting more traffic which required upgrade of router.

The router has two interfaces, which are serial0, connected to the leased line to the Internet, and fastethernet0 connected to the GIAC Enterprise network.
The router mainly performs routing function for the network, with additionally access list applied to perform egress and ingress filtering.

Firewall/VPN

Firewall as the gateway between internal and external network of GIAC Enterprise, perform filtering of traffic in and out of those networks and segregating the network into several segments. It also serves as VPN gateway, terminating the VPN connections from VPN clients. CyberGuard KnightStar 2U firewall/VPN appliance, with UnixWare version 5.0 PSU 2 firewall software will be used for this purpose.

CyberGuard firewall is a hybrid architecture firewall, which perform traffic filtering using combination of stateful packet filtering and proxy. This architecture will be useful as for

some traffic like HTTP, HTTPS and SMTP can be filtered using strong application proxies, which allow a more granular control over the traffic up to the application layer. Other types of traffic where specific proxy for them is not available or is not preferred will use stateful packet filtering.

CyberGuard firewall provides integrated operating system together with the firewall software, which eliminates the needs of hardening the operating system separately as well as maintaining different patches for the OS and the firewall. The OS is already hardened by design, which certified under NSA Orange Book certification at B1 level. Both the OS and the firewall are maintained together by one vendor (CyberGuard) only. CyberGuard firewall is also certified under Common Criteria at EAL 4. These certifications will ensure that the firewall has certain level of security tested and verified.

Besides main firewall function, it provides and will also run Split DNS services, as well as Network Address Translations.

As a VPN gateway, all VPN connection from the VPN clients will be terminated at the firewall end, and in this configuration, the firewall will also performing filtering of traffic coming from VPN tunnel.

CyberGuard KnightStar by default comes with 5 Fast Ethernet interfaces, formed by 1 onboard interface on the motherboard and 4 interfaces under 1 quad card. With the design consideration and future expansion taken into account, 1 other quad card, consists of 4 Fast Ethernet interfaces, is added. Total of 9 interfaces are available in the firewall.

Security Architecture Design

To cover all access requirements as well as providing the optimum security for the network, GIAC Enterprise's network is designed as shown in the following network diagram (Figure 1).

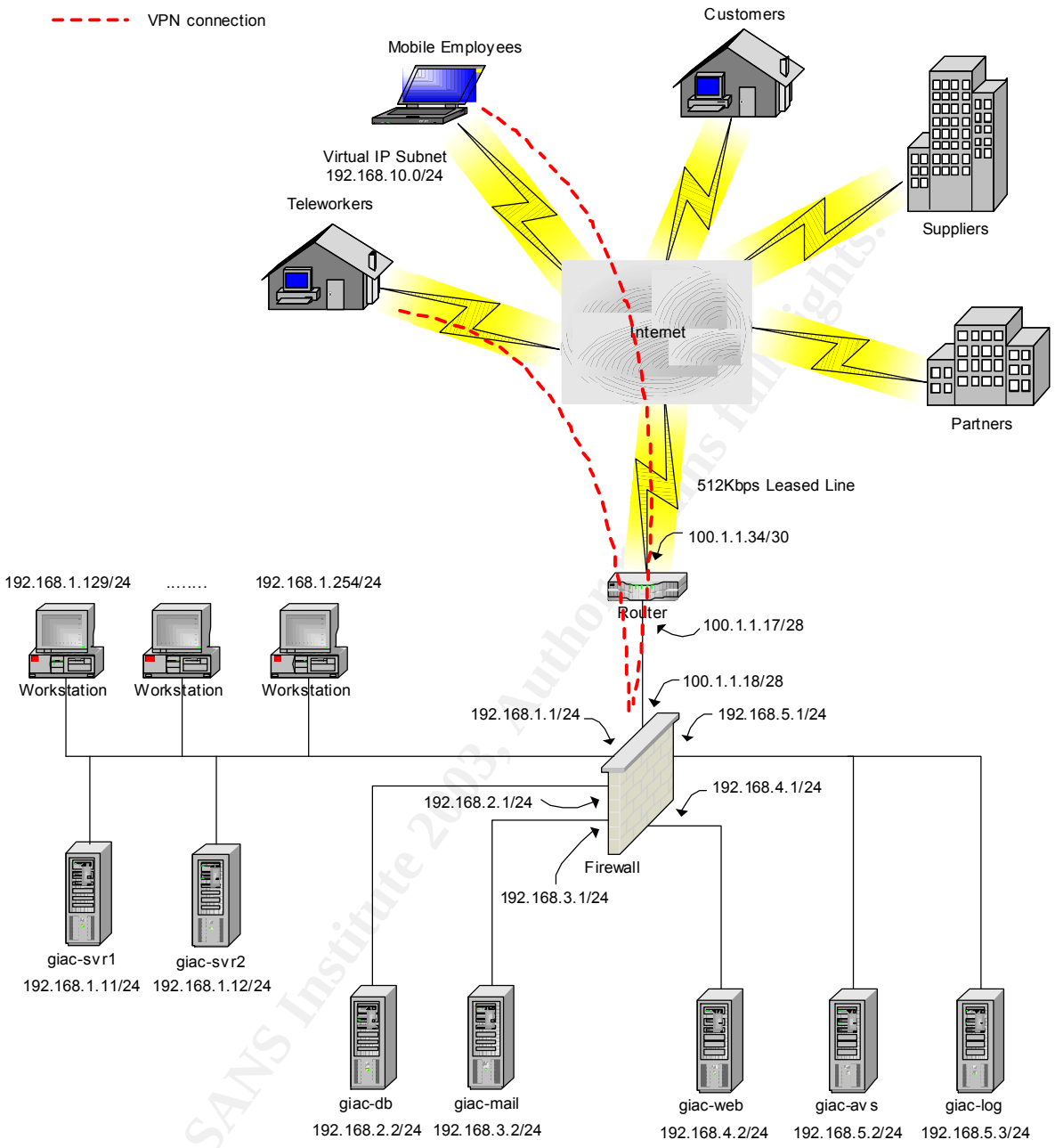

Figure 1: GIAC Enterprise Network Design

As seen in the diagram above, the network is separated into six segments by the Firewall. Six interfaces available on the firewall are utilized to separate the network, with 3 other interfaces left unused.
The concept of the design is that, as much as possible isolate and protect important services from others, meaning that access to that particular services must be through filtering gateways (firewall and/or router). In this design, the firewall is playing an important role in controlling access among the components that it separates.

Second layer firewall is not required at least not at this stage, since the protection can be achieved by separate the services in different interfaces.

IP addressing schemes of the network segments are shown in the table below.

Segment Name	Segment Addresses
EXTERNAL	100.1.1.16/28
INTERNAL1	192.168.1.0/24
INTERNAL2	192.168.2.0/24
SRVNET1	192.168.3.0/24
SRVNET2	192.168.4.0/24
SRVNET3	192.168.5.0/24

Firewall interfaces are configured with IP addresses as can be seen in the diagram above and details as follows. Interfaces naming are following what CyberGuard is using.

Interface Name	Type	IP Address
dec0	External	100.1.1.18/28
dec1	Internal	192.168.1.1/24
dec2	Internal	192.168.2.1/24
dec3	Internal	192.168.3.1/24
dec4	Internal	192.168.4.1/24
dec5	Internal	192.168.5.1/24

Firewall performs Network Address Translation for internal network addresses to be able to communicate with other hosts in the Internet.

External Address	Internal Address	NAT Type	Description
100.1.1.18	All internal addresses	Dynamic	Many to one translation for internal hosts to make outgoing connections, using firewall dec0 interface address
100.1.1.19	192.168.3.2	Static	Address translation for giac-mail
100.1.1.20	192.168.4.2	Static	Address translation for giac-web
100.1.1.21	192.168.1.12	Static	Address translation for giac-log

Dynamic NAT allows internal network addresses to be translated to public address of the firewall interface, so that they can communicate with hosts in the Internet.

Static NAT, which one to one translation, will allow certain hosts to be contactable from the Internet. In this case giac-mail and giac-web, need to be reachable from the Internet, according to their function. While giac-svr2, is used as Syslog server, to receive logs from the router, which sits on the EXTERNAL segment, so it also has to be reachable from there, which is why it is translated.

Assignment 2 – Security Policy and Tutorial

Border Router Security Policy

Security policy for the border router will consist of two parts, network traffic filtering passing through the router and security of the router itself.

Router Static Filtering

The border router, besides its main function to provide routing function for the network, also configured to perform simple static filtering of network traffic. Simple filtering here is referenced to ingress and egress filtering using Extended Access List provided by Cisco IOS. This is done to keep the router to effectively perform what it can do best, which is routing, and not overload it with other functions. Besides that, stronger filtering can be done better by the firewall sitting behind it.
By performing this filtering, the border router will help in keeping totally unwanted traffic to exit or enter the network.

The router performs the filtering on a per interface basis. Different set of filter rules will need to be defined for each interface used. Traffic will be filtered in the inbound direction of that particular interface, as this will save the router resources for processing unwanted traffic. Filters will be read on top to bottom sequence, whichever match first will be used.
There are two parts of filtering being done on the router:

- Ingress filtering
  Filtering traffic coming to the network from the Internet, being done at the serial interface (serial0) of the router, make use of Extended Access List.
- Egress filtering
  Filtering traffic leaving the network to the Internet, being done at the Ethernet interface (fastethernet0) of the router, make use of Extended Access List.

With reference from the network diagram and access requirements, type of traffic required to pass the router can be determined and then filtering policy of router is defined accordingly. Need to also remember that the router is performing static packet filtering, in which for each connection, two directions of traffic must be considered. Referring to access requirements of the network, filtering over traffic passing through the router will be done for:

- Outbound to Internet

- Inbound from Internet
- VPN traffic

There are three components behind the router that need to communicate with Internet either outbound or inbound, represented by their public IP addresses, which are:

- Firewall dec0 interface address, 100.1.1.18
- *giac-mail*, translated address by firewall, 100.1.1.19
- *giac-web*, translated address by firewall, 100.1.1.20

Firewall (in this case using its dec0 address, 100.1.1.18) is translating addresses of internal hosts (Dynamic NAT) that need to communicate outbound with Internet. The other function carried out using this address is as VPN Gateway. VPN hosts/clients will be contacting this address to setup the VPN tunnel. External DNS Server on the Firewall is also using this address, so DNS communication is also expected to happen to and from this address. Characteristics of traffic send to and receive from Internet by the firewall dec0 address is explained in the following table.

Traffic Type	Outgoing Port(s)	Incoming Port(s)
Outbound HTTP	80/TCP	1024-65535/TCP
Outbound HTTPS	443/TCP	1024-65535/TCP
Outbound FTP	21/TCP, 20/TCP	1024-65535/TCP
Outbound DNS	53/TCP, 53/UDP	53/TCP, 53/UDP
Inbound DNS	53/TCP, 53/UDP	53/TCP, 53/UDP
Outbound VPN	500/UDP, IP protocol 50	500/UDP, IP protocol 50
Inbound VPN	500/UDP, IP protocol 50	500/UDP, IP protocol 50

giac-mail, communicating with Internet using IP address 100.1.1.19, translated by the firewall. Characteristic of the traffic for this IP address is shown below.

Traffic Type	Outgoing Port(s)	Incoming Port(s)
Outbound SMTP	25/TCP	1024-65535/TCP
Inbound SMTP	1024-65535/TCP	25/TCP

giac-web, communicating with Internet using IP address 100.1.1.20, translated by the firewall, Characteristic of the traffic for this IP address is shown below.

Traffic Type	Outgoing Port(s)	Incoming Port(s)
Inbound HTTP	1024-65535/TCP	80/TCP
Inbound HTTPS	1024-65535/TCP	443/TCP

Egress Filtering

Firstly, egress filtering is done to block traffic to addresses that not suppose to exist in the Internet[5], as follows:

- Deny traffic to historical broadcast addresses, 0.0.0.0/8
- Deny traffic to private addresses, 10.0.0.0/8
- Deny traffic to loopback address, 127.0.0.0/8
- Deny traffic to link local networks, 169.254.0.0/16
- Deny traffic to private addresses, 172.16.0.0/12
- Deny traffic to TEST-NET, 192.0.2.0/24
- Deny traffic to private addresses, 192.168.0.0/16
- Deny traffic to Class D multicast addresses, 224.0.0.0/4
- Deny traffic to Class E reserved addresses, 240.0.0.0/5
- Deny traffic to unallocated addresses, 248.0.0.0/5
- Deny traffic to broadcast address, 255.255.255.255/32

Outgoing traffic to Internet coming from the three defined addresses of the network above and specific ports required are the only traffic allowed to leave the network. This will reduce the chances of other undefined addresses in the network of being used, in the case of somebody add illegal machine attach to the network, and connect to the Internet using the other available addresses.
It will also help in limiting the ports going out to Internet, reducing the chances of use of unauthorized protocols.
As this filters are only static filtering, a lot of numbers of ports still need to be opened, so it only help in minimizing traffic that can go out to Internet.
As the last rule, everything else that not defined will be dropped, and log packets hitting this rule.
In summary, the rules are:

- Permit traffic from firewall dec0 address, 100.1.1.18, destination TCP port 20
- Permit traffic from firewall dec0 address, 100.1.1.18, destination TCP port 21
- Permit traffic from firewall dec0 address, 100.1.1.18, destination TCP and UDP port 53
- Permit traffic from firewall dec0 address, 100.1.1.18, destination TCP port 80
- Permit traffic from firewall dec0 address, 100.1.1.18, destination TCP port 443
- Permit traffic from firewall dec0 address, 100.1.1.18, destination UDP port 500
- Permit traffic from firewall dec0 address, 100.1.1.18, destination IP Protocol 50
- Permit traffic from giac-mail address, 100.1.1.19, destination TCP port 25
- Permit traffic from giac-mail address, 100.1.1.19, destination TCP ports greater than 1023
- Permit traffic from giac-web address, 100.1.1.20, destination TCP ports greater than 1023
- Deny everything else and log.

[5] Reference from US DoE CIAC, http://www.ciac.org/ciac/bulletins/k-032.shtml

The complete policy of the rules using Cisco IOS Extended Access List and its format, as follows:

```
access-list 100 deny ip any 0.0.0.0 0.255.255.255 log
access-list 100 deny ip any 10.0.0.0 0.255.255.255 log
access-list 100 deny ip any 127.0.0.0 0.255.255.255 log
access-list 100 deny ip any 169.254.0.0 0.0.255.255 log
access-list 100 deny ip any 172.16.0.0 0.15.255.255 log
access-list 100 deny ip any 192.0.2.0 0.0.0.255 log
access-list 100 deny ip any 192.168.0.0 0.0.0.255 log
access-list 100 deny ip any 224.0.0.0 15.255.255.255 log
access-list 100 deny ip any 240.0.0.0 7.255.255.255 log
access-list 100 deny ip any 248.0.0.0 7.255.255.255 log
access-list 100 deny ip any 255.255.255.255 0.0.0.0 log
access-list 100 permit tcp host 100.1.1.18 any eq 20
access-list 100 permit tcp host 100.1.1.18 any eq 21
access-list 100 permit tcp host 100.1.1.18 any eq 53
access-list 100 permit udp host 100.1.1.18 any eq 53
access-list 100 permit tcp host 100.1.1.18 any eq 80
access-list 100 permit tcp host 100.1.1.18 any eq 443
access-list 100 permit udp host 100.1.1.18 any eq 500
access-list 100 permit 50 host 100.1.1.18 any
access-list 100 permit tcp host 100.1.1.19 any eq 25
access-list 100 permit tcp host 100.1.1.19 any gt 1023
access-list 100 permit tcp host 100.1.1.20 any gt 1023
access-list 100 deny any any log
```

Ingress Filtering

Ingress filtering is set first to block unwanted addresses or not suppose to exist addresses in the Internet to come to the network[6], as these will be part of somebody try to spoof those addresses, and waste the network resources.
Those rules are as follows:

- Deny traffic from historical broadcast addresses, 0.0.0.0/8
- Deny traffic from private addresses, 10.0.0.0/8
- Deny traffic from loopback address, 127.0.0.0/8
- Deny traffic from link local networks, 169.254.0.0/16
- Deny traffic from private addresses, 172.16.0.0/12
- Deny traffic from TEST-NET, 192.0.2.0/24
- Deny traffic from private addresses, 192.168.0.0/16
- Deny traffic from Class D multicast addresses, 224.0.0.0/4
- Deny traffic from Class E reserved addresses, 240.0.0.0/5
- Deny traffic from unallocated addresses, 248.0.0.0/5
- Deny traffic from broadcast address, 255.255.255.255/32
- Deny traffic from own addresses, 100.1.1.16/28

[6] Reference from US DoE CIAC, http://www.ciac.org/ciac/bulletins/k-032.shtml

Incoming traffic from Internet should only be directed for the three addresses existed in the network, with specific ports in use. Other than to those addresses, they should be dropped, because those other addresses or ports are not in use, or being used illegally. Similar as egress filtering, this is also static filtering in which both directions of the traffic should be considered.
The last rule, is deny everything else that not match the rules, and log packets hitting this rule.
In summary:

- Permit traffic to firewall dec0 address, 100.1.1.18, destination TCP ports greater than 1023
- Permit traffic to firewall dec0 address, 100.1.1.18, destination TCP and UDP ports 53
- Permit traffic to firewall dec0 address, 100.1.1.18, destination UDP port 500
- Permit traffic to firewall dec0 address, 100.1.1.18, destination IP Protocol 50
- Permit traffic to giac-mail address, 100.1.1.19, destination TCP ports greater than 1023
- Permit traffic to giac-mail address, 100.1.1.19, destination TCP port 25
- Permit traffic to giac-web address, 100.1.1.20, destination TCP port 80
- Permit traffic to giac-web address, 100.1.1.20, destination TCP port 443
- Deny everything else and log

Policy in the Cisco IOS Extended Access List format:

```
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny ip 192.168.0.0 0.0.0.255 any log
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
access-list 101 deny ip 240.0.0.0 7.255.255.255 any log
access-list 101 deny ip 248.0.0.0 7.255.255.255 any log
access-list 101 deny ip 255.255.255.255 0.0.0.0 any log
access-list 101 deny ip 100.1.1.16 0.0.0.15 any log
access-list 101 permit tcp any host 100.1.1.18 gt 1023
access-list 101 permit tcp any host 100.1.1.18 eq 53
access-list 101 permit udp any host 100.1.1.18 eq 53
access-list 101 permit udp host 100.1.1.18 any eq 500
access-list 101 permit 50 host 100.1.1.18
access-list 101 permit tcp host 100.1.1.19 any gt 1023
access-list 101 permit tcp host 100.1.1.19 any eq 25
access-list 101 permit tcp host 100.1.1.20 any eq 80
access-list 101 permit tcp host 100.1.1.20 any eq 443
access-list 101 deny any any log
```

From both the egress and ingress filtering rules, can be seen that on the sequence of the rules, a set of deny rules is being put first before the permit rules. This will enable the deny rules to block off the unnecessary traffic going to or coming in from unwanted IP addresses first, although that traffic may use the correct protocols. The set of permit

rules then will determine what are the correct IP addresses and protocols should be used by the network traffic. And lastly, if there are still traffic not met by the above sets of filters, it will be drop by the last rule.

Securing The Router

While the router is able to do filtering to protect the network, actions should also be taken to protect and secure the router itself.

Disabling Unneeded Services

The router is equipped with few services for different purposes and functions, but not all of them are required and running them could pose security risks. These unneeded services will be disabled.

- **Disabling CDP**
  CDP (Cisco Discovery Protocol), which used to automatically detect directly connected Cisco routers/switches should be disabled, as it would reveal some information about the router such as model number and software version.
  Global configuration command used:
  ```
  no cdp run
  ```

- **Disabling HTTP Server**
  HTTP server is used to allow router management and configuration through HTTP. It is not used here and will be disabled. This is actually done by default.
  Global configuration command used:
  ```
  no ip http server
  ```

- **Disabling Bootp Server**
  Bootp server, which intended to allow other Cisco devices to get the IOS software from the router over the network, is not used and will be disabled.
  Global configuration command used:
  ```
  no ip bootp server
  ```

- **Disabling Configuration Auto-Loading**
  Cisco routers have a feature that enables them to load configuration from the network. This will not be allowed, as the router will only need to load the configuration from its local memory. This is disabled by default.
  Global configuration command used:
  ```
  no service config
  ```

- **Disabling Source Routing**
  Source routing, allowing IP packets to determine its own routes, is not needed and should not be allowed. All traffic should use normal network routing. The router

should not process packets with source route, so the support for this will be disabled.
Global configuration command used:

```
no ip source route
```

- **Disabling TCP and UDP Small Services**
  TCP and UDP small servers, which following the protocol standards should exist in hosts, are not required in the router. The use of these services could reveal information on the router to outsiders. They are disabled by default.
  Global configuration command used:

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

- **Disabling Finger**
  Finger service is used to query the router of users logging in to the router. The query request can come from remote source, which is not desirable. This feature is not required and is disabled by default.
  Global configuration commands used:

```
no service finger
no ip finger
```

- **Disabling Proxy ARP**
  Proxy ARP is only needed when the router is segmenting two LAN interfaces. Because it is not, then the feature will be disabled. Disabling this will be done on each interface, serial0 and fastethernet0.
  Interface configuration command used:

```
no ip proxy-arp
```

- **Disabling IP Directed Broadcast**
  Broadcast should only be allowed on each individual subnet, and not going across to others, as in directed broadcast. The router should not forward these packets. Each interface will be configured to disable this.
  Interface configuration command used:

```
no ip directed-broadcast
```

- **Disabling ICMP Unreachable**
  The router functionality of sending ICMP unreachable should be disabled, as it will give information that certain hosts do not exist. This could help attacker in performing network mapping. Each interface will be configured to disable this.
  Interface configuration command used:

```
no ip unreachable
```

- **Disabling ICMP Redirect**
  ICMP redirect messages will be sent by router as a response for certain routed packets. This will not be required for normal network traffic. Each interface will be configured to disable this.
  Interface configuration command used:

```
no ip unreachable
```

- **Disabling ICMP Mask Reply**
  ICMP mask reply will be sent by router, containing the router interface subnet mask, in response to ICMP mask request. This should not be allowed, and will be disabled on each interface.
  Interface configuration command used:
  ```
  no ip mask-reply
  ```

- **Disabling NTP**
  The router will use its own internal clock as time reference. NTP service is not required and will be disabled on each interface. By default it is already disabled.
  Interface configuration command used:
  ```
  ntp disable
  ```

- **Disabling SNMP**
  SNMP for router management will not be used, so this service is disabled. By default it is already disabled.
  Global configuration command used:
  ```
  no snmp server
  ```

Controlling Access to Router

Due to the fact that the router has an important role as the gateway between the network and Internet, access to device should be limited. This include of assigning to only authorized persons, with certain methods and from certain location only.

- **Enabling access methods**
  Cisco routers support few methods of accessing them, but only console and telnet will be required.
  - Enabling console
    Console is enabled by default, and will be the method of accessing router locally and physically. Console configurations will be done using line configuration at con 0.

  - Enabling telnet
    Telnet is a method used to access the router from network, so remotely the administrator can control the router. Telnet access is using virtual terminal (vty) line.
    Configuration lines:
    ```
    vty 0 4
      transport input telnet
    ```

- **Enforcing authentication**
  Assigning access to the authorized persons will be done by enforcing authentication when users trying to log into the router.

- Defining local user names and passwords
  Few pairs of user names and passwords are defined in the router for few administrators allowed to access the router.
  Global configuration commands used:

```
username admin1 password [password1]
username admin2 password [password2]
```

- Enforcing authentication to console access
  When user accessing the router through console, he will be asked user name and password. Only with the correct information, then he will be granted access.
  Line configuration commands:

```
line con 0
  login local
```

- Enforcing authentication to telnet access
  Similar case here, user name and password will be asked from user to access the router.
  Line configuration commands:

```
vty 0 4
  login local
```

- **Passwords**
  Passwords, as one element of authentication also need to be kept secret and difficult to guess and read.
  - Basic protection
    Password should not be saved and displayed in clear, but at least should have some form of encryption. The below command should be used for password protection, although it is only give minimum protection using simple Vigenere cipher.
    Global configuration command:

```
service password-encryption
```

  - Enable secret
    In order to enter privilege mode, which have more rights in performing administrative tasks on the router, additional password should be requested. This will form additional protection of access. Enable secret command should be use for this purpose. It is using MD5 for password hashing.
    Global configuration command:

```
enable secret 5 [password]
```

- **Filtering access to router**
  Only certain IP address will be allowed to connect to the router for configuration. Administrator is using only *giac-log* to access the router. As the firewall is performing the Static Network Address Translation, router would see its public address, 100.1.1.21. On the router, 100.1.1.21 will be the one allowed to do telnet to it.
  The following line will be added into the fastethernet0 access-list 100 before the last deny rule:

```
access-list 100 permit tcp 100.1.1.21 100.1.1.17 eq 23
```

Logging

The router is configured to send logs to centralized Syslog server, which is *giac-log*. From the router, this server can be reach at IP address 100.1.1.21, which then translated by the firewall to its actual address. Violations against access list, which define with keyword log in each access list line as seen in the access list 100 and 101, will be sent to this Syslog server. Interface status changes and changes to the system configuration will also be sent.
Default logging level to syslog is used, which is informational.
Configuration lines for logging:

```
logging 100.1.1.21
```

Logs being generated by the router will be time-stamped, to provide time information on it. The following is used for generating the time-stamp:

```
service timestamps log datetime localtime show-timezone
```

The complete router configuration can be seen on Appendix A.

Firewall Security Policy

By using the design above and access requirements defined, filtering over traffic passing through the firewall will be done for:

- Outbound to Internet
- Inbound from Internet
- Internal traffic – Internal users to *giac-web*
- Internal traffic – Internal users to *giac-db*
- Internal traffic – Internal users to *giac-mail*
- Internal traffic – *giac-mail* to Domain Controllers (*giac-svr1* and *giac-svr2*)
- Internal traffic – *giac-web* to *giac-db*
- Router to *giac-log*
- Firewall to *giac-log*
- Firewall to *giac-avs*

The firewall, which is CyberGuard, supports both Packet Filtering and Application Proxy, so the filtering policy will be split into using both of the architecture.
As much as possible, Proxy will be used, as it offers more granular control over the IP packets. And the rest of the traffic types, where the proxies for them are not available, will be filtered using stateful/dynamic packet filtering.

Both proxy policy and packet filtering policy has to be defined in the same firewall Packet-Filtering Rules engine. Everything that needs to pass through, to or from the firewall has to be defined in the Packet-Filtering Rules.

Types of actions for the Packet-Filtering Rules are:

- Permit, to allow traffic using dynamic packet filtering
- Proxy, to allow traffic using proxy
- Deny, to deny traffic

Rules inspection sequence is from top to bottom, means which rule met first will be followed.
If same rules created for both packet filtering (permit rules) and proxy, sequence will take precedence.
The last rule in the packet filter is deny for every traffic, which implicitly built in into the engine.

For proxy policy, besides rules definition in the Packet-Filtering Rules, proxy service for the specific type of traffic has to be enabled, in order for the connections to be serviced using proxy. Additional application level filtering for the specific proxy can also be defined after that.

Specifically for proxy, rules definitions in the Packet-Filtering Rules vary based on the direction settings of each proxy enabled.
There are four definitions:

- Inbound To
  This is for proxying traffic from clients to the server in the internal side of the firewall. The clients need to connect explicitly to the firewall address in order to reach the server.
- Inbound Through
  This is for proxying traffic from clients to the server in the internal side of the firewall. The clients transparently use the server addresses to connect to it.
- Outbound To
  This is for proxying traffic from internal to external, with explicitly firewall address need to be used.
- Outbound Through
  This is for proxying traffic from internal to external transparently.

In defining the Packet-Filtering Rules, several definitions for host names and group names are created. This will help in the rules administration in a condition of IP addresses for certain hosts changed, only the host definition need to be changed, not individual rules with the changed IP addresses.

Host definition

Name	IP address
giac-router	100.1.1.17
giac-svr1	192.168.1.11
giac-svr2	192.168.1.12
giac-db	192.168.2.2
giac-mail	192.168.3.2
giac-web	192.168.4.2
giac-avs	192.168.5.2

Group definition

Name	Member
giac-users	192.168.1.128/25
giac-dc	Giac-svr1, giac-svr2

For hosts with Network Address Translation (NAT), the actual IP addresses of the hosts must be used instead of translated addresses, when being defined in the rules.

Proxy filtering policy

Proxies available are limited to certain applications. In this case, traffic types that will be filtered using proxy are:

- FTP, outbound
- HTTP, outbound and inbound
- SMTP, outbound and inbound
- SSL, outbound and inbound

These proxies are servicing all access requirements between GIAC network and Internet, in which this will offer the best security for those accesses.

Filtering using proxy will offer better level of security. Firstly it is intercepting the communication between client and server, so no direct connection between them. The client will communicate first with the firewall then the firewall will open another connection to the server. Secondly, it is performing application level inspection, which done differently according to the application protocol types. This cannot be achieved by using stateful packet filtering.

FTP Proxy Policy

FTP Proxy is used to filter access of internal users when performing ftp connection to Internet. Outbound Through proxy is used, so the users will transparently do their accesses without any changes required on the client side.

FTP Proxy rules in the Packet-Filtering Rules for Outbound Through described below:

Type	Service	Origin	Destination	Option
proxy	ftp/tcp	giac-users	ALL_EXTERNAL	

Several application level inspections are available for FTP Proxy. But the one required is only to enable CVP support so that every FTP connections will be scanned for possible hazardous contents. The FTP proxy will forward traffic to *giac-avs* using CVP connections for content scanning. If there are infected files, the anti virus server will try to disinfect them, but if failed they will be dropped.
Scanning will be done for both directions, files coming in and going out.

The following is the policy for FTP Proxy:

Configuration Options	Settings	Description
Enable CVP	Yes	Enable CVP
CVP Server address	giac-avs	CVP server name/address
CVP Server port	18181	CVP server port to be contacted
Scan inbound	Yes	Scan inbound files
Scan outbound	Yes	Scan outbound files
Disinfect	Yes	Try to disinfect files, if failed then drop

HTTP Proxy Policy

HTTP Proxy is used with Inbound Through for inbound access for Internet users to come to GIAC web site. Inbound Through is used because the clients will be contacting *giac-web* using its own address, which is NAT address. This proxy will protect the web server of direct contact with external clients.
Access by internal users to *giac-web* will also be done using Inbound Through connections. Inbound proxy is used to perform filtering where there are defined servers that it has to protect. It doesn't matter whether the clients coming from external or internal interfaces.

Outbound access by internal users to connect to Internet will be using Outbound Through proxy which transparently proxies the connections. The use of proxy will be very useful to protect internal users from direct connections to Internet. Web is one of the most widely used protocols in the Internet, which also one of the largest source of hazardous contents.

HTTP Proxy rules in Packet-Filtering Rules for Inbound Through:

Type	Service	Origin	Destination	Option
proxy	http/tcp	ALL_EXTERNAL	giac-web	
proxy	http/tcp	giac-users	giac-web	

HTTP Proxy rules for Outbound Through:

Type	Service	Source	Destination	Option
proxy	http/tcp	giac-users	ALL_EXTERNAL	
proxy	http/tcp	giac-avs	ALL_EXTERNAL	

With the Inbound Proxy used, the web server address protected by the proxy has to be defined. Filtering of HTTP commands to the web server, which are post, put and delete, can then be defined, whether to allow or block them.

Another important part is to have the web connection being scanned by the anti virus server using CVP, to allow removal of hazardous content. This can only be achieved if the connection is filtered using HTTP Proxy, and the CVP option is enabled. Scanning should be done for inbound and outbound files, and disinfecting of infected files is preferable.

HTTP Proxy policy is explained below.

Configuration Options	Settings	Description
Web Server Handler	Independent	The server reside outside of the firewall
Enable https throughput	Yes	Enable https:// proxy support
Enable ftp throughput	Yes	Enable ftp:// proxy support
Define Server		
Web Server	giac-web	Web server name/address protected by proxy
Allow post	No	Allow http post commands
Allow put	No	Deny http put commands
Allow delete	No	Deny http delete commands
Enable CVP	Yes	Enable CVP
CVP Server address	giac-avs	CVP server name/address
CVP Server port	18181	CVP server port to be contacted
Scan inbound	Yes	Scan inbound files
Scan outbound	Yes	Scan outbound files
Disinfect	Yes	Try to disinfect files, if failed then drop

SMTP Proxy Policy

SMTP Proxy is enabled for Inbound Through and Outbound Through. SMTP is used for email transfers between *giac-mail* and other SMTP servers in the Internet. SMTP Proxy will intercept connections for both directions, so there is no direct communication between the servers. This will also eliminate the needs of mail relay to secure the connection.

SMTP Proxy rules for Inbound Through:

Type	Service	Source	Destination	Option
proxy	smtp/tcp	ALL_EXTERNAL	giac-mail	

SMTP Proxy rules for Outbound Through:

Type	Service	Source	Destination	Option
proxy	smtp/tcp	giac-mail	ALL_EXTERNAL	

Mail server protected by the proxy should be defined, which is *giac-mail*. The proxy also allowing the use of alias file to map the email users existed in the server, so that if no match for the specific users, the email will be rejected by the firewall. But in this case, this filtering is not being used, so the alias file name will be set to none, and emails will be passed to the mail server.
The domain used by mail server, which is *giac.com*, is set here, so that only emails sent to recipients with email address of that domain being passed to the mail server. This feature will protect the mail server from being used as mail relay for spamming.

Lastly, as emails are considered as popular method of spreading harmful content, scanning against them is recommended and here will be done with CVP, for both directions, inbound and outbound. Disinfecting of files will be tried first if possible.

SMTP Proxy policy defined below:

Configuration Options	Settings	Description
Default Domain Name	giac.com	Default domain used by the outgoing email
Define Server		
Mail server	giac-mail	Mail server name/address protected by proxy
Alias file name	NONE	No alias file
Domains	giac.com	Allowed domain name for recipients
Pass mail for unaliased user	Yes	Pass emails for recipients not listed in the alias file
Enable CVP	Yes	Enable CVP
CVP Server	giac-avs	CVP server name/address

CVP Server port	18181	CVP server port to be contacted
Scan inbound	Yes	Scan inbound files
Scan outbound	Yes	Scan outbound files
Disinfect	Yes	Try to disinfect files, if failed then drop

SSL Proxy Policy

SSL Proxy is enabled for Inbound Through to protect access from Internet to *giac-web*. Similarly, access from internal users is also using this type of proxy.
It is also enabled for Outbound Through for internal users to access through SSL to Internet.

SSL Proxy rules for Inbound Through:

Type	Service	Source	Destination	Option
proxy	https/tcp	ALL_EXTERNAL	giac-web	
proxy	https/tcp	giac-users	giac-web	

SSL Proxy rules for Outbound Through:

Type	Service	Source	Destination	Option
proxy	https/tcp	giac-users	ALL_EXTERNAL	

Since SSL connection is an encrypted connection, what the proxy can inspect on the traffic is very limited to the unencrypted portion. Basically what is being done is to break or intercept the connections, so that there are no direct communication between the client and the server.
Additionally for inbound proxy, server name or address protected by the proxy has to be defined

SSL Proxy policy described below:

Configuration Options	Settings	Description
Web server host	giac-web	Web server protected by SSL Proxy

Packet Filtering Policy

Stateful packet filtering is used to filters traffic among the internal components of the network. Most of the protocols involved here are normally used only for internal communication in the private networks, no proxy are available for them and since they are internal, stateful packet filtering should be sufficient. Besides, stateful or dynamic packet filtering will give better performance for these LAN protocols, which are more resource hungry compare to those Internet traffic.

Packet filtering policy in the Packet-Filtering Rules is described below, according to the access requirements and the network design.

Type	Service	Source	Destination	Option
# Internal users to access giac-db				
permit	1433/tcp	giac-users	giac-db	
# Internal users to access giac-mail				
permit	135/tcp	giac-users	giac-mail	
permit	1026/tcp	giac-users	giac-mail	
permit	1027/tcp	giac-users	giac-mail	
permit	1028/tcp	giac-users	giac-mail	
# giac-mail to access domain controllers				
permit	53/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	53/tcp	giac-mail	giac-dc	
permit	88/tcp	giac-mail	giac-dc	
permit	88/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	123/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	135/tcp	giac-mail	giac-dc	
permit	389/tcp	giac-mail	giac-dc	
permit	389/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	445/tcp	giac-mail	giac-dc	
permit	3268/tcp	giac-mail	giac-dc	
permit	1025/tcp	giac-mail	giac-dc	
# giac-web to access giac-db				
permit	1433/tcp	giac-web	giac-db	
# router to send syslog to giac-log				
permit	514/udp	giac-router	giac-log	
# giac-log to perform remote access to router				
permit	23/tcp	giac-log	giac-router	
# CVP rule				
permit	18181/tcp	FIREWALL	giac-avs	

In the packet filtering policy above, can be seen that host names are used instead of their IP addresses. This will be a more efficient approach, as names are easier to remember than addresses, and also if the IP addresses for these host names changed, only one reference inside the host tables need to be changed.

Seen also that in the option field, ENABLE_REPLY is being used for UDP protocols. This option is a feature in the CyberGuard firewall, which used to enable the firewall to track sessions for connectionless protocols, such as UDP. For connection oriented protocols like TCP, it doesn't matter whether this is used or not, because these protocols already have built in functionality in tracking sessions. By default is not turned on, so for TCP traffic it will be left as default, while for UDP traffic it will be turned on.

Exception here is for Syslog, since only one direction of traffic required, from client to syslog server, no ENABLE_REPLY required.

There are two rules in the policy above, which are 53/udp and 53/tcp from *giac-mail* to *giac-dc*, used as DNS communication. These rules need to be specifically permitted, to allow *giac-mail* to communicate with DNS server in the *giac-dc*. Need to remember that *giac-mail* is a Windows domain member, so its name resolution must use DNS servers located in both of the Domain Controllers. This is important, since the firewall itself also serving as DNS servers, but *giac-mail* cannot directly use them as its DNS server.

Additionally, with the Proxies make use of CVP, a rule for firewall to communicate with CVP server (*giac-avs*) is created automatically.

Split DNS

The firewall has the Split DNS feature, which being used for outgoing DNS resolution to Internet as well as hosting the Internet domain for *giac.com*.
Enabling this feature will also involve creating several automatically generated rules in the Packet-Filtering Rules to enable DNS traffic in and out of the network as necessary.

Servers Definition

Two DNS Servers will be activated when Split DNS is enabled. One is External DNS Server or Public Name Server and the other one is Internal DNS Server or Private Name Server.
IP addresses where these servers can be contacted are the addresses of the network interfaces of the Firewall. External network interfaces are used for External DNS Server, while the Internal network interfaces are used for Internal DNS Server. Unless only one interface is available for each server, which interfaces to respond to the DNS requests can be selected.

Type	Interfaces	Host Name
External	100.1.1.18/28	giac-external
Internal	192.168.1.1/24	giac-internal

For external, only one interface is available, so it will be chosen. For internal, there are actually five interfaces, but only one chosen. Host Names here will be used as NS record for name server definition.

The Split DNS architecture is enforcing that the Internal DNS will always forward to External DNS for any request to Internet. Therefore, the forwarder address for the Internal DNS will be the External DNS address 100.1.1.18. Optional for External DNS, forwarder addresses can be configured to other DNS Servers. In this case, ISP DNS Servers will be used.

Limiting the ability of others to do zone transfer to the DNS servers is a security feature that will be used. For External, only Secondary DNS in the ISP will be allowed to do zone transfer. While for Internal, no zone transfer is allowed.

Zones and Hosts Information

Zones need to be defined for domains that the DNS servers are hosting. Two zones have to be created, one for External and one for Internal.

External Zone
On the External Name server, a zone will be created to host *giac.com* domain, where Internet users will refer to for name queries. This zone will be created automatically, since the Firewall is defined to use the *giac.com* as its domain name. Mail server host for mail exchange (MX record) and hosts definitions (A records) will also be defined.

Parameters	Value
Zone Name	giac.com
Type	Primary
Mail Server	mail

Hosts definitions are explained in the table below.

Host Name	IP Address	Description
mail	100.1.1.19/28	Mail server, giac-mail
www	100.1.1.20/28	Web server, giac-web

Whenever requests come for *mail.giac.com* or *www.giac.com*, it will be translated accordingly to the respective IP addresses. Similarly, for request to email addresses with @*giac.com*, it will then be directed to the mail server address.

Internal Zone
Similar as External, the Firewall will create the *giac.com* zone automatically for Internal name server. The Internal name server will not host any hosts or mail server host information. It's only being used to relay the DNS request from DNS servers in the *giac-svr1* and *giac-svr2* to External DNS.

Parameters	Value
Zone Name	giac.com
Type	Primary

Split DNS Rules

Enabling Split DNS will create rules automatically in the Packet-Filtering Rules. These rules will allow external users to contact only external DNS, represented by the external interfaces; internal users to only contact internal DNS.

Type	Service	Source	Destination	Option
permit	domain/tcp	ALL_EXTERNAL	EXTERNAL_INTERFACES	
permit	domain/tcp	EXTERNAL_INTERFACES	ALL_EXTERNAL	
permit	domain/udp	ALL_EXTERNAL	EXTERNAL_INTERFACES	ENABLE_REPLY
permit	domain/udp	EXTERNAL_INTERFACES	ALL_EXTERNAL	ENABLE_REPLY
permit	domain/tcp	ALL_INTERNAL	INTERNAL_INTERFACES	
permit	domain/tcp	INTERNAL_INTERFACES	ALL_INTERNAL	
permit	domain/udp	ALL_INTERNAL	INTERNAL_INTERFACES	ENABLE_REPLY
permit	domain/udp	INTERNAL_INTERFACES	ALL_INTERNAL	ENABLE_REPLY
deny	domain/tcp	EVERYONE	EVERYONE	
deny	domain/udp	EVERYONE	EVERYONE	

Several descriptions of keywords used on the table above:

- ALL_EXTERNAL - hosts on the network(s) connected to the firewall interface(s) labeled External
- EXTERNAL_INTERFACES - firewall interfaces labeled External
- ALL_INTERNAL - hosts on the network(s) connected to the firewall interface(s) labeled Internal.
- INTERNAL_INTERFACES - firewall interfaces labeled Internal
- EVERYONE - all network connected to the firewall and the firewall itself.

Alerts and Activity Logs

Logging or auditing system in the firewall is configured to record activities of traffic passing through the firewall as well as generate alerts if some events happened on the firewall. Two types of logs are used, Alerts and Activity Logs.

Table below explains Alerts to be enabled on the firewall.

Alerts Enabled	Description
Disk partition full	Detecting usage of disk
Failed login attempts	Detecting unsuccessful login attempts
Packet forwarding attacks	Detecting attempts to route inbound packets through different route than usual
Land attacks	Detecting Land attacks
Ping of death attacks	Detecting Ping of death attacks
TCP SYN flood attacks	Detecting TCP SYN flood attacks
IP interface spoofing attempts	Detecting IP spoofing

Network port scan attempts	Detecting network port scan
File transmission blocked	Detecting file blocked by content scanning software
Audit archiving activity	Detecting archiving of logs activities
VPN IKE alert	Detecting issue occur with IKE
VPN IPSec alert	Detecting issue occur with IPSec
VPN Interceptor alert	Detecting issue occur with ESP or AH session

The above alerts will be set to send to:

- File - alert files in the firewall
- Window - alert window in the firewall
- Syslog - syslog daemon in the firewall

Table below explains activity logs enabled on the firewall.

Activity Type	Description
All packets scanned by packet filter	Packets compared against packet-filtering rules
Packets permitted	Packets permitted by the firewall
Packets denied	Packets denied by the firewall
Packets denied because no rule matched	Packets denied because they do not match any rules
Content scanning activity	CVP virus scanning to files
FTP Proxy activity	FTP communication relayed by FTP proxy
HTTP Proxy activity	HTTP communication relayed by HTTP proxy
SMTP Proxy activity	SMTP communication relayed by SMTP proxy
SSL Proxy activity	SSL communication relayed by SSL proxy
VPN IKE activity	Activities associated with IKE
VPN IPSec activity	Activities associated with IKE
VPN Interceptor activity	Activities associated with ESP or AH sessions

The above activity logs will be set to send to:

- File - activity log files in the firewall
- Syslog – sending to Syslog server, *giac-log*, located at 192.168.5.3

With Syslog logging configured, additional rule will be added automatically to the Packet-Filtering Rules for the firewall to send syslog messages to Syslog server, *giac-log*, as follows:

Type	Service	Source	Destination	Option
permit	syslog/udp	FIREWALL	giac-log	

VPN Security Policy

The VPN infrastructure in GIAC Enterprise network is used to interconnect between the main network and the remote employees, including teleworkers and mobile employees, which are using their laptops or home PCs to connect to the GIAC network. It comprises of two components, VPN Gateway and VPN Hosts. VPN Gateway, which is the CyberGuard firewall, will be the endpoint of the VPN at the GIAC network, while VPN Hosts, which are CyberGuard VPN Clients, will be the endpoint of the VPN at the remote employees side.
In order for both sides of the endpoints to communicate each other, compatible policies must be set for both of them. Before establishing the connections, both parties will negotiate on the communication parameters, and only with the same policies set, then they will reach an agreement of policy to be used for data transmission.

General VPN Policy

As mentioned above, to establish communication on both endpoints protected by VPN, both sides must have compatible policy applied for VPN.
Policy for VPN can be divided into four parts: IKE, IPSec, Protected Networks and Filtering Rules.

IKE Policy

Prior to establishing the data transfer using IPSec, Internet Key Exchange (IKE) protocol will be activated first to exchange keys and other parameters for IPSec communication. During the data transfer using IPSec, with the selected time, IKE will also be activated again to do the same thing. The following parameters are used for IKE communications.

Parameters	Value
Pre-shared Secret	xxxxxxxxx
Encryption Algorithm	3DES
Hash Algorithm	SHA1
Diffie-Hellman Group	2
SA Lifetime (seconds)	10800
IKE Mode	Main Mode
PFS Group	2

IPSec Policy

Few parameters for encrypting the communication by IPSec must be agreed between the two endpoints. These parameters are communicated by IKE.

Parameters	Value
SA Mode	Tunnel Mode
Protocol	ESP
Encryption Algorithm	3DES-CBC
Authentication Algorithm	HMAC-SHA1
SA Lifetime (seconds)	28800

Tunnel mode has to be chosen because the VPN type is Gateway to Host, where the gateway is not the end entity of the VPN. While to provide confidentiality of the data transmission, ESP is chosen, because it will encrypt the whole packets.

Protected Networks

With VPN, there are private networks hidden inside the communication between the VPN endpoints. Behind the VPN Gateway, normally there are few private networks, while with VPN Host, only one private network, which is the host itself.
When defining VPN tunnel, these private or protected networks has to be defined, or else it will not be reachable through the tunnel.

Protected networks behind VPN Gateway can be defined based on the access requirements in the previous section:

- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

For VPN Hosts, virtual addresses will be created used as protected network. These addresses are assigned one to each hosts, where one subnet or more can be used depend to the number of VPN users. When communication occurs among hosts through VPN, these virtual addresses are the addresses used to represent the VPN Hosts.
One subnet is assigned for virtual addresses: 192.168.10.0/24

Filtering Rules

With Gateway to Host VPN configuration, the VPN Hosts are exposed to the Internet, and beyond the protection of the perimeter defense of the network. Limiting the traffic that allowed passing through the VPN tunnel to the internal network is one of the way to enforce more control over these hosts. This is can be done on the VPN Gateway, which in this case using Packet-Filtering Rules of the CyberGuard firewall. More on this will be explained on the VPN Gateway policy.

On the VPN Hosts, several policies can be defined for different type of traffic. Normally will be VPN traffic and normal Internet traffic. VPN traffic will be secured using the VPN

tunnels policy, while Internet traffic can be controlled whether to be passed or to be blocked.
When the VPN Hosts are communicating using VPN, other Internet traffic can be blocked so that only pure VPN traffic is active on the hosts. This will increase the level of security.

VPN Gateway Policy

Policy for VPN Gateway on the Firewall will comprise of four parts, IKE Protection Strategy, IPSec Protection Strategy, VPN Secure Channels and VPN Packet-Filtering Rules.

IKE Protection Strategy

This part will determine policy to be used in IKE communication between the Gateway and the Hosts. The policy here will follow the IKE policy defined above.

Parameters	Value
Protection Strategy Name	giac-ike
Encryption Algorithm	3DES
Hash Algorithm	SHA1
Diffie-Hellman Group	2
SA Lifetime (seconds)	10800

IPSec Protection Strategy

This part is determining policy used for encrypting data in IPSec connections, following the IPSec policy above.

Parameters	Value
Protection Strategy Name	giac-ipsec
Encryption Algorithm	3DES-CBC
Authentication Algorithm	HMAC-SHA1
SA Lifetime (seconds)	28800

VPN Secure Channels

This policy will define what type of VPN channels or tunnels will be used, as well as key exchange characteristics.

Channel Information
Only one channel or tunnel will be defined here, with peer type is Host. When Host peer type is used, interface on the Firewall where the Host will connect to it will be used, instead of defining the IP address of that Host. This is because VPN Host can connect to the Gateway from any IP address in the Internet. Key exchange method linked to each tunnel will also be defined here, which in this case is using IKE. IKE protection strategy that will be used is specified here.

Parameters	Value
Channel Name	giac_to_hosts
Peer Type	Host
Interface Name	dec0
Establish Keys Using	IKE
Preshared Secret	xxxxxxxxx
IKE Protection Strategy	giac-ike
IKE Mode	Main Mode
PFS Group	2

Peer Protected Networks
As mentioned above, protected network(s) of the peer need to be defined to establish VPN tunnel communication. From the Gateway point of view, its peer will be the virtual addresses of the Hosts.

Parameters	Value
Channel Name	giac_to_hosts
Protected Network Address	192.168.10.0/24

VPN Packet-Filtering Rules

Activating VPN on the firewall will be completed by defining the rules in the Packet-Filtering Rules for traffic to pass through VPN tunnels. To make these rules protected by VPN, Protect using IPSec option for each of them need to be activated. If this option is selected, IPSec parameters can then be defined.

Rules definitions for VPN traffic, created based on the access requirements, are presented in the table below. In the Option field, UDP traffic will be using ENABLE_REPLY, explained in the Packet Filtering policy above.

Type	Service	Source	Destination	Option
# VPN users to connect to giac-db				
permit	1433/tcp	giac-vpnhosts	giac-db	
# VPN users to connect to giac-mail				
permit	135/tcp	giac-vpnhosts	giac-mail	
permit	1026/tcp	giac-vpnhosts	giac-mail	
permit	1027/tcp	giac-vpnhosts	giac-mail	

permit	1028/tcp	giac-vpnhosts	giac-mail	
# VPN users to connect to domain controllers				
permit	1029/tcp	giac-vpnhosts	giac-dc	
permit	53/tcp	giac-vpnhosts	giac-dc	
permit	53/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	88/tcp	giac-vpnhosts	giac-dc	
permit	88/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	123/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	135/tcp	giac-vpnhosts	giac-dc	
permit	389/tcp	giac-vpnhosts	giac-dc	
permit	389/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	445/tcp	giac-vpnhosts	giac-dc	
permit	3268/tcp	giac-vpnhosts	giac-dc	

Protect using IPSec option policy will be created similarly for all the traffic above, since they will all use the same IPSec policy, as shown in the table below.

Parameters	Value
IPSec Protection Strategy	giac-ipsec
SA Granularity	Host

SA Granularity will determine how the Security Associations (SAs) will be created. Since Host is used here, then an SA will be created for a host communication with its peer, regardless how many protocols used between them.

The Firewall will be able to automatically match the specific rules with the channel/tunnel they should be using. This auto detection will only work if the rules and the channel parameters are set correctly, as what has been defined here. However, manual selection of channel can also be performed if required.

VPN Host Policy

CyberGuard VPN Client is installed on the remote users PC or laptop as VPN Host. Policy of the VPN Host will be applied according to the VPN Policy to communicate with the VPN Gateway.

Following the term used by the CyberGuard VPN Client, policy of the VPN Host will be divided into Connections, with each Connection represent each destination host(s) behind the VPN gateway that the VPN Host need to connect to.

Connection	Connection Security	Description
giac-db	Secure	VPN connection to giac-db
giac-mail	Secure	VPN connection to giac-mail
giac-dc	Secure	VPN connection to giac-dc
Other Connections	Non-secure	Other non-secure traffic to Internet

Each Connection, except for *Other Connections*, consists of same policy parameters, divided into three parts, Remote Party Identity and Addressing, My Identity and Security Policy. Figure 2 shows a screen shot of the VPN Client.

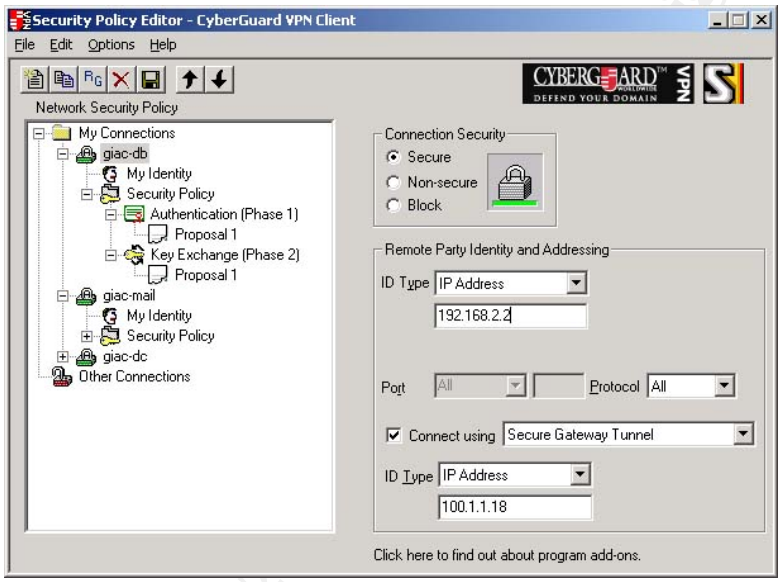

Figure 2: VPN Client

Remote Party Identity and Addressing

Two areas need to be defined here. First is the identity of the destination in the internal or private network behind the VPN gateway, which are the other endpoint from the VPN Host point of view, defined here as Remote Party Identity. Second is the identity of the VPN Gateway that the VPN Host will connect to, defined here as Secure Gateway Tunnel.
Each of the Connection will have different destinations in the internal network behind the Gateway, but will connect to the same Gateway.

Connection	Remote Party Identity			Secure Gateway Tunnel	
	ID Type	Value	Protocol	ID Type	Value
giac-db	IP Address	192.168.2.2	All	IP Address	100.1.1.18
giac-mail	IP Address	192.168.3.2	All	IP Address	100.1.1.18
giac-dc	IP Address Range	192.168.1.11-192.168.1.12	All	IP Address	100.1.1.18

My Identity

Identity of the VPN Host connecting to the VPN Gateway will be determined here. This is how the VPN Gateway will differentiate of which client connecting to it. This is shown in Figure 3.

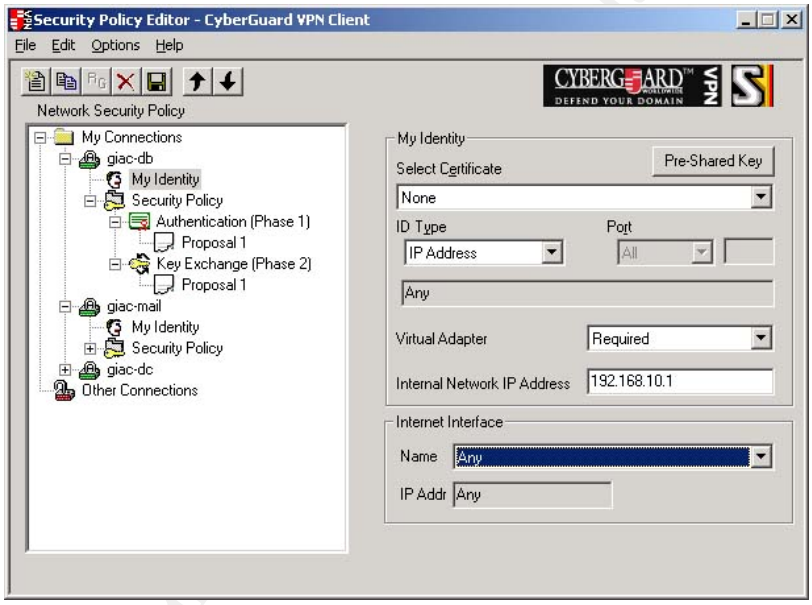

Figure 3: My Identity

Pre-Shared Key will be set here, with the same value of what the VPN Gateway has. VPN Host will use a Virtual IP address in the VPN communication, and the VPN Gateway will create the tunnel and filter the traffic based on this Virtual IP addresses. All the Connections in the same VPN Host will use same Virtual IP address. Different VPN Hosts will be assigned different Virtual IP address. One subnet, 192.168.10.0/24 is assigned for Virtual IP addresses of VPN Hosts.

Security Policy

Security Policy will determine the IKE and IPSec properties used to communicate with the Gateway. All the Connections in a VPN Host, as well as all the VPN Hosts, will use the same Security Policy. Security Policy further divided into two parts, Authentication

(Phase 1) for IKE policy and Key Exchange (Phase 2) for IPSec policy. Figure 4 shows options for Security Policy.

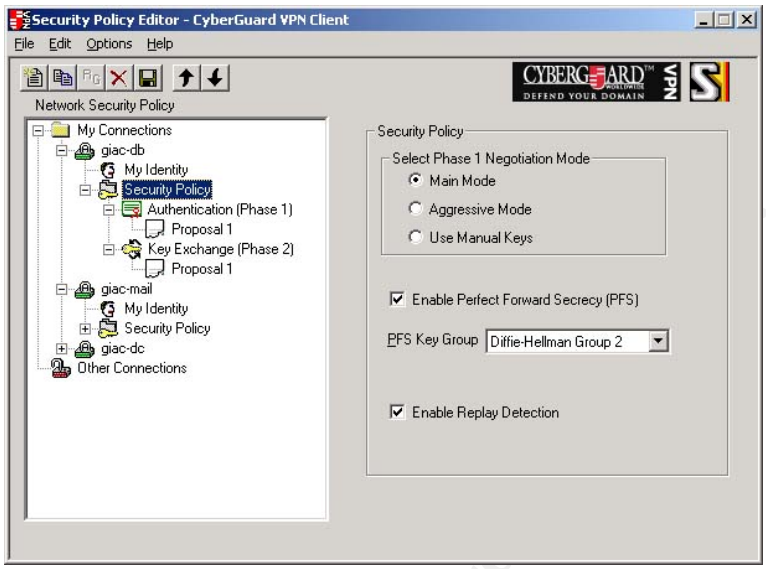

Figure 4: Security Policy

Several parameters for IKE negotiation are defined at the Security Policy level as well as at the Authentication (Phase 1), as shown in Figure 5.
At the Security Policy level, defined the Phase 1 Negotiation Mode as Main Mode, and Enabling Perfect Forward Secrecy (PFS) using Diffie-Hellman Group 2.
While at the Authentication (Phase 1) level, defined the values as follows:

Parameters	Value
Authentication Method	Pre-Shared Key
Encryption Algorithm	3DES
Hash Algorithm	SHA-1
SA Lifetime (Seconds)	10800

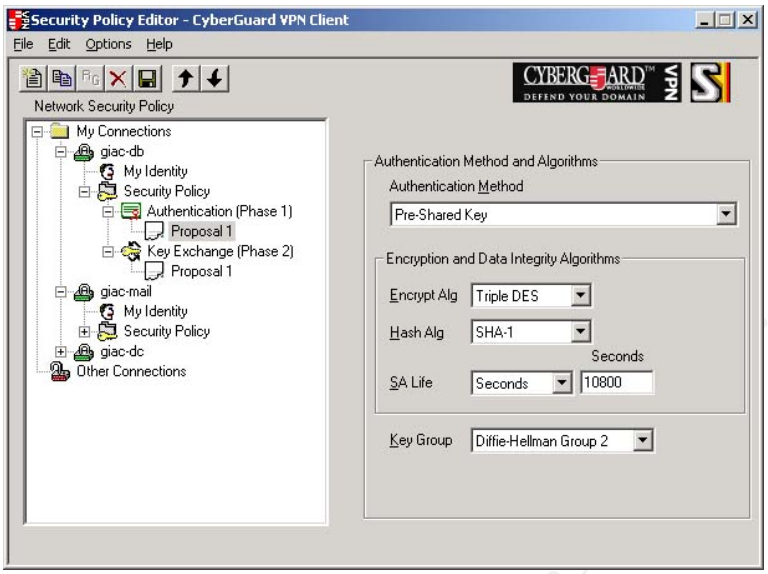

Figure 5: IKE

IPSec policy, defined in the Key Exchange (Phase 2) level, as shown in Figure 6, has the following values:

Parameters	Value
SA Life (Seconds)	28800
Compression	None
Protocol	ESP
Encryption Algorithm	3DES
Hash Algorithm	SHA-1
Encapsulation	Tunnel

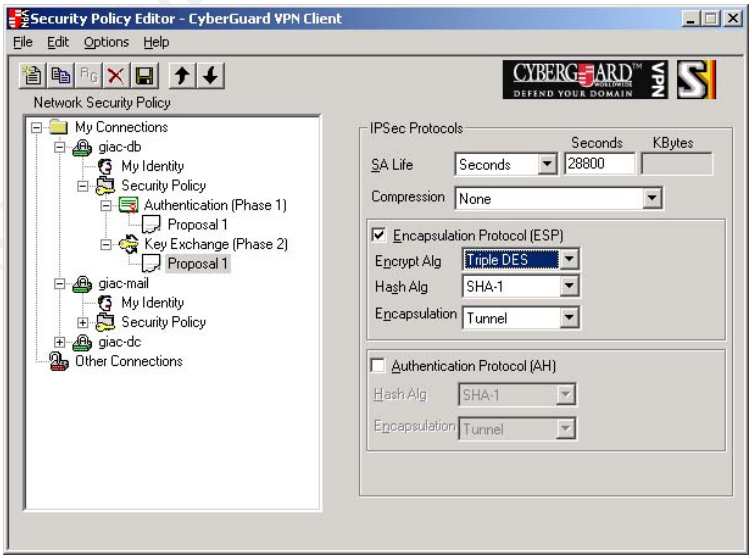

Figure 6: IPSec

Other Connections

Other Connections (Figure 7) will represent other traffic not specified in either one of the Connections, such as normal Internet traffic. The policy for this Other Connections is either Non-secure or Block. Non-secure can be used when there is a need to get normal Internet traffic when this VPN Client is active. Block can be used to block normal Internet traffic when VPN Client is connecting through VPN tunnel to the VPN Gateway, in which this action will secure the host for only talking through VPN.

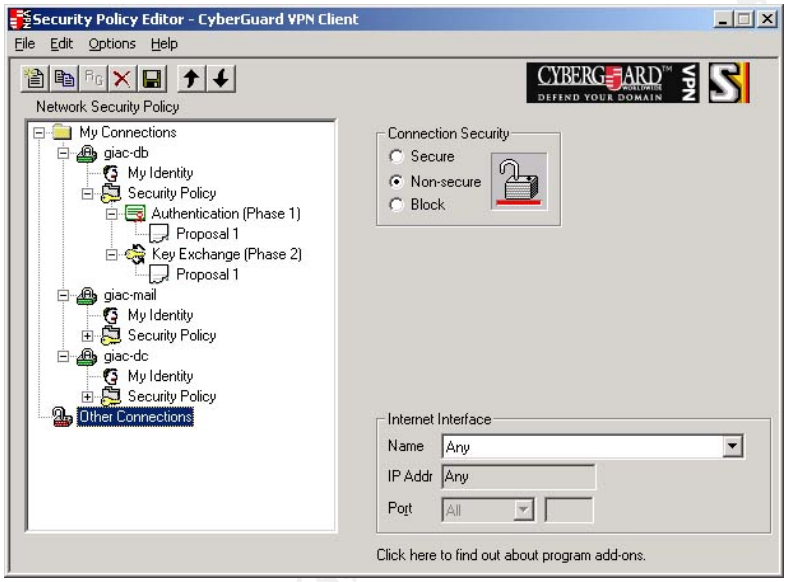

Figure 7: Other Connections

Firewall Packet-Filtering Rules

The Firewall is used to apply both Firewall security policy and VPN security policy. Both of these policies are applied to a single Packet-Filtering Rules engine that inspects the rules using top to bottom sequence. Order of the rules is important to ensure no contradicting situation where the security or functional intention of the traffic using the rules is not met. Further analysis is required since many components are defined, which are proxies rules, packet filtering rules, Split DNS rules and VPN rules. Some of these rules like in proxies and Split DNS are created automatically, which placed in the certain area of the Packet-Filtering Rules.

Generally, manually created rules can be placed anywhere in the Packet-Filtering Rules with the rules sequence applied. However, there are recommended placement for these rules, which are above the automatic generated rules. There are pointers in the configuration GUI for Packet-Filtering Rules on where to place the rules.

Placement of the rules can be done by per group basis, which is using the following sequence accordingly:

1. Packet filtering policy rules
2. VPN policy rules
3. Split DNS rules
4. Proxies rules

Packet filtering policy rules should go first, since those are involving hosts in the LAN with Microsoft Windows environment, which are very noisy and will be very frequently used.
VPN policy rules follow in second, where they use similar kind of traffic as in LAN, but less users involved and smaller bandwidth of WAN link compare to LAN.
Next are Split DNS rules, placed automatically by the firewall, below the manually added rules.
And lastly, proxy filter rules, placed automatically by the firewall, below the Split DNS rules. These rules will then being edited according to proxy policies.

The last rule will be deny everything else, as shown in the table below:

Type	Service	Source	Destination	Option
deny	ALL	EVERYONE	EVERYONE	ENABLE_REPLY

Full Packet-Filtering Rules policy can be seen on Appendix B.

Firewall Tutorial

Besides its main function to filter traffic either using Proxy or Packet Filtering, the firewall here is also used for DNS Server as well as VPN gateway. This tutorial section will cover only the main function, filtering of traffic. Screen shots included later are taken from CyberGuard Firewall Manuals[7]. Tutorial will explain on how to implement the policy described in the Firewall Security Policy section.

Configuration of the CyberGuard firewall is done through its Graphical User Interface (GUI), which uses X-Window. Locally, can be done by using monitor, keyboard and mouse connected to the appliance.

As shown in figure 8, the GUI consists of menu bar with four main configuration menus: **System**, **Configuration**, **Reports** and **Tools**. Additionally there is also Online Help available.

Figure 8: CyberGuard Firewall Main Menu

[7] Due to the difficulty of taking the screen shots from the firewall, they are taken from the manuals, where they may not reflecting the exact configuration discussed

Under each of the menu on the menu bar, there are options/features that can be chosen to configure the firewall, as shown in Figure 9. Each of the options, once chosen, will be showing the configuration window for that particular option.

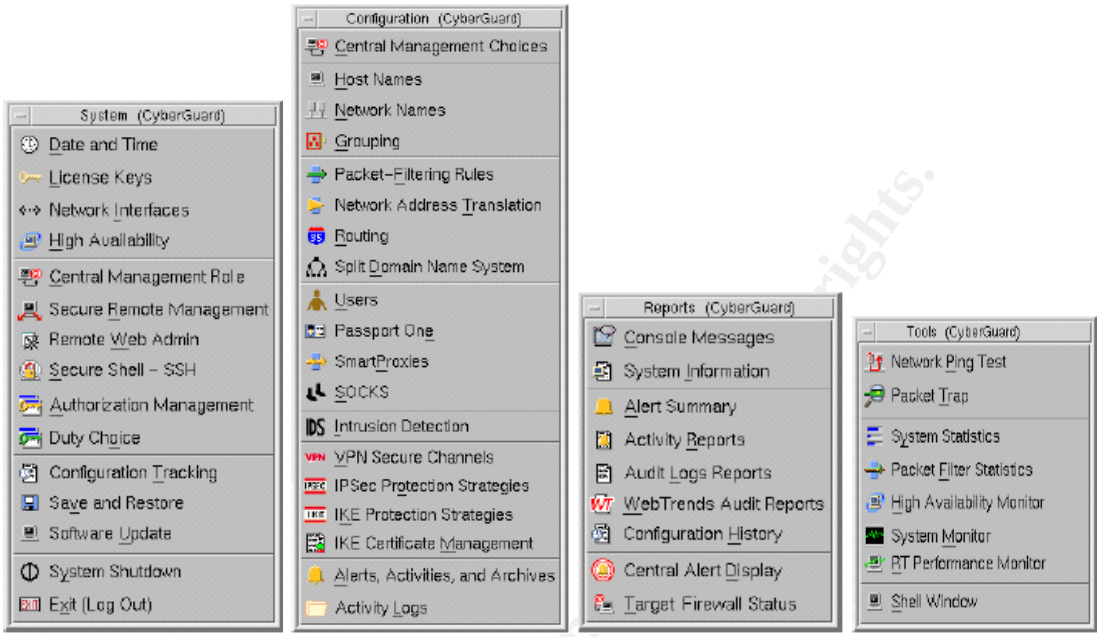

Figure 9: Configuration menus

Several characteristics of the configuration window, explained below:

- Every time there are changes on the configuration, the configuration must be saved before changes can take effect. This saving of configuration will be done on per window basis. Each window will have **Save** button, to save the configuration changes, which will change color to yellow when there are new changes on that particular window. If no changes, this button will be grayed out.
- Few windows will have **Save** and **Use** buttons. Both buttons will grayed out for no changes, and turn to yellow when there are new changes. For these window, **Save** will only save the configuration, but will not apply the changes to the current running configuration, until firewall being rebooted. To apply to the current running configuration **Use** button will be used.
- On each configuration window, there are fields, which either yellow or white color. Yellow color fields are compulsory fields that have to be filled in. White color fields are optional fields.

Packet-Filtering Rules

This configuration window, as shown in Figure 10, is the main component where all the traffic will be controlled whether they allowed to pass the firewall, as well as how they going to be filtered.

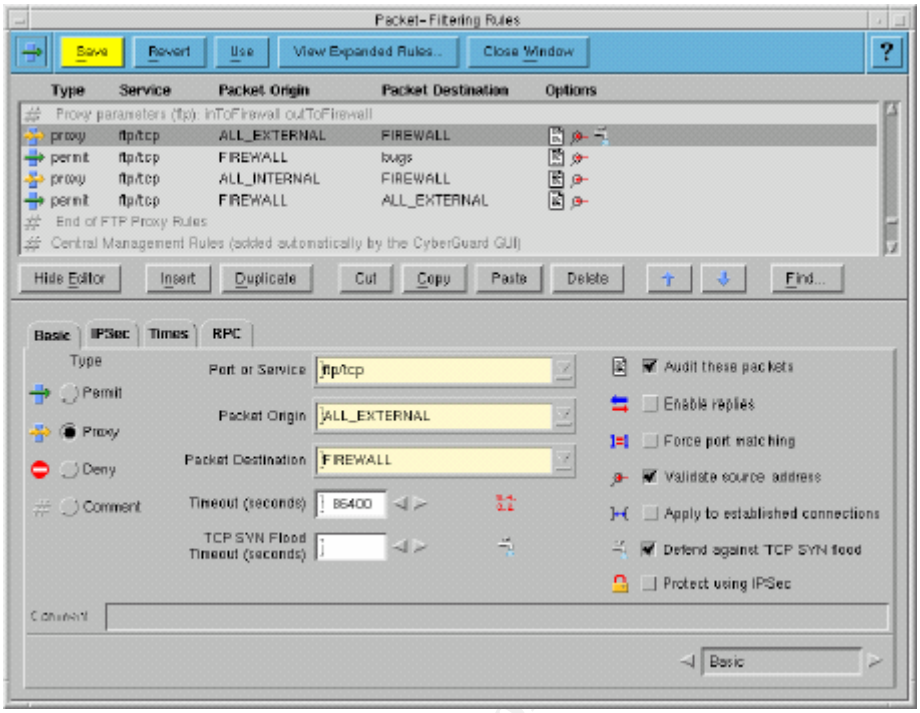

Figure 10: Packet-Filtering Rules Window

As mentioned earlier in front, the order of the rules is important because the firewall will inspect the traffic by using top to down approach. The last rule will be deny everything, which built in into the firewall engine. Since this firewall is stateful firewall, only one direction for traffic need to be specified, which is from who will initiate the connection.

For this section, only **Basic** page that will be explained, since only this part is relevant to the Firewall policy created for GIAC Enterprise.
The options shown in the **Basic** page is applied for each individual rule. So every rule can have different kind of configuration. New rule is created by first choose the location for that rule, then either use **Insert**, **Duplicate**, or **Cut**, **Copy** or **Paste** buttons to configure the rule.

Type radio buttons are used to determine what kind of action that the specific rules will be doing.

- **Permit**, to allow traffic using dynamic packet filtering
- **Proxy**, to allow traffic using proxy
- **Deny**, to deny traffic
- **Comment**, to make the specific line commented or to be used for documentation

Port or Service field is used to define what kind of protocol will be associated with the specific rule. The notation used here is *service[/protocol]*. There are number of ways to fill this field:

- Using keywords of services available in the drop down list, such as http/tcp, domain/udp, etc.
- Using group of services (must be defined in Grouping window). This can be done by either type the group them manually, or select it from the drop down list. Automatically, every time group of services created, they will be added into this drop down list.
- Using numbers, which follow the ports number and/or protocols number standard. This is especially useful when defining port or protocol not listed in the firewall. Example: 135/tcp, ALL/50
- Using range of ports, such as 137-139/udp. The ports must be in sequence.

Packet Origin and **Packet Destination**, as their names imply, will be determining in which direction the traffic passing the firewall will be filtered.
In the drop down list, there are several keywords available:

- ALL_INTERNAL, referring to hosts on the network(s) connected to the firewall interface(s) labeled Internal.
- ALL_EXTERNAL, referring to hosts on the network(s) connected to the firewall interface(s) labeled External.
- *device*_NETWORK, such as dec0_NETWORK, dec1_NETWORK, etc, referring to hosts on the network connected to the specific firewall interface.
- FIREWALL, referring to local host of the firewall.
- EVERYONE, referring to all network connected to the firewall and the firewall itself.

Besides the existing keyword, the following values can also be entered:

- Group of Hosts/Networks type. These groups will be added automatically into the drop down list, once they are created in the Grouping window.
- Host names, referring to host names created in Host Names window. This has to be entered manually and need to be an existing hosts definition in the Host Names window.
- IP address, which the individual IP addresses.
- Networks, referring to Network addresses and their masks. For example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24

Several other options are turned on by default when creating a new rule:

- **Audit these packets**, enable the firewall to log hits against that specific rule.
- **Validate source address**, enable the firewall to check whether the incoming packets are coming from the correct interfaces. This being used to defend against IP spoofing.

Other option that needs to be enabled for certain traffic is **Enable replies**. This will be required for UDP traffic, to enable the firewall apply the state to them. For TCP this is not required, since TCP already has mechanism of determining sessions. This option is explained in the Firewall Security Policy, Packet Filtering Policy section as the ENABLE_REPLY option.

Accordingly, all rules for Packet-Filtering Rules from the Firewall Security Policy and VPN Security Policy defined in the previous section will be placed in this Packet-Filtering Rules window, either manually or automatically.

SmartProxies

SmartProxies window, shown in Figure 11, is the place to configure proxy services. Proxies have to be enabled from here before they can be used to filter traffic.

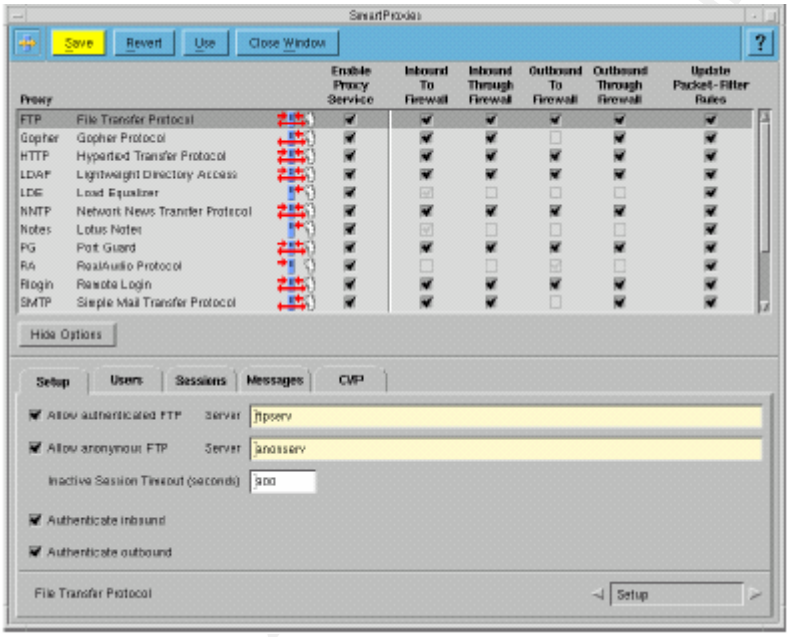

Figure 11: SmartProxies Window

On the **SmartProxies** window can be seen that there are two main parts of the window. The top part is the list of proxies available, with check boxes configuration options. The bottom part contain configuration that will change accordingly every time different proxy is highlighted on the top part. If for example FTP Proxy is highlighted on the top part, the bottom part will show configuration options for FTP Proxy, same thing goes for other proxies.

The first step to do in configuring proxy is to choose which proxy to be enabled, which available on the list on the top part of the window.. This can be done, by checking the **Enable Proxy Service** check box for each individual proxy. After that, choosing the directions, whether to use **Inbound To Firewall**, **Inbound Through Firewall**, **Outbound To Firewall** or **Outbound Through Firewall**. Definition of these terms has already being covered on the firewall policy section.

Update Packet-Filter Rules check boxes are used to automatically create rules in the Packet Filtering Rules associated with each proxy enabled and the type of that proxy,

Inbound and/or Outbound, To and/or Through. These rules can then be seen in the **Packet-Filtering Rules** window.
Generally, the rules created are very generic, as typically described below:

- Inbound To

Type	Service	Origin	Destination
proxy	*service*	ALL_EXTERNAL	FIREWALL
permit	*service*	FIREWALL	*server*

- Inbound Through

Type	Service	Origin	Destination
proxy	*service*	ALL_EXTERNAL	*server*

- Outbound To

Type	Service	Origin	Destination
proxy	*service*	ALL_INTERNAL	FIREWALL
permit	*service*	FIREWALL	ALL_EXTERNAL

- Outbound Through

Type	Service	Origin	Destination
proxy	*service*	ALL_INTERNAL	ALL_EXTERNAL

As they are very generic, changes can then be done in later step from **Packet-Filtering Rules** window to tighten them. After changes being done manually in the **Packet-Filtering Rules** window, **Update Packet-Filter Rules** check boxes should be un-checked when any further changes are being done on the **SmartProxy** window. If these are still checked, then the manual changes in the **Packet-Filtering Rules** window will be replaced by the automatic generated rules.

Although the automatic generated rules are generic rules, they are useful to be used as guidelines when creating rules for proxies. It will help in determining what kind of rules required for what kind of proxies.

The second step is to configure each proxy with its specific configuration options, which shown on the bottom part of the window. The proxies are inspecting traffic at application level, so each of them will inspect different things based on what kind of application protocols they are for.

With the two steps above, proxy configuration in the **SmartProxies** window is complete. The last step will be to go to **Packet-Filtering Rules** window to edit the rules created for proxies.

FTP Proxy Configuration

In the Firewall policy, FTP Proxy will be used in Outbound Through configuration and only CVP configuration need to be changed. The rest of the configuration can be left as default values. Configuration options for FTP Proxy are shown in Figure 12.

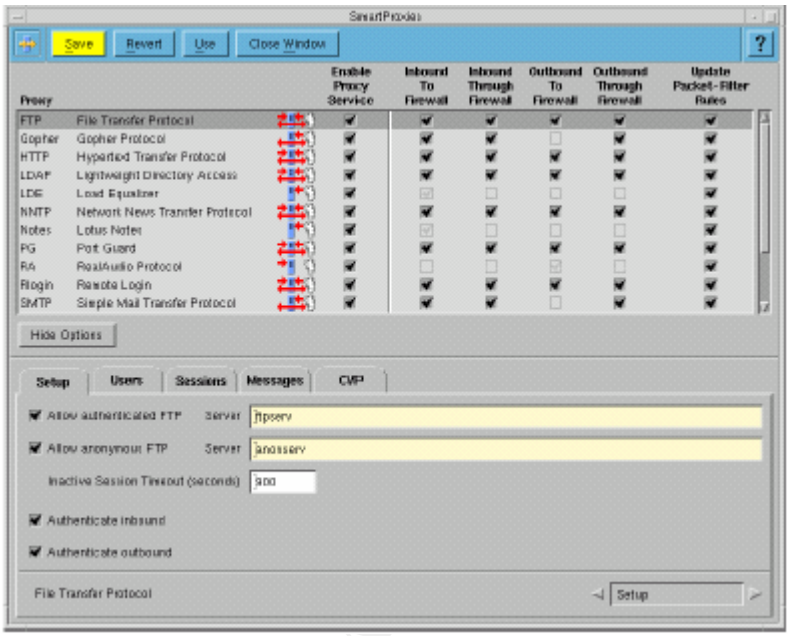

Figure 12: FTP Proxy Configuration Options

To configure the FTP Proxy, from the **SmartProxies** window, **FTP** should be highlighted. The appropriate settings on the proxy line should be chosen accordingly. **Enable Proxy Service**, **Outbound Through Firewall** and **Update Packet-Filter Rules** at the FTP line are checked. With the FTP highlighted, on the bottom part of the window, can be seen five tabs for FTP Proxy configurations, **Setup**, **Users**, **Sessions**, **Messages** and **CVP**.

FTP Setup Page
In the **Setup** page, shown in Figure 12, the two check boxes **Allow authenticated FTP** and **Allow anonymous FTP** will be left un-checked, since these are only to be used with inbound FTP. Same thing goes for **Authenticate inbound** check box. **Authenticate outbound** can be used to add extra authentication for users before they are able to perform FTP to external FTP server, but in this case it will be left un-checked, because it is not required here.

FTP Users Page
This page is used to lists users allowed to perform FTP operations, as shown in Figure 13.

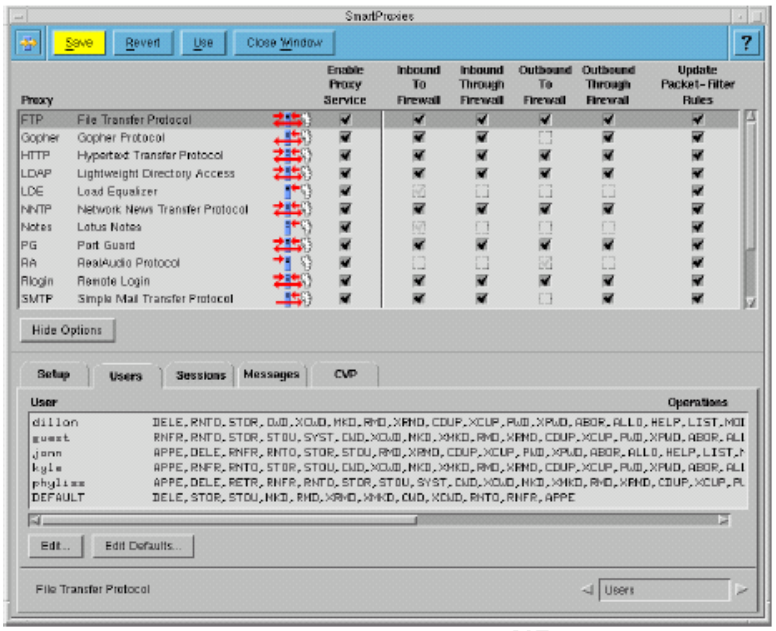

Figure 13: FTP Proxy Users Page

By default there is a *DEFAULT* user listed in this page, which refer to anybody using FTP proxy, unless his username is specified. This *DEFAULT* user definition is sufficient here, and no other users need to be added. **Operation** field states FTP commands each user can perform.

FTP Sessions Page

This page, as shown in Figure 14, is used to define FTP operations that are permitted for an FTP session between a specified source address and destination address.

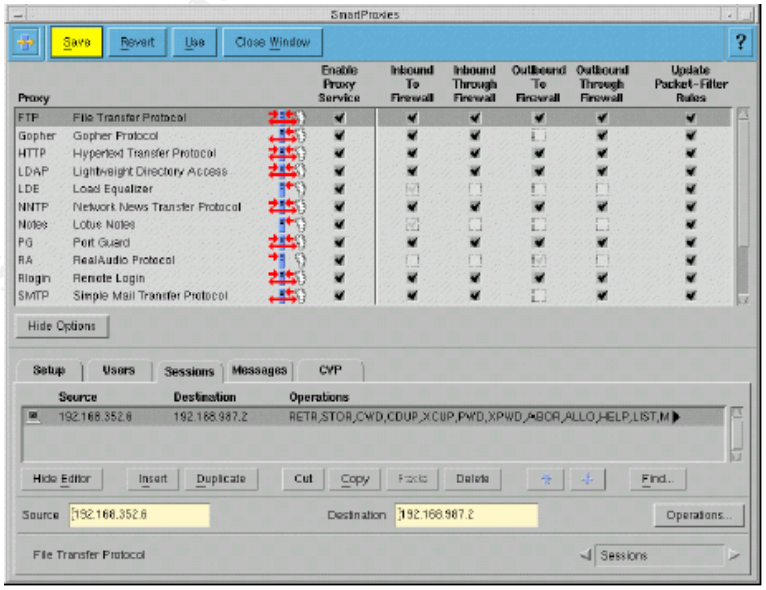

Figure 14: FTP Proxy Sessions Page

It will be left empty, as default, since for the outbound FTP session, internal users are allowed to connect to any FTP servers in the Internet.

FTP Messages Page
This page, used to set the login greeting message, login failure message, and anonymous FTP usage message is also left empty, as this is used for inbound FTP connection, which not available here.

FTP CVP Page
CVP content scanning is enabled and configured in this page (Figure 15)

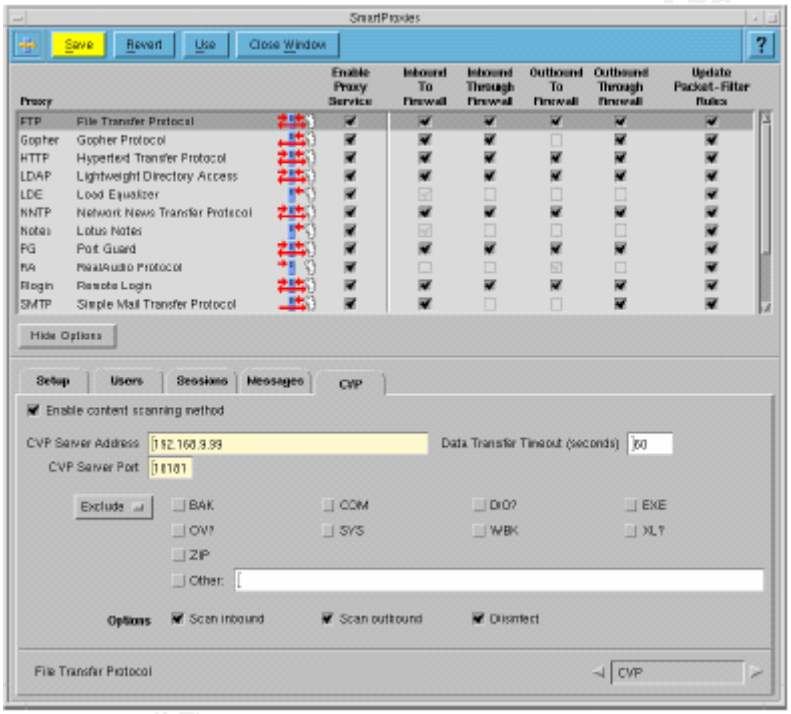

Figure 15: FTP Proxy CVP Page

Enable content scanning method check box should be checked to enable scanning using CVP. **CVP Server Address** field will be filled in with the Anti Virus Server address and **CVP Server Port** field with the CVP communication port used.

Scanning will be done for all files, without doing any exclusion for any file types. There is a drop down list besides the file extensions choices used to configure this, containing **Scan All** (to scan all files), **Include** (to scan files with the selected file extensions) and **Exclude** (to scan files with file extensions that are not selected), which in this case Scan All should be selected.

On the **Options**, three check boxes **Scan inbound**, **Scan outbound**, **Disinfect** will also be checked.

HTTP Proxy Configuration

Several configurations will be done with HTTP Proxy, which used in outbound and inbound configuration. **Enable Proxy Service**, **Inbound Through Firewall**, **Outbound Through Firewall** and **Update Packet-Filter Rules** are checked at the HTTP line on the Proxy list.
HTTP Proxy configuration contains of several pages - **Setup**, **Servers**, **Clients**, **Chaining**, **URL Translation**, **Language Blocking** and **CVP**. Changes only required on the **Setup**, **Servers** and **CVP** pages, with the rest left with default values.

HTTP Setup Page
Location of web server used is configured here, along with enabling https:// and ftp:// support. Figure 16 shows this page.

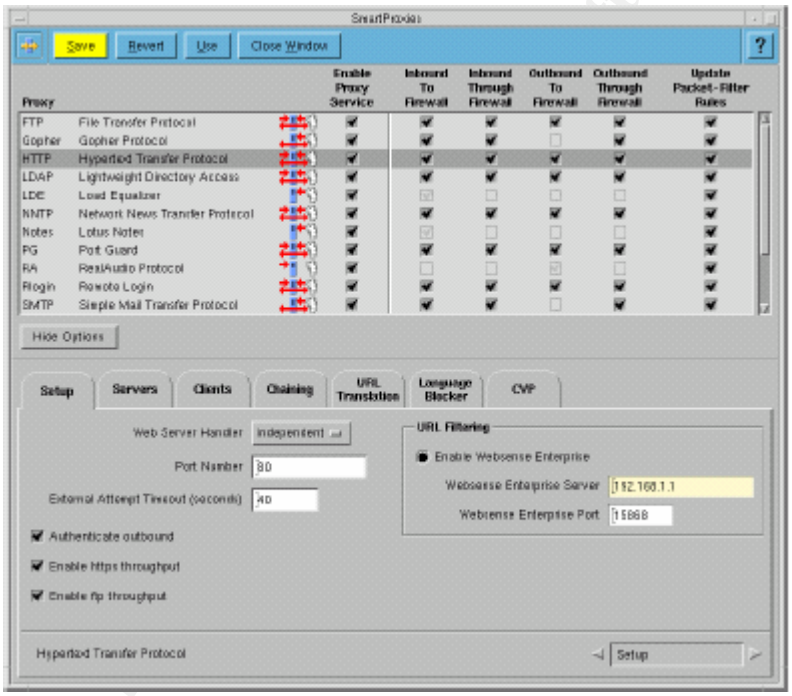

Figure 16: HTTP Proxy Setup Page

Location of web server is configured with **Web Server Handler** drop down list, which has three options, referring to internal web server protected by firewall:

- **None** – no web server
- **Built-in** – built in web server in the firewall
- **Independent** – separate web server outside the firewall

Independent will be chosen, since web server (*giac-web*) is separate system outside the firewall.

Port Number, defining port the HTTP Proxy will listen, use the default value 80 and **External Attempt Timeout (seconds)**, is left as default, 40. URL Filtering is not enabled, so **Enable Websense Enterprise** button is left unchecked, which then cause

the **Websense Enterprise Server** and **WebSense Enterprise Port** fields to be grayed out.

Authenticate outbound, which cause the outbound web user required to authenticate to firewall before getting the access, is not used, so it's left unchecked.
To enable support for https:// and ftp://, the two check boxes, **Enable https throughput** and **Enable ftp throughput** are checked.

HTTP Servers Page
Since inbound HTTP Proxy is required, **Servers** page (Figure 17) should be configured to define the web servers and allowed type of commands to access them.

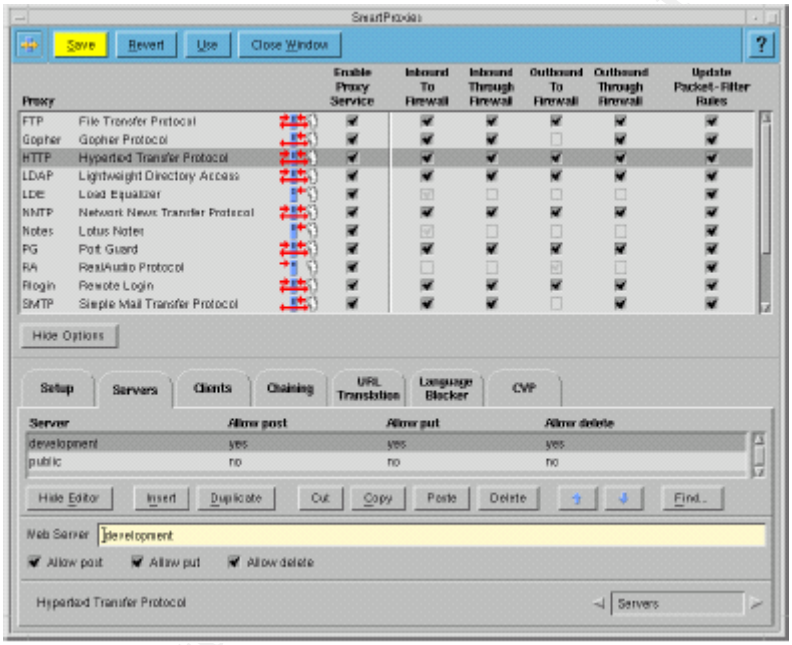

Figure 17: HTTP Proxy Servers Page

One web server definition is required here, which is done by clicking **Insert**, entering *giac-web* on the **Web Server** field, and uncheck **Allow post**, **Allow put** and **Allow delete**.

HTTP Clients Page
Within HTTP Proxy, filtering can be done to limit access from certain internal users to certain external servers, and define what kind of content scanning will be applied to these users. The filters applied here are referring to outbound connection only. Figure 18 shows the **Clients** page.

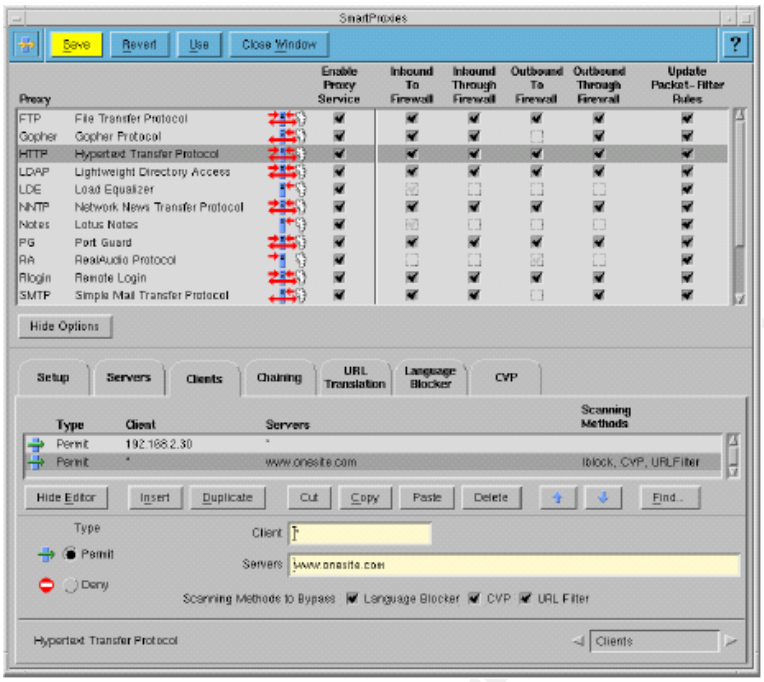

Figure 18: HTTP Proxy Clients Page

Default setting for this is to permit any client to any server and apply all filtering by Language Blocker, CVP and URL Filter. Default value is used here.
When highlighting the rule, can be seen that **Type** will be **Permit**, **Client** will be * to refer to any clients, **Server** will also be * to refer to any server. On the **Scanning Methods to Bypass**, three options - **Language Blocker**, **CVP** and **URL Filter** are unchecked

HTTP CVP Page
CVP configuration for HTTP is similar to those in FTP, shown in Figure 19.

Enable content scanning method check box should be checked to enable scanning using CVP. **CVP Server Address** field will be filled in with the Anti Virus Server address and **CVP Server Port** field with the CVP communication port used.

Scanning will be done for all files, without doing any exclusion for any file types. There is a drop down list besides the file extensions choices used to configure this, containing **Scan All** (to scan all files), **Include** (to scan files with the selected file extensions) and **Exclude** (to scan files with file extensions that are not selected), which in this case Scan All should be selected.

On the **Options**, three check boxes **Scan inbound**, **Scan outbound**, **Disinfect** will also be checked

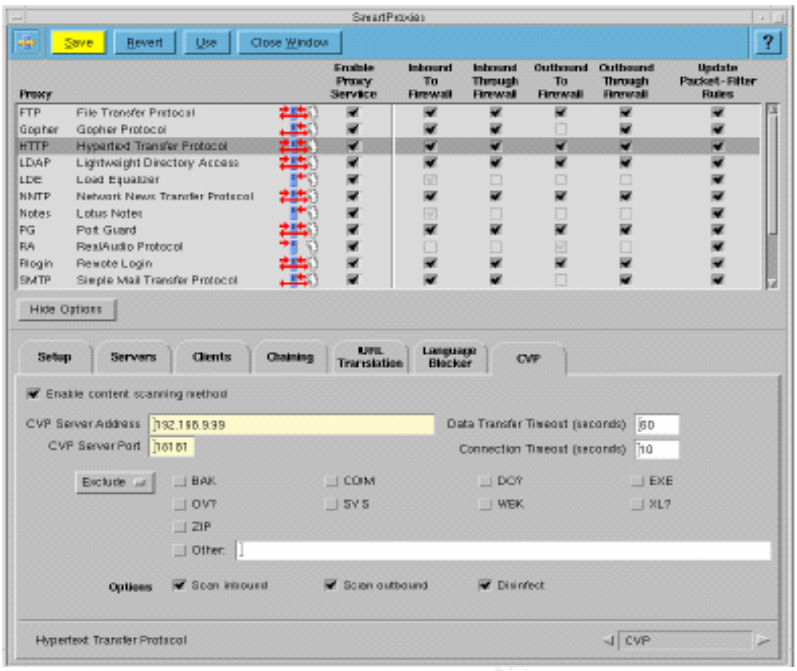

Figure 19: HTTP Proxy CVP Page

SMTP Proxy Configuration

SMTP Proxy is used in inbound and outbound configuration to and from the mail server, *giac-mail*. **Enable Proxy Service**, **Inbound Through Firewall**, **Outbound Through Firewall** and **Update Packet-Filter Rules** are checked at the SMTP line of the Proxy list.
SMTP Proxy configuration containing of several pages – **Setup**, **Servers**, **Users**, **Blocking** and **CVP**, but **Users** and **Blocking** pages are left out to default because they are not required here.

SMTP Setup Page
Figure 20 shows this page, where several characteristics are defined here, including default domain used and number of protocol errors allowed before connection closed.

Default Domain Name value by default will be using the firewall domain name defined in **Network Interfaces** window. No changes required here, so *giac.com* is used here. **Number of Protocol Errors Allowed** is using default value, 5. **Post default domain for outbound mail** check box is checked to allow replacement of internal mail server name in the outbound mail header to the default domain name of the firewall. This feature will hide the internal name from being exposed to external servers.

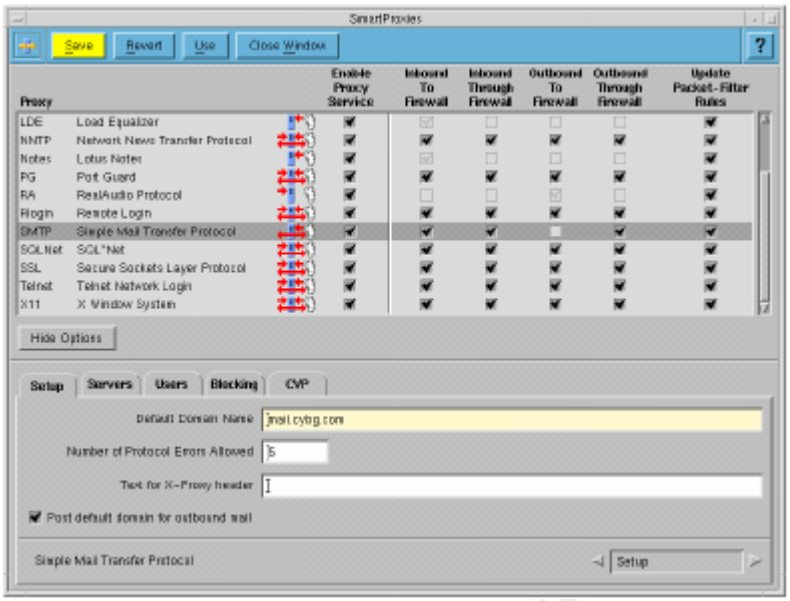

Figure 20: SMTP Proxy Setup Page

SMTP Servers Page
Internal server used will be defined in this page (Figure 21)

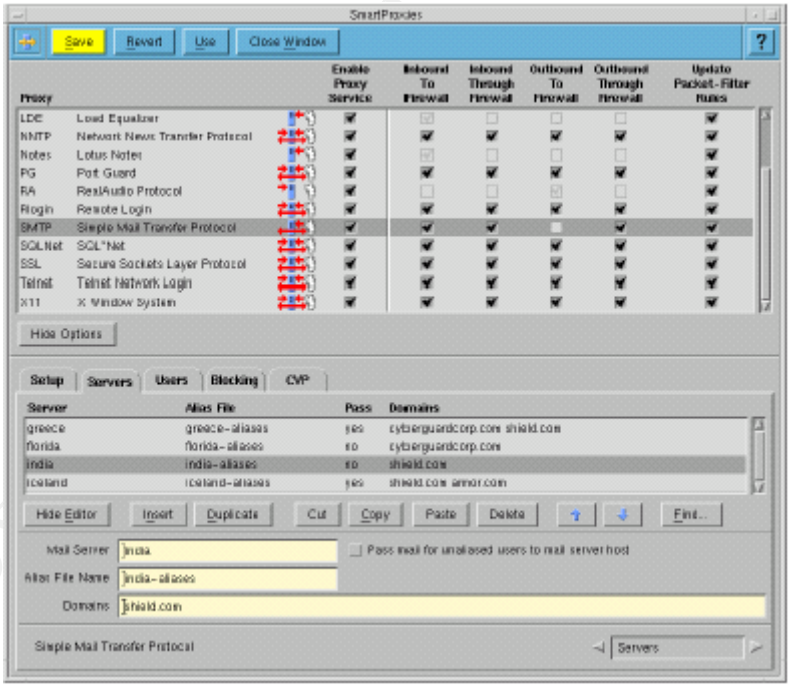

Figure 21: SMTP Proxy Servers Page

One server definition is required, which after pressing **Insert** button, Mail Server field is filled with *giac-mail*, referring to the server name used.

Pass mail for unaliased users to mail server host check box is checked and will cause the **Alias File Name** filled automatically with *NONE*. These two choices will cause all incoming mails to be sent to the internal mail server without comparing the mail recipient to the alias file.

Domains field is filled with *giac.com*, which will allow only mails sent to recipients with *giac.com* domain. This will prevent external people using the mail server as relay. Any mails with recipient's domain other than specified here will be dropped.

SMTP CVP Page
CVP configuration for SMTP is similar to those of FTP and HTTP with exception that there is no option to select certain file types to scan, so it will scan all file types, as shown in Figure 22.

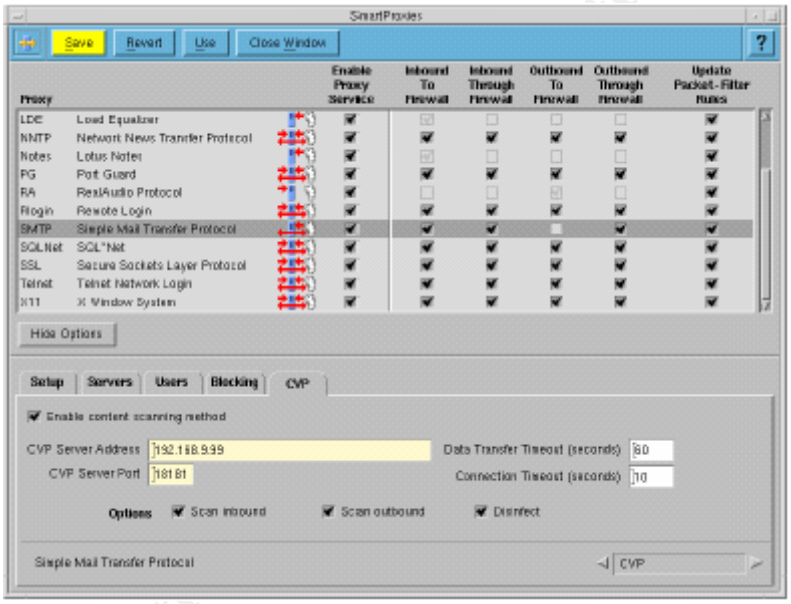

Figure 22: SMTP Proxy CVP Page

Enable content scanning method check box should be checked to enable scanning using CVP. **CVP Server Address** field will be filled in with the Anti Virus Server address and **CVP Server Port** field with the CVP communication port used.

On the **Options**, three check boxes **Scan inbound**, **Scan outbound**, **Disinfect** will also be checked.

SSL Proxy Configuration

SSL Proxy is used in inbound and outbound configuration. In the SSL line of Proxy list, **Enable Proxy Service**, **Inbound Through Firewall**, **Outbound Through Firewall** and **Update Packet-Filter Rules** are checked to enable the desired configuration.

Because of the nature of SSL where the data are fully encrypted, it is not possible for the proxy to really inspect the data. It is limited to breaking up direct connection between the client and the server, and inspects the unencrypted portion of the connection.
There are two configuration pages in the SSL Proxy, **Setup** and **Clients**.

SSL Setup Page
Internal web server protected by the proxy will be defined in this page, along with the port where the proxy will listen on. Figure 23 shows this page.

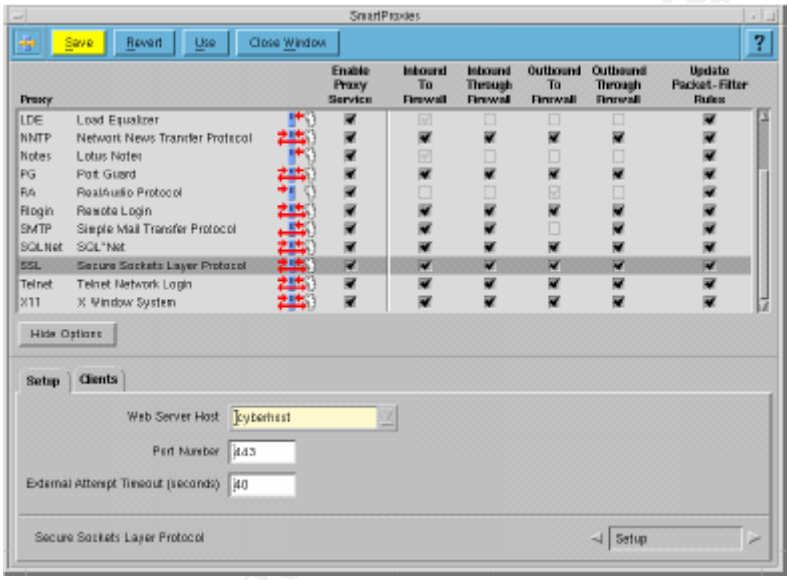

Figure 23: SSL Proxy Setup Page

Web Server Host, is filled with the web server name, *giac-web* and **Port Number** will use the default value, which is 443.

SSL Clients Page
This page, shown in Figure 24, is used to filter access from internal users to external servers for outbound SSL connections. It is similar to the same page name in HTTP Proxy.

Default value, which is permit any clients to any server, is used here. **Type** will be Permit, **Client** will be *, **Servers** will be * and **Tunnel** check box will be unchecked. **Tunnel** check box is used to perform SSL tunneling.

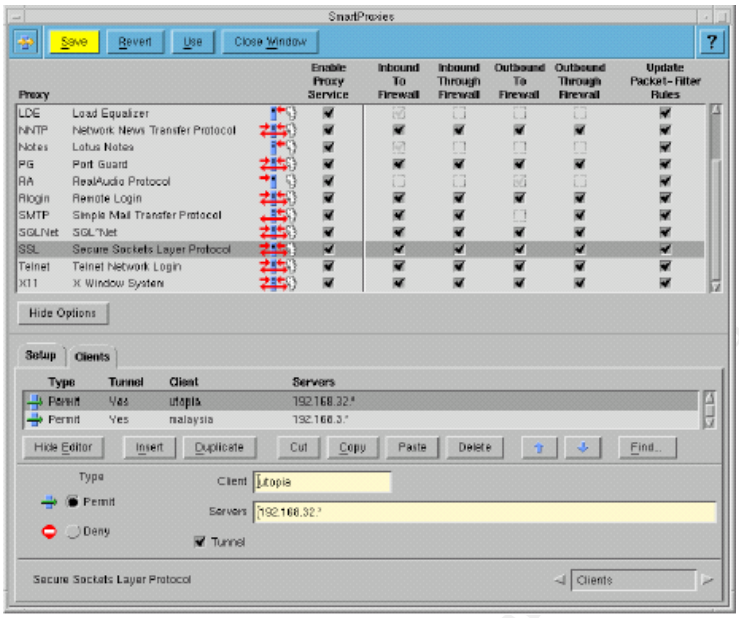

Figure 24: SSL Proxy Clients Page

Assignment 3 – Verify the Firewall Policy

Audit Plan

After the firewall has been implemented and configured according to the defined policy, audit to the firewall will be conducted to make sure that the firewall performs the functions as what it is tasked to do.

Audit will be focused only on the firewall itself, to verify its policy and its ability to defend against attacks.

Technical Approach

Audit will be done in several parts to verify the functions carried out by the firewall, which are:

- Firewall testing
  Perform test on the firewall host itself of how it can defend against attacks and identifying services running on the firewall.
- Firewall rules verification
  Verify rules on the firewall, whether they are configured properly to comply with the firewall policy.
- Proxy services testing
  Perform testing on the services protected by proxies, to validate how the proxy performs the inspection.

Firewall testing

Firewall testing is meant to test the firewall host, which divided into two phases:

- Vulnerability scanning to the firewall, which testing the ability of the firewall to defend itself against attacks and vulnerabilities.
- Service scanning to the firewall, perform scan to the firewall to identify services running on the firewall.

To perform the vulnerability scanning, a vulnerability scanner will be used to penetrate the firewall with various kinds of attacks signatures, including Denial of Service attacks. Report produced by the scanner and checks on the firewall logs and firewall condition will be used to make a conclusion.
The vulnerability scanner will be scanning from each interface of the firewall.

For the service scanning, a network scanner will be used to scan the firewall to find any services open on the firewall. The scanner will be scanning from each interface of the firewall to produce a complete result, since the services may not run on each interface.

Scanning will be done with few methods:

- SYN scan for TCP ports
  SYN scan is done by sending TCP SYN packet to the target port, and wait for response. If SYN/ACK packet received, the port is open. If RST is received, the port is closed. If the port is closed, the firewall may silently drop the packet. If this situation occurs, the scan will take longer time to finish. Since SYN scan is using normal behavior for any hosts to open connection, SYN scan will be giving the most valid results compare to FIN scan and ACK scan, but also most likely will be captured by the firewall alerts.
- UDP scan for UDP ports
  UDP scan is done by sending UDP packet to the target port, and wait for response. If ICMP port unreachable message received, the port is closed. If nothing received, it will be assumed as open. This scan is very slow due to the fact that most of hosts implement limiting of ICMP error messages sent.

Firewall Rules Verification

This part of audit is meant to test the firewall rules, whether they are really controlling traffic as what they are supposed to do, by allowing only permitted traffic and dropping denied traffic.
This rules testing will involve both stateful packet filtering and proxy rules.

The test will be done with the following methods:

- Network scanner placed in one segment to scan other hosts in another segment passing through the firewall.
- On the target segment, a network sniffer is placed to capture the traffic sent by the scanner.

- On the firewall, the auditing system should also capture the traffic, as well as sending network port scan alert. In this case, this activity can also be used to verify whether the firewall auditing system is working well.
- With the firewall set to send logs to the Syslog server, this server will be checked whether the traffic generated by the scanner are logged.

Conclusion of the result will be taken by comparing results from the scanner, sniffer, firewall logs in the firewall and Syslog server. Attention will be given to permitted traffic found. The results are analyzed based on which components are capturing the traffic generated. The results will then be compared with the firewall policy definition to see if the rules are conformed to the policy or not.

By using the testing method above, one segment is tested from one other segment at one time. Every segment has to be tested from every other segment. Every existing host will be targeted for scanning. For certain segments, where there are rules specifying access allowed from certain IP addresses, scanner will be configured to do scanning by using both the allowed IP addresses and not allowed or non existed IP addresses. This is the approach to prove that those specific rules are really limiting the access.

For each individual test on each segment, several types of scans will be conducted, similarly as described on the firewall testing.

Testing from Internal segments to External segment will be done differently, because perform scanning to any host in the Internet should be avoided. IP address of the sniffer machine placed on the EXTERNAL segment will be used as target. But since this machine doesn't have services that maybe permitted in the firewall, it will not respond to the scanner as open ports for those services. Instead, the sniffer is used to capture the connections, and prove that actually the scan have leaked through the firewall.

Proxy Services Testing

The proxies on the firewall provide inspection up to the application level. With different type of application proxies, different kinds of inspections are done by each of the proxies. Similar process performs by the proxies will be on intercepting connection between client and server, and breaking it into two different sessions. Verification on this process will be covered on the Firewall Rules Verification phase.

This part will be focusing on testing each different type of inspections done by each proxy, to comply with the firewall policy.
Outbound FTP Proxy, HTTP Proxy, and SMTP Proxy will not be specifically tested, since mainly the inspection for the traffic using these two types of connections are to break direct communication between the client and the server. Similarly, SSL proxy either outbound or inbound will not be specifically tested, since due to the nature of SSL, the proxy will be limited to protect against direct connection.

Testing Inbound HTTP Proxy for blocking HTTP commands

- Perform Telnet to port 80 from external network to the web server, issue several HTTP commands inspected by the firewall, which are POST, PUT and DELETE, and see how the firewall reacts.

Testing Inbound SMTP Proxy for blocking mail relaying

- Perform Telnet to port 25 from external network to the mail server, using SMTP commands, send email to recipients with domains other than *giac.com*.

Tools for Audit

To perform the audit, two laptops are provided. One laptop will be installed with Windows 2000 Professional, and the other with RedHat Linux 7.3. Two different OSs are used to facilitate the tools going to be used.

Several tools are used:

- **Vigilante SecureScan NX**, a commercial vulnerability assessment tool by Vigilante.com, Inc. (http://www.vigilante.com). This tool is used to perform firewall testing, running on Windows. Version 2.6 is used.
- **Nmap**, open source network security scanner by Fyodor (http://www.insecure.org/nmap). This tool is capable to perform various type of network scanning required for the audit. Version 3.00 is used.
- **Windump**, open source network sniffer (http://windump.polito.it), the Windows version of **Tcpdump**. This tool is used to sniff the network traffic during various phases of audit. Version 3.6.2 is used.

Risks and Considerations

Conducting the audit will involve certain risks, which identified and addressed as follows:

- During the audit, network operation will be interrupted, which cause operational of the company will also be affected. This is due to the fact that for certain phases of the audit, the servers will need to be disconnected from the network. A good schedule plan of the audit will address this issue, and will definitely be done outside of official business hours.
- Interruption of the services will cause complaints to arise. To prevent this to happen, prior to the audit, all related parties should be notified of the audit activity. These include internally - company officers, IT staffs, remote users and externally – customers, suppliers and partners.
- As the impact of the audit testing, the servers or the firewall might experience slow down or even crash. They might need to be rebooted, which caused services disruptions. Worse case, crash of the systems may not be resolved by simply rebooting, reinstallation may need to be done. Full backup of the systems should be

done prior conducting the audit. If reinstall is required, restore from backups will fasten the process.

Costs and Schedule

The audit will be conducted by GIAC's IT staffs themselves without involving third party consultants. Costs involved will be the staffs' time taken to concentrate on audit. Two staffs are tasked to do the audit. Two machines used for the audit are reserved machines, which not only used for this activity.

Costs estimation are explained below:

Components	Time (hours)
Planning and research	24
Firewall testing	2
Firewall rules verification	10
Proxy services testing	1
Evaluation and creating reports	24
Additional hours for unexpected issues	4
Total	65

The audit will be conducted outside official business hour, where no staffs are working locally, which then will have less impact to the company operation. 'No impact' condition cannot be expected, since business operations is also being done online through Internet, which has international coverage with different time zones. Because GIAC is also selling fortunes to online customers, weekends are also expected to be peak periods, but still less users compare to the weekdays. Considering these conditions and time required to perform the audit, which approximately 13 hours, the best schedule for executing the audits will be on Sunday starting from 8 am.

Audit Execution

Firewall Testing

Vulnerability scanning

Vulnerability scanning to the firewall will be done using vulnerability assessment tool, Vigilante SecureScan NX. When performing the scan, SecureScan NX is running several phases of scans by default, which are:

1. **Port Scanning**, performing TCP and UDP scan against the target host to find any open services. This phase will be the same as what Nmap is doing. Result from this phase can be used for comparison with result gathered from scan using Nmap.

2. **OS Detection**, performing identification of the OS type used by the target system.
3. **Test Case Execution**, running the Test Cases (vulnerability signatures) against the target system. This by default will be optimized by only running relevant Test Cases for the specific OS identified during the OS Detection phase.

Figure 25 shows the GUI of SecureScan NX.

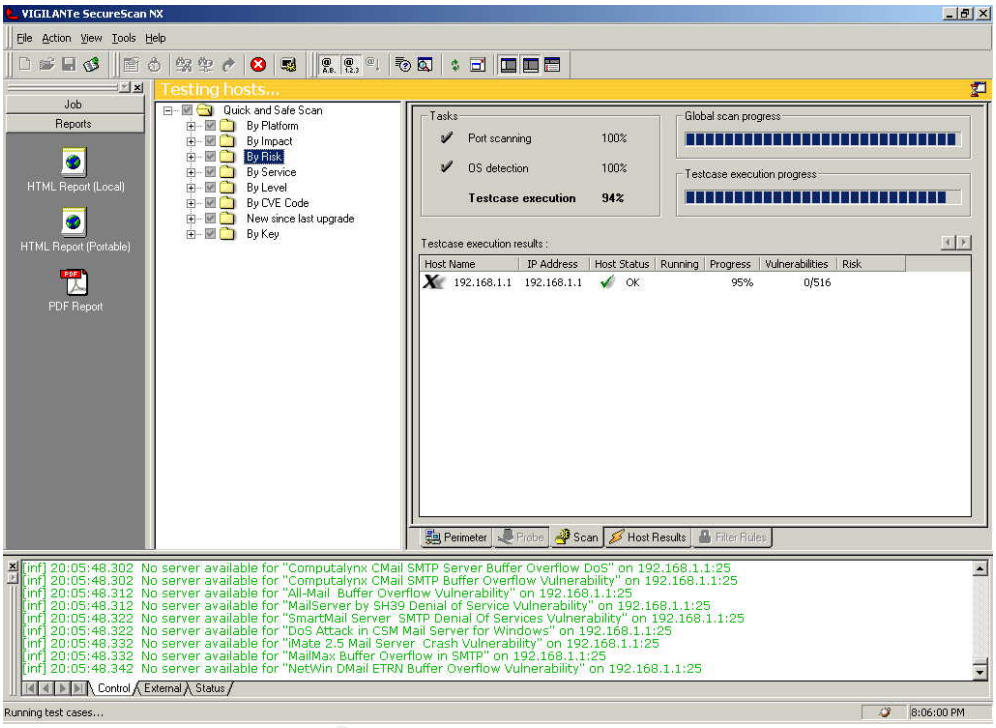

Figure 25: Vigilante SecureScan NX

The vulnerability scan is being done from each segment to each interface of the firewall. With six interfaces used on the firewall, scanning is being done six times.

Scanning execution results:

- **Scanning dec0 - 100.1.1.18**
  Port Scanning found the following ports opened: *TCP 53*, *UDP 53*, *UDP 500*
  OS Detection found the following OS: *SCO UnixWare 2.1.2*
  Test Case Execution found the following results:
    - *0* High risk vulnerabilities found
    - *0* Medium risk vulnerabilities found
    - *0* Low risk vulnerabilities found

- **Scanning dec1 - 192.168.1.1**
  Port Scanning found the following ports opened: *TCP 53*, *UDP 53*
  OS Detection found the following OS: *SCO UnixWare 2.1.2*
  Test Case Execution found the following results:

    - *0* High risk vulnerabilities found
    - *0* Medium risk vulnerabilities found
    - *0* Low risk vulnerabilities found

- **Scanning dec2 - 192.168.2.1, dec3 - 192.168.3.1, dec4 - 192.168.4.1 and dec5 - 192.168.5.1**
  Port Scanning found the following ports opened: -
  OS Detection found the following OS: *SCO UnixWare 2.1.2*
  Test Case Execution found the following results:
    - *0* High risk vulnerabilities found
    - *0* Medium risk vulnerabilities found
    - *0* Low risk vulnerabilities found

Vigilante defines the risk level[8] as follows:

- High risk - any vulnerability that can unilaterally and directly (not combined with any other vulnerability) lead to compromise the host.
- Medium risk – any vulnerability that can lead to the compromise of the host, but not by itself. They can be combined with at least one other medium vulnerability to compromise a host. Medium risk vulnerability in conjunction with information gathered from several low risk vulnerabilities can lead to compromise a host.
- Low risk – vulnerability that makes a host more susceptible to further compromise.

Port Scanning results from each interface can be summarized that on the external dec0, DNS ports and IKE are opened; on the dec1, DNS ports are opened; other interfaces no ports are opened. These open ports found are expected.

OS Detection has found that the OS used by the system is SCO UnixWare 2.1.2, which is the correct result, because CyberGuard firewall UnixWare OS actually originated from this version from SCO, which then heavily modified.

Test Case Execution has found no vulnerabilities on the firewall host. Three categories of vulnerabilities are reporting zero results.
Checking on the firewall itself, no damages have happened, and the firewall still functioning as per normal.

Service scanning

Service scanning on the firewall will be done using Nmap to perform port scan and OS detection against the firewall host. Similarly, the scans will be done to each of firewall interfaces. Port 1 to 65535 will be scanned and no host discovery will be performed (ICMP or TCP ping).
The results from Nmap can be compared to the results from Vigilante SecureScan NX.

[8] Taken from Sample Report at URL:
http://www.vigilante.com/securescan/perimeter/sample_report/scex_classic.zip

In general, the scans will be executed with the following syntax:

Scan type	Syntax
SYN scan	`nmap -P0 -sS –O target_IP -p1-65535`
UDP scan	`nmap -P0 -sU target_IP -p1-65535`

Options used on the commands:

Option	Description
`nmap`	Nmap executable
`-P0`	Do not try to ping before scan
`-sS`	Perform SYN scan
`-sU`	Perform UDP scan
`-O`	Perform OS identification
target_IP	IP address of the host to be scanned
`-p1-65535`	Scan port 1 to 65535

Scan results with Nmap:

- **Scanning dec0 – 100.1.1.18 and dec1 – 192.168.1.1**

  SYN scan with the commands:

```
nmap -P0 -sS -O 100.1.1.18 -p1-65535
nmap -P0 -sS –O 192.168.1.1 -p1-65535
```

  Generate the following results:

```
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
53/tcp     open        domain
Remote operating system guess: SCO UnixWare 2.1.2
```

  UDP scan with the command:

```
nmap -P0 -sU 100.1.1.18 -p1-65535
nmap -P0 -sU 192.168.1.1 -p1-65535
```

  Generate the following result:

```
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
53/udp     open        domain
```

- **Scanning dec2 – 192.168.2.1, dec3 – 192.168.3.1, dec4 – 192.168.4.1 and dec5 – 192.168.5.1**

  SYN scan with the following commands:

```
nmap -P0 -sS 192.168.2.1 -p1-65535
nmap -P0 -sS 192.168.3.1 -p1-65535
nmap -P0 -sS 192.168.4.1 -p1-65535
nmap -P0 -sS 192.168.5.1 -p1-65535

nmap -P0 -sU 192.168.2.1 -p1-65535
nmap -P0 -sU 192.168.3.1 -p1-65535
nmap -P0 -sU 192.168.4.1 -p1-65535
nmap -P0 -sU 192.168.5.1 -p1-65535
```

Generate the same result: all ports scanned are closed.

Summary for service scanning on the firewall, open ports found are DNS ports (TCP and UDP port 53) on the dec0, 100.1.1.18 and dec1, 192.168.1.1. These open ports are expected. Somehow, Nmap doesn't found IKE port open on the external interface. The rest of the ports scanned are found closed.
Nmap guess the OS of the firewall as SCO Unixware 2.1.2.

Comparing the results from Vigilante Securescan NX and Nmap, they gather similar results, except for the IKE port, which found by Vigilante Securescan NX, but not by Nmap.

Firewall Rules Verification

Testing will be conducted following the planning. When performing the scanning using Nmap, P0 option is used to avoid the scanner performing host discovery (ICMP ping) before doing the port scan. The firewall is prohibiting ping, so the scan will not be able to continue the scan if the option is not enabled. Scan will be performed for port 1 to 65535. Syntax of the scans is similar to the ones used for service scanning on firewall testing. One unused IP address, 100.1.1.29, is used as the target address when scanning to EXTERNAL segment
.
In the GIAC network, there are six segments connected and separated by the firewall. Scanning sequence will be done as follows:

1. **Scanning from EXTERNAL segment**
   From the EXTERNAL segment, every host in the Internet is able to connect to certain services behind the firewall. For the scanning purpose, one public IP address of the EXTERNAL segment, 100.1.1.30, is used to represent the rest of the Internet, since all of them will have same rules through the firewall.
   Additionally, the router, which also located in the EXTERNAL segment, is configured to send log to Syslog server behind the firewall. With this condition, the router IP address will also be used to scan, to see what can be reached behind the firewall using it.
   With the firewall performing Dynamic NAT, only addresses configured with Static NAT can be reached from Internet, so only these addresses will be tested. The

INTERNAL1 and INTERNAL2 segments will not be scanned, since there are no Static NAT mappings to the hosts in those segments.

From		To	
Segment Name	**IP Address**	**Segment Name**	**IP Address**
EXTERNAL	100.1.1.30	INTERNAL1	-
		INTERNAL2	-
		SRVNET1	100.1.1.19
		SRVNET2	100.1.1.20
		SRVNET3	100.1.1.21
	100.1.1.17	INTERNAL1	-
		INTERNAL2	-
		SRVNET1	100.1.1.19
		SRVNET2	100.1.1.20
		SRVNET3	100.1.1.21

SYN scan from 100.1.1.30 to 100.1.1.19 with the command:

```
nmap -P0 -sS 100.1.1.19 –p1-65535
```

Generate the result:

```
(The 65533 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
53/tcp     filtered    domain
```

The firewall logs record the following permitted connection:

```
Date                                    : Mon Mar  3 13:53:20 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Proxy
    Source                              : 100.1.1.30
      Interface                         : dec0
      Port                              : 49816
    Destination                         : 192.168.3.2
      Interface                         : dec3
      Port                              : 25
    Protocol                            : tcp
      Flags                             : 0x2
       Direction                        : Receive
```

Windump doesn't record any connection from 100.1.1.30

SYN scan from 100.1.1.30 to 100.1.1.20 with the command:

```
nmap -P0 -sS 100.1.1.20 –p1-65535
```

Generate the result:

```
(The 65532 ports scanned but not shown below are in state: closed)
Port       State       Service
53/tcp     filtered    domain
80/tcp     open        http
443/tcp    open        https
```

Firewall log records two permitted connections, one for http and one for https:

```
Date                                    : Mon Mar  3 14:19:32 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Proxy
    Source                              : 100.1.1.30
      Interface                         : dec0
      Port                              : 48246
    Destination                         : 192.168.4.2
      Interface                         : dec4
      Port                              : 80
    Protocol                            : tcp
      Flags                             : 0x2
    Direction                           : Receive
```

For simplicity, log record for https is not shown here, but similar to the record above, except that the port is 443 instead of 80.

Windump doesn't record any connection from 100.1.1.30

SYN scan from 100.1.1.30 to 100.1.1.21 with the command:

```
nmap -P0 -sS 100.1.1.21 –p1-65535
```

Found all ports scanned closed.
Firewall logs doesn't record any permitted connections.
Windump doesn't record any connection from 100.1.1.30.

UDP scan from 100.1.1.30 to the three addresses with the commands:

```
nmap -P0 -sU 100.1.1.19 –p1-65535
nmap -P0 -sU 100.1.1.20 –p1-65535
nmap -P0 -sU 100.1.1.21 –p1-65535
```

Found all ports scanned closed.
Firewall logs doesn't record any permitted connections.
Windump doesn't record any connection from 100.1.1.30

Scanning from 100.1.1.17 (router address) with similar commands issued as with the scanning from 100.1.1.30, all the results are the same, except for UDP scanning to 100.1.1.21.

UDP scanning from 100.1.1.17 to 100.1.1.21, with the command:

```
nmap -P0 -sU 100.1.1.21 –p1-65535
```

Generate the following results:

```
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
514/udp    open        syslog
```

Firewall log shows the following:

```
Date                                : Mon Mar  3 14:25:17 2003
Event name                          : ng_permit
Process(lwp) id                     : -1
Status(code)                        : Success
  Credentials:
    User(Real:Effective)            : nobody:nobody
    Group(Real:Effective)           : nobody:nobody
    Session id                      : -1
  Netguard Packet                   : Permit
    Source                          : 100.1.1.17
      Interface                     : dec0
      Port                          : 41441
    Destination                     : 192.168.5.3
      Interface                     : dec5
      Port                          : 514
    Protocol                        : udp
    Direction                       : Receive
```

Windump captures the following:

```
14:25:19.026093 100.1.1.17.41441 > 192.168.1.2.514:  udp 0
```

2. Scanning from INTERNAL1 segment

From this segment, 3 addresses are used to scan other segments. Two are the domain controllers addresses, 192.168.1.11 and 192.168.1.12, which have several specific rules defined for them in the firewall. The third address, 192.168.1.150, is one of the workstation addresses, which used to represent other workstations which have similar access through the firewall.

From		To	
Segment Name	**IP Address**	**Segment Name**	**IP Address**
INTERNAL1	192.168.1.11	EXTERNAL	100.1.1.29
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2
		SRVNET3	192.168.5.2
			192.168.5.3
	192.168.1.12	EXTERNAL	100.1.1.29
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2
		SRVNET3	192.168.5.2
			192.168.5.3
	192.168.1.150	EXTERNAL	100.1.1.29
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2
		SRVNET3	192.168.5.2
			192.168.5.3

SYN scan is done from each of the two addresses 192.168.1.11 and 192.168.1.12 with the following commands:

```
nmap -P0 -sS 100.1.1.29 –p1-65535
nmap -P0 -sS 192.168.2.2 –p1-65535
nmap -P0 -sS 192.168.3.2 –p1-65535
nmap -P0 -sS 192.168.4.2 –p1-65535
nmap -P0 -sS 192.168.5.2 –p1-65535
nmap -P0 -sS 192.168.5.3 –p1-65535
```

UDP scan is done from each of the two addresses 192.168.1.11 and 192.168.1.12 with the following commands:

```
nmap -P0 -sU 100.1.1.29 –p1-65535
nmap -P0 -sU 192.168.2.2 –p1-65535
nmap -P0 -sU 192.168.3.2 –p1-65535
nmap -P0 -sU 192.168.4.2 –p1-65535
nmap -P0 -sU 192.168.5.2 –p1-65535
nmap -P0 –sU 192.168.5.3 –p1-65535
```

From both scans, all ports scanned are found closed.
Firewall log doesn't show any permitted traffic from 192.168.1.11 and 192.168.1.12.
Same thing happened on Windump.

SYN scan is done from 192.168.1.150 to 100.1.1.29 with the following command:

```
nmap -P0 -sS 100.1.1.29 –p1-65535
```

The scan shows the following result:

```
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
443/tcp    open        https
```

Firewall log captures the permitted traffic for the four open ports, as follows:

```
Date                                    : Mon Mar  3 14:51:08 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Proxy
    Source                              : 192.168.1.150
      Interface                         : dec1
      Port                              : 48241
    Destination                         : 100.1.1.29
      Interface                         : dec0
      Port                              : 21
    Protocol                            : tcp
      Flags                             : 0x2
    Direction                           : Receive
```

Only one shown here, the other three are similar with different port values - 25, 80 and 443.

However, Windump doesn't capture any traffic from 100.1.1.18 (translating the original address 192.168.1.150).

UDP scan from 192.168.1.150 to 100.1.1.29 with the following command:

```
nmap -P0 -sU 100.1.1.29 –p1-65535
```

Found all ports scanned closed, no permitted traffic on the firewall as well as on Windump.

SYN scan from 192.168.1.150 to 192.168.2.2 (*giac-db*) with the following command:

```
nmap -P0 -sS 192.168.2.2 –p1-65535
```

Generate the following result:

```
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
1433/tcp   open        ms-sql-s
```

Firewall log captures the connection as shown below:

```
Date                                    : Mon Mar  3 15:01:15 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Permit
    Source                              : 192.168.1.150
      Interface                         : dec1
      Port                              : 17588
    Destination                         : 192.168.2.2
      Interface                         : dec2
      Port                              : 1433
    Protocol                            : tcp
      Flags                             : 0x2
    Direction                           : Receive
```

Windump shows the following:

```
15:02:24.866564 192.168.1.150.17588 > 192.168.2.2.1433: S
3678866036:3678866036(0) win 3072
```

UDP scan from 192.168.1.150 to 192.168.2.2 (*giac-db*) with the following command:

```
nmap -P0 -sU 192.168.2.2 –p1-65535
```

Found all ports scanned closed, no permitted traffic on the firewall and Windump.

SYN scan from 192.168.1.150 to 192.168.3.2 (*giac-mail*) with the following command:

```
nmap -P0 -sS 192.168.3.2 –p1-65535
```

Found the following result:

```
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
1026/tcp   open        LSA-or-nterm
1027/tcp   open        IIS
1028/tcp   open        ms-lsa
```

Firewall captures the traffic above:

```
Date                                    : Mon Mar  3 15:14:34 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Permit
    Source                              : 192.168.1.150
      Interface                         : dec1
      Port                              : 11359
    Destination                         : 192.168.3.2
      Interface                         : dec3
      Port                              : 135
    Protocol                            : tcp
      Flags                             : 0x2
    Direction                           : Receive
```

Other ports, which are 1026, 1027 and 1028 also shown in the similar log records not shown here.

Windump also captures them:

```
15:15:11.506564 192.168.1.150.11359 > 192.168.3.2.135: S
2396814955:2396814955(0) win 3072

15:17:14.066564 192.168.1.150.11359 > 192.168.3.2.1026: S
3678866036:3678866036(0) win 3072

15:15:13.746564 192.168.1.150.11360 > 192.168.3.2.1027: S
4134619797:4134619797(0) win 3072

15:16:12.786564 192.168.1.150.11359 > 192.168.3.2.1028: S
4134619797:4134619797(0) win 3072
```

UDP scan from 192.168.1.150 to 192.168.3.2 (*giac-mail*) with the following command:

```
nmap -P0 -sU 192.168.3.2 –p1-65535
```

Found all ports scanned closed, no permitted traffic record on the firewall log and none on Windump.

SYN scan from 192.168.1.150 to 192.168.4.2 (*giac-web*) with the following command:

```
nmap -P0 -sS 192.168.4.2 –p1-65535
```

Found the following result:

```
(The 65533 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
443/tcp    open        https
```

Firewall log shown the permitted traffic:

```
Date                                    : Mon Mar  3 15:32:46 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Proxy
    Source                              : 192.168.1.150
      Interface                         : dec1
      Port                              : 18352
    Destination                         : 192.168.4.2
      Interface                         : dec4
      Port                              : 80
    Protocol                            : tcp
      Flags                             : 0x2
    Direction                           : Receive
```

Only log for port 80 shown here, but 443 is similar to this.
Windump doesn't capture anything.

UDP scan from 192.168.1.150 to 192.168.4.2 (*giac-web*) with the following command:

```
nmap -P0 -sU 192.168.4.2 –p1-65535
```

Found all ports scanned closed.
Firewall log doesn't show any permitted traffic, and Windump doesn't capture any traffic.

SYN scan and UDP scan from 192.168.1.150 to 192.168.5.2 (*giac-avs*) and 192.168.5.3 (*giac-log*) with the following commands respectively:

```
nmap -P0 -sS 192.168.5.2-3 –p1-65535
nmap -P0 -sU 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.
Firewall log doesn't capture any permitted traffic, and Windump doesn't capture any traffic from 192.168.1.150.

3. Scanning from INTERNAL2 segment

The *giac-db* address, 192.168.2.2 is used to scan other segments. Additionally, unused IP address, 192.168.2.10, will also be used.

From		To	
Segment Name	**IP Address**	**Segment Name**	**IP Address**
INTERNAL2	192.168.2.2	EXTERNAL	100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2
		SRVNET3	192.168.5.2
			192.168.5.3
	192.168.2.10	EXTERNAL	100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2
		SRVNET3	192.168.5.2
			192.168.5.3

SYN scan from both addresses to addresses in other segments with the following commands:

```
nmap -P0 -sS 100.1.1.29 –p1-65535
nmap -P0 -sS 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sS 192.168.3.2 –p1-65535
nmap -P0 -sS 192.168.4.2 –p1-65535
nmap -P0 -sS 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.

Similarly, UDP scan with the following commands:

```
nmap -P0 -sU 100.1.1.29 –p1-65535
nmap -P0 -sU 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sU 192.168.3.2 –p1-65535
nmap -P0 -sU 192.168.4.2 –p1-65535
nmap -P0 -sU 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.

Firewall log doesn't capture any permitted traffic for the two types of scans. Windump also doesn't capture any traffic generated from the scanner addresses.

4. Scanning from SRVNET1 segment

The *giac-mail* address, 192.168.3.2 and unused address, 192.168.3.10 are used to scan other segments.

From		To	
Segment Name	**IP Address**	**Segment Name**	**IP Address**
SRVNET1	192.168.3.2	EXTERNAL	100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		INTERNAL2	192.168.2.2
		SRVNET2	192.168.4.2
		SRVNET3	192.168.5.2
			192.168.5.3
	192.168.3.10	EXTERNAL	100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		INTERNAL2	192.168.2.2
		SRVNET2	192.168.4.2
		SRVNET3	192.168.5.2
			192.168.5.3

SYN scan from 192.168.3.2 (*giac-mail*) to 100.1.1.29 with the following command:

```
nmap -P0 -sS 192.168.2.2 -p1-65535
```

Generate the following result:

```
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
```

Firewall captures the following:

```
Date                                    : Mon Mar  3 15:46:48 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Proxy
    Source                              : 192.168.3.2
      Interface                         : dec3
      Port                              : 18450
    Destination                         : 100.1.1.29
```

```
      Interface                       : dec4
      Port                            : 25
    Protocol                          : tcp
      Flags                           : 0x2
    Direction                         : Receive
```

Windump doesn't capture any traffic from 100.1.1.18 (firewall is translating the original address 192.168.3.2).

SYN scan from 192.168.3.2 (*giac-mail*) to 192.168.1.11, 192.168.1.12 and 192.168.1.129 to 192.168.1.254 with the following command:

```
nmap -P0 -sS 192.168.1.11-12,129-254 -p1-65535
```

Generate the following result for 192.168.1.11 and 192.168.1.12:

```
(The 65528 ports scanned but not shown below are in state: closed)
Port       State       Service
53/tcp     open        domain
88/tcp     open        kerberos-sec
135/tcp    open        loc-srv
389/tcp    open        ldap
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
3268/tcp   open        globalcatLDAP
```

Firewall log captures permitted traffic on the following:

```
Date                                  : Mon Mar  3 16:04:11 2003
Event name                            : ng_permit
Process(lwp) id                       : -1
Status(code)                          : Success
  Credentials:
    User(Real:Effective)              : nobody:nobody
    Group(Real:Effective)             : nobody:nobody
    Session id                        : -1
  Netguard Packet                     : Permit
    Source                            : 192.168.3.2
      Interface                       : dec3
      Port                            : 26554
    Destination                       : 192.168.1.11
      Interface                       : dec1
      Port                            : 53
    Protocol                          : tcp
      Flags                           : 0x2
    Direction                         : Receive
```

The rest of the log records for other ports captured are similar to this, as well as the scans to 192.168.1.12.

Windump captures the following traffic from 192.168.3.2:

```
16:05:02.646564 192.168.3.2.26554 > 192.168.1.11.53: S
4019927700:4019927700(0) win 4096

16:05:02.646564 192.168.3.2.26554 > 192.168.1.11.88: S
4019927700:4019927700(0) win 4096

16:05:02.646564 192.168.3.2.26555 > 192.168.1.11.135: S
4019927700:4019927700(0) win 4096

16:05:02.646564 192.168.3.2.26554 > 192.168.1.11.389: S
4019927700:4019927700(0) win 4096

16:05:02.656564 192.168.3.2.26555 > 192.168.1.11.445: S
4019927700:4019927700(0) win 4096

16:05:02.656564 192.168.3.2.26554 > 192.168.1.11.1025: S
4019927700:4019927700(0) win 4096

16:05:02.656564 192.168.3.2.26554 > 192.168.1.11.3268: S
4019927700:4019927700(0) win 4096
```

Traffic captured by Windump from the scan to 192.168.1.12 are similar to these. UDP scan from 192.168.3.2 (*giac-mail*) to 192.168.1.11, 192.168.1.12 and 192.168.1.129 to 192.168.1.254 with the following command:

```
nmap -P0 -sU 192.168.1.11-12,129-254 -p1-65535
```

Generate the following result for scan to 192.168.1.11 and 192.168.1.12:

```
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
53/udp     open        domain
88/udp     open        kerberos-sec
123/udp    open        ntp
389/udp    open        ldap
```

Firewall log captures the following:

```
Date                                    : Mon Mar  3 16:15:47 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Permit
    Source                              : 192.168.3.2
      Interface                         : dec3
      Port                              : 41352
    Destination                         : 192.168.1.11
      Interface                         : dec1
      Port                              : 53
    Protocol                            : udp
```

```
Direction                              : Receive
```

The log record above is for UDP port 53, the rest will be the similar, with different port values, which are 88, 123 and 389.

Windump captures the following:

```
14:25:19.244758 192.168.3.2.41352 > 192.168.1.11.53:  udp 0

14:25:19.244990 192.168.3.2.41352 > 192.168.1.11.88:  udp 0

14:25:19.244324 192.168.3.2.41352 > 192.168.1.11.123:  udp 0

14:25:19.554198 192.168.3.2.41352 > 192.168.1.11.389:  udp 0
```

Similar traffic captured by Windump for scans to 192.168.1.12.

For both scans to 192.168.1.129 to 192.168.1.254, all ports scanned are closed, with firewall log doesn't capture any permitted traffic. Windump also doesn't capture any traffic from the scanner address.

SYN scan from 192.168.3.2 (*giac-mail*) to 192.168.2.2, 192.168.4.2, 192.168.5.2 and 192.168.5.3 with the following commands:

```
nmap -P0 -sS 192.168.2.2 –p1-65535
nmap -P0 -sS 192.168.4.2 –p1-65535
nmap -P0 -sS 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.

UDP scan from 192.168.3.2 (*giac-mail*) to 100.1.1.29, 192.168.4.2, 192.168.5.2 and 192.168.5.3 with the following commands:

```
nmap -P0 -sU 100.1.1.29 –p1-65535
nmap -P0 -sU 192.168.2.2 –p1-65535
nmap -P0 -sU 192.168.4.2 –p1-65535
nmap -P0 -sU 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.

SYN scan and UDP scan from 192.168.3.10 (unused IP address) to all target addresses in other segments with the following commands:

```
nmap -P0 -sS 100.1.1.29 –p1-65535
nmap -P0 -sS 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sS 192.168.2.2 –p1-65535
nmap -P0 -sS 192.168.4.2 –p1-65535
nmap -P0 -sS 192.168.5.2-3 –p1-65535

nmap -P0 -sU 100.1.1.29 –p1-65535
```

```
nmap -P0 -sS 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sS 192.168.2.2 –p1-65535
nmap -P0 -sU 192.168.4.2 –p1-65535
nmap -P0 -sU 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.

For all scans found scanned ports closed, firewall log doesn't capture permitted traffic, and Windump doesn't capture traffic originated from the scanner addresses.

5. Scanning from SRVNET2 segment

The *giac-web* address, 192.168.4.2 and unused address, 192.168.4.10 are used to scan other segments.

From		To	
Segment Name	**IP Address**	**Segment Name**	**IP Address**
SRVNET2	192.168.4.2	EXTERNAL	100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET3	192.168.5.2
			192.168.5.3
	192.168.4.10	EXTERNAL	100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET3	192.168.5.2
			192.168.5.3

SYN scan from 192.168.4.2 (*giac-web*) to 192.168.2.2 (*giac-db*) with the following command:

```
nmap -P0 -sS 192.168.2.2 –p1-65535
```

Generate the following result:

```
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
1433/tcp   open        ms-sql-s
```

Firewall captures the traffic:

```
Date                                    : Mon Mar  3 16:27:33 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Permit
    Source                              : 192.168.4.2
      Interface                         : dec4
      Port                              : 1656
    Destination                         : 192.168.2.2
      Interface                         : dec2
      Port                              : 1433
    Protocol                            : tcp
      Flags                             : 0x2
    Direction                           : Receive
```

Windump captures the traffic:

```
16:28:51.206564 192.168.4.2.1656 > 192.168.2.2.1433: S
2396814955:2396814955(0) win 3072
```

SYN scan from 192.168.4.10 (*giac-web*) to 192.168.2.2 (*giac-db*) with the following command:

```
nmap -P0 -sS 192.168.2.2 –p1-65535
```

Found all ports scanned closed.

SYN scan from both addresses to the rest of addresses in other segments with the following commands:

```
nmap -P0 -sS 100.1.1.29 –p1-65535
nmap -P0 -sS 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sS 192.168.3.2 –p1-65535
nmap -P0 -sS 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.

UDP scan to all addresses in other segments with the following commands:

```
nmap -P0 -sU 100.1.1.29 –p1-65535
nmap -P0 -sU 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sU 192.168.2.2 –p1-65535
nmap -P0 -sU 192.168.3.2 –p1-65535
nmap -P0 -sU 192.168.5.2-3 –p1-65535
```

Found all ports scanned closed.

For the scans found ports closed, firewall log doesn't capture any permitted traffic, and Windump doesn't capture traffic from scanner addresses.

6. Scanning from SRVNET3 segment

The *giac-avs* address, 192.168.5.2, *giac-log* address, 192.168.5.3 and unused address, 192.168.5.10 are used to scan other segments.

From		To	
Segment Name	**IP Address**	**Segment Name**	**IP Address**
SRVNET3	192.168.5.2	EXTERNAL	100.1.1.17
			100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2
	192.168.5.3	EXTERNAL	100.1.1.17
			100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2
	192.168.5.10	EXTERNAL	100.1.1.17
			100.1.1.29
		INTERNAL1	192.168.1.11
			192.168.1.12
			192.168.1.129-254
		INTERNAL2	192.168.2.2
		SRVNET1	192.168.3.2
		SRVNET2	192.168.4.2

SYN scan from 192.168.5.2 to 100.1.1.17 (router) and 100.1.1.29 with the command:

```
nmap -P0 -sS 100.1.1.17,29 -p1-65535
```

Generate the following result for 100.1.1.29:

```
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
80/tcp     open        http
```

Firewall log captures the following:

```
Date                                    : Mon Mar  3 16:51:08 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Proxy
    Source                              : 192.168.5.2
      Interface                         : dec5
      Port                              : 45935
    Destination                         : 100.1.1.29
      Interface                         : dec0
      Port                              : 80
    Protocol                            : tcp
      Flags                             : 0x2
    Direction                           : Receive
```

Windump doesn't capture any traffic from 100.1.1.18 (firewall translating original address 192.168.5.2)

Scan to 100.1.1.17 shows all ports scanned closed, with the firewall log doesn't capture any permitted traffic, and Windump doesn't capture traffic from the scanner.

SYN scan from 192.168.5.3 to 100.1.1.17 (router) and 100.1.1.29 with the command:

```
nmap -P0 -sS 100.1.1.17,29 -p1-65535
```

Generate the following result for 100.1.1.17:

```
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet
```

Firewall log captures the following:

```
Date                                    : Mon Mar  3 16:59:31 2003
Event name                              : ng_permit
Process(lwp) id                         : -1
Status(code)                            : Success
  Credentials:
    User(Real:Effective)                : nobody:nobody
    Group(Real:Effective)               : nobody:nobody
    Session id                          : -1
  Netguard Packet                       : Permit
    Source                              : 192.168.5.3
      Interface                         : dec5
      Port                              : 1653
    Destination                         : 100.1.1.17
```

```
    Interface                       : dec0
    Port                            : 23
  Protocol                          : tcp
    Flags                           : 0x2
  Direction                         : Receive
```

Windump captures the following:

```
17:00:49.363687 100.1.1.17.21558 > 100.1.1.17.23: S
3076462020:3076462020(0) win 3072
```

Scan to 100.1.1.29 shows all ports scanned closed, with the firewall log doesn't capture any permitted traffic, and Windump doesn't capture traffic from the scanner.

SYN scan from 192.168.5.2 and 192.168.5.3 to target addresses in internal segments, with the following commands:

```
nmap -P0 -sS 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sS 192.168.2.2 –p1-65535
nmap -P0 -sS 192.168.3.2 –p1-65535
nmap -P0 -sS 192.168.4.2 –p1-65535
```

Found all ports scanned closed.
Firewall log captures no permitted traffic, and Windump also doesn't capture traffic from the scanner.

UDP scan from 192.168.5.2 and 192.168.5.3 to all target addresses in other segments with the commands:

```
nmap -P0 -sU 100.1.1.17,29 –p1-65535
nmap -P0 -sU 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sU 192.168.2.2 –p1-65535
nmap -P0 -sU 192.168.3.2 –p1-65535
nmap -P0 -sU 192.168.4.2 –p1-65535
```

Found all ports scanned closed.
Firewall log captures no permitted traffic, and Windump also doesn't capture traffic from the scanner.

SYN scans and UDP scans from 192.168.5.10 to all target addresses in other segments with the following commands:

```
nmap -P0 -sS 100.1.1.17,29 –p1-65535
nmap -P0 -sS 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sS 192.168.2.2 –p1-65535
nmap -P0 -sS 192.168.3.2 –p1-65535
nmap -P0 -sS 192.168.4.2 –p1-65535

nmap -P0 -sU 100.1.1.17,29 –p1-65535
nmap -P0 -sU 192.168.1.11-12,129-254 –p1-65535
nmap -P0 -sU 192.168.2.2 –p1-65535
```

```
nmap -P0 -sU 192.168.3.2 –p1-65535
nmap -P0 -sU 192.168.4.2 –p1-65535
```

Found all ports scanned closed, firewall doesn't log any permitted traffic, and Windump doesn't capture any traffic from the scanner address.

Summary of firewall rules verification:

- Comparing the results on firewall rules verification with firewall policy, can be said that open ports found are supposed to be opened, and closed or blocked ports are also blocked by the firewall.
- All traffic for open ports found by the scanner are captured on the firewall log as permitted traffic. However, not all of these traffic are captured by Windump, which was located at the target segments.
- None of the traffic for closed ports found by the scanner are captured on the firewall as permitted traffic and neither they captured by Windump.

Proxy Services Testing

Testing HTTP Proxy

From the external segment, telnet command is executed against the IP address of the web server, 100.1.1.20. Testing will be done three times, each with different command, POST, PUT and DELETE.

POST command:

```
Telnet 100.1.1.20 80
Trying 100.1.1.20...
Connected to 100.1.1.20.
Escape character is '^]'.
POST / HTTP/1.0
```

PUT command:

```
Telnet 100.1.1.20 80
Trying 100.1.1.20...
Connected to 100.1.1.20.
Escape character is '^]'.
PUT / HTTP/1.0
```

DELETE command:

```
Telnet 100.1.1.20 80
Trying 100.1.1.20...
Connected to 100.1.1.20.
Escape character is '^]'.
DELETE / HTTP/1.0
```

For the three commands execution above, the HTTP Proxy return the following:

```
HTTP/1.0 403 Forbidden
Date: Friday, 14-Mar-03 04:48:01 GMT
Server: Web_Proxy
Content-type: text/html
Connection: close

<HTML>
<TITLE>Web Proxy</TITLE>
<HR>
<H1>Web Proxy</H1>
<HR>

<H3>This site is protected by a firewall.
All requests are screened and logged.</H3><P>

<H2>You are not permitted to access the requested URL /.</H2><P>

<HR>
<center>
<H4>For further information contact:
<ADDRESS>admin@giac.com</ADDRESS></H4>
</center>
</HTML>
```

The HTTP Proxy is rejecting the execution of those commands, as stated in the Firewall policy.

Testing SMTP Proxy

From the external segment, using IP address 100.1.1.29, telnet command is executed against the IP address of the web server, 100.1.1.20. Connection will be done to test whether mail relaying is allowed.

Mail relay testing:

```
Telnet 100.1.1.20 80
Trying 100.1.1.20...
Connected to 100.1.1.20.
Escape character is '^]'.
220 fw SMTP Proxy Service Ready (Version: Mon Apr 29 10:19:16 EDT 2002)
HELO mail.test.com
250 fw Hello 100.1.1.29 [100.1.1.29], pleased to meet you
MAIL FROM:<mytest@test.com>
250 MAIL FROM:sony2@mytest.com
RCPT TO:<mytest@test.com>
550 Relaying not allowed
```

The SMTP Proxy is rejecting the sending of email to *mytest@test.com*, because it only allow recipients address with *giac.com* domain.

Audit Evaluation and Recommendation

Audit Analysis and Evaluation

Analyzing and evaluating the audit results, below are several things to point out:

- Generally, the audit results reflecting that the firewall configuration has clearly implement the defined firewall policy.

- Taking note from the port scans (SYN scan and UDP scan) with Nmap to or through the firewall, the results for ports that not found opened are stated as closed. But when checks are done against firewall log, these ports are not permitted (denied). Another checks with Windump shows that there are no closed ports traffic passing through the firewall from the scanner address. This means that the firewall is blocking the traffic. Normally with Nmap, if the traffic is blocked by the firewall, they should be stated as filtered.
  Further analysis shows that although the firewall is blocking the traffic, it sends replies to the sender. Meaning it sent RST packets for SYN scan and ICMP unreachable for UDP scan.
  This is due to the default deny rule as the last rule, which has ENABLE_REPLY option turned on.
  To silence the firewall, so that it will not send any replies for denied packets, ENABLE_REPLY option should be removed from the last deny rule.
  With this option removed, if SYN scan is conducted against the firewall, it will take longer to finish since the scanner will need to wait for timeout before decides that the ports are blocked by the firewall. Nmap will then also state not opened ports as filtered.
  For UDP scan, removing this option will cause the scanner to give inaccurate conclusion. Either guessing all ports opened or filtered, because no ICMP unreachable packets are sent to it by the firewall.

- Several results found for open ports that actually permitted by using proxies, where the scanner found these ports as open, firewall log capture them as permitted but Windump didn't capture any traffic originating from the scanner. This is the normal behavior of the proxies in CyberGuard firewall. The proxies will wait for the TCP three way handshake process of the request from the client to complete first before they open another session to the server. The SYN scan probes only send SYN packet without further reply with ACK packet when the firewall sends SYN/ACK as the reply of the initial SYN packet.
  Further information of the permitted traffic by proxies can be seen on the related log entry, which shown that field *netguard packet* is of type *proxy* instead of *permit*.
  This behavior will be an effective solution against SYN flood attack, since the attack will stop at the firewall without even talking to the server protected by the firewall.

- The proxies are able to provide more protection beyond the packet filtering, by inspecting some part of the application layer, as proven in the testing.

Recommendations for Network Architecture Improvements

The current design of network infrastructure should be sufficient to provide adequate services and protection for the online business operations. However, it still can be improved to achieve better environment in terms of network operation as well as its security. This can be done along the way as the company grows.

Upgrading the firewall to High Availability system
The firewall used in the current environment is a single point of failure. If for any reasons it goes down, all other network components will be affected, which cause total failure to the business operation it is servicing. This situation can be improved by upgrading the firewall system to use High Availability. Using this system, two firewalls are required, in which one firewall will be active firewall, servicing the traffic and the other will be standby firewall, stand in for the active firewall. If the active firewall goes down, the standby firewall will take over to become active. During the transition between the active goes down and standby take over, there are few seconds required to make the connectivity up and running again. Two additional network interfaces are required on High Availability feature for the firewalls to check each other's status. Each of the network segments should be connected to the two firewalls. By using this system, minimum down time of the network can be achieved.

Adding several new web servers for functional separation
The current network structure is using a single web server to provide both HTTP and HTTPS traffic. HTTPS service is servicing the Partners as well as the Customers. This will make it a single point of failure. Enhancing the structure, several other web servers can be added, which have separate duties. Three web servers can be used, one serving HTTP (labeled *giac-web*), one HTTPS server for Partners (labeled *giac-sweb1*) and one HTTPS server for Customers (labeled *giac-sweb2*). If any of the server goes down, it will not affecting other servers serving for other function.

Adding second layer firewall, additional database server and mail server
Second layer firewall can be added into the network structure to protect critical servers. The domain controllers and file servers can be moved behind this second layer firewall, protecting them from the internal users and VPN users.
Because the database is a critical part of the business, the database system can also be separated into two servers, internal and external database servers (labeled *giac-intdb* and *giac-extdb* respectively). All interactive transactions to database will be performed to the external database servers. On scheduled times, the internal database server will pull the updates from the external database server. This system will ensure that there is a secure backup of the database.
Additional mail server acting as mail relay (labeled *giac-extmail*) can be added in place of the current mail server, and relocate the mail server (now labeled *giac-intmail*) behind the internal firewall. The mail relay will accept the SMTP traffic, then relay the SMTP traffic to the mail server and vice versa. Other server in the Internet will only communicate with the mail relay. This will enhance the mail system security, although the SMTP proxy actually already offered additional protection. Mail relay should be

using different mail server application from the internal mail server, and should be running under different operating system.

Placing Intrusion Detection systems into the network
Intrusion Detection systems can be installed in the network to monitor network activities and generate alerts when suspicious traffic detected. Ideally, IDS sensors are placed on each of the network segments, to provide a full view of the whole network. But placing one sensor on the external and one other in the internal would be sufficient to monitor most part of the traffic. The external sensor will monitor traffic coming in and out of the network including those who may bypass the router filters. Internal sensor will monitor the activities happened among the hosts in the internal network as well as traffic communicated to and from other segments connected to the firewall including the Internet.

Adding redundant link to Internet
With the current network relying on only one link to Internet, it introduces single point of failure. In the event of failure to the link or the ISP, the whole connection to Internet will go down as well. Additional link to Internet should be added and subscription of the line should be made not to the same ISP. With two links available, redundancy is achieved. A load balancer switch that can perform Internet link load balancing could then be introduced to the network. With this switch, the two links will be fully utilized at all time.

Enhancement on the network design is shown in Figure 26. IP addresses and other parties communicating to GIAC network are omitted from the diagram for ease of showing the new changes.

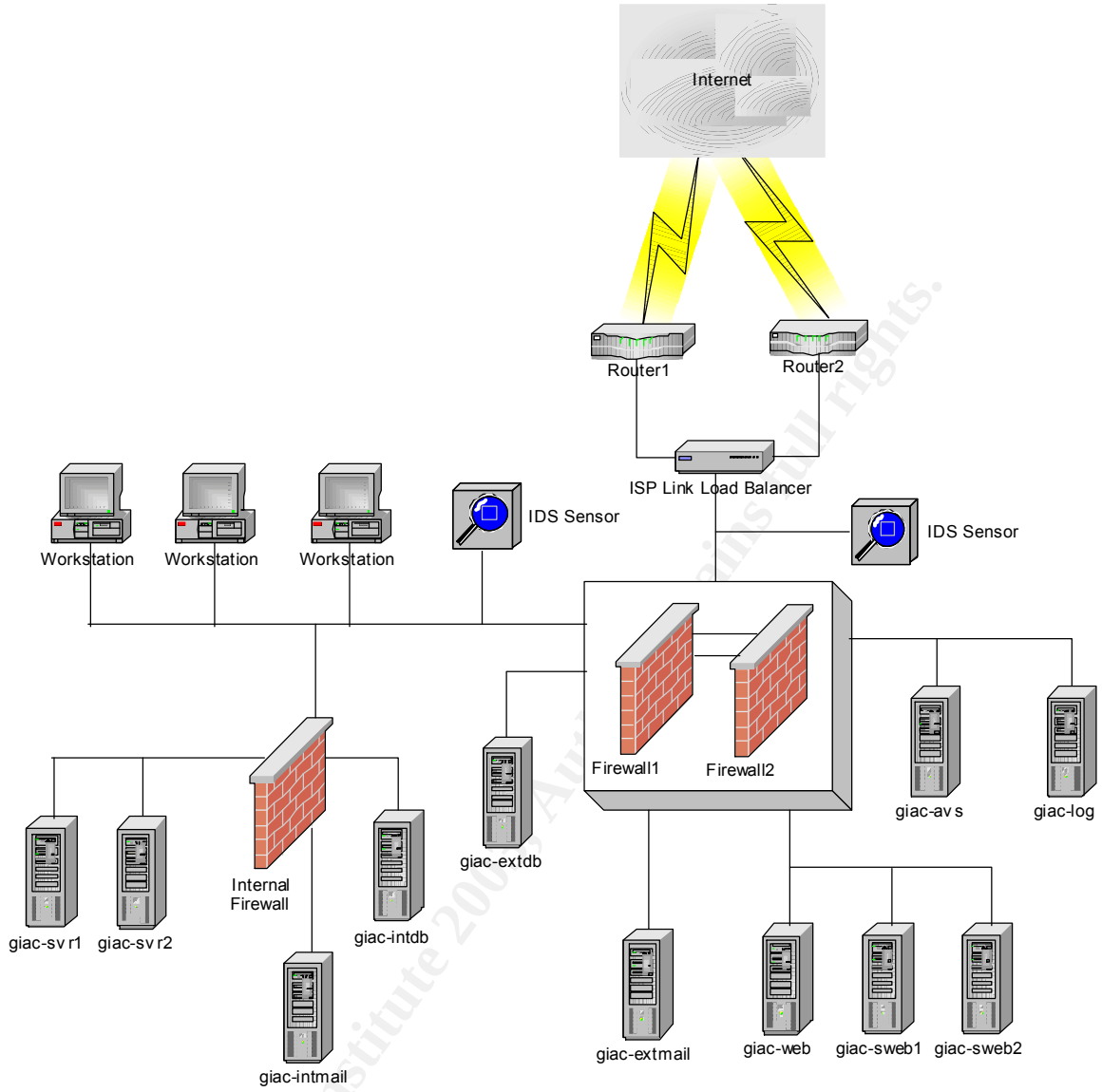

Figure 26: Enhanced GIAC Network Design

Assignment 4 – Design Under Fire

For this part of assignment, the network design done by Kevin Bong, Analyst number 0361, will be used as the target of the attacks (http://www.giac.org/practical/GCFW/Kevin_Bong_GCFW.pdf). Figure 27 shows the network diagram depicted from his practical.

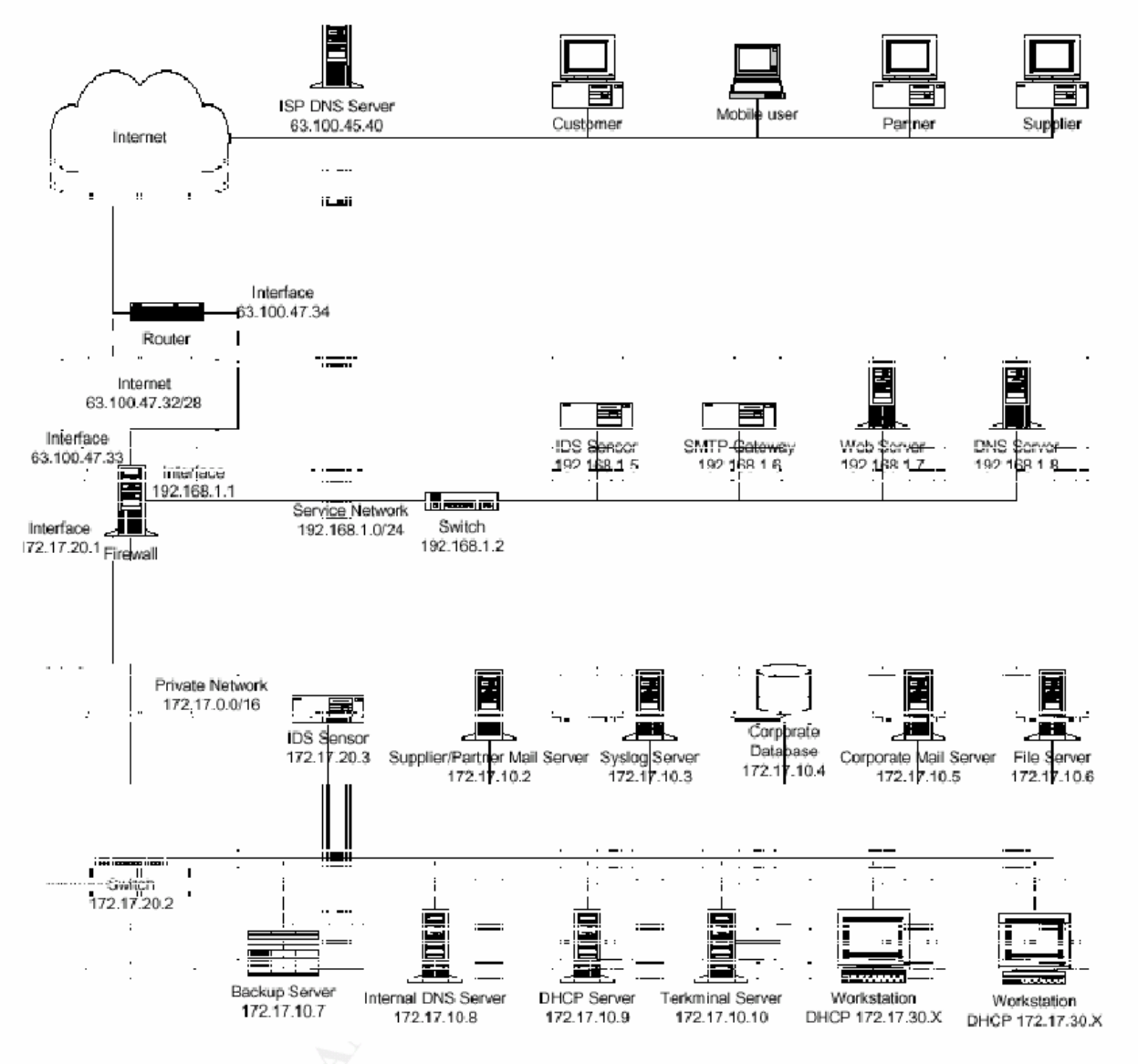

Figure 27: Kevin Bong's network design

Attack Against Firewall

Firewall used in the network design chosen is Symantec Enterprise Firewall/VPN 7.0 running on Windows 2000 Service Pack 3.

Research from the Security Focus website on vulnerabilities for this version of firewall, http://www.securityfocus.com/bid, shows several results, which the latest two are:

- **Symantec Enterprise Firewall RealAudio Proxy Buffer Overflow Vulnerability (BID 6389)**[9]
  This is the latest vulnerability found for Symantec Enterprise Firewall, which may have higher chances of success. Unfortunately, there are no further information can be found on how to carry out the attack, and no exploits are available. Furthermore, in Kevin's firewall policy, RealAudio Proxy is not used and disabled during his audit process.

- **Multiple Symantec HTTP Proxy Denial of Service Vulnerability (BID 5958)**[10]
  Kevin's firewall is configured to use HTTP Proxy, which make exploiting this vulnerability may have the chance of success. However, this vulnerability has been found quite some time, and there is patch available for it that maybe already applied on the firewall. This will be the attack of choice.

Firewall Attack Plan

Vulnerability chosen as discussed above is **Multiple Symantec HTTP Proxy Denial of Service Vulnerability (BID 5958)**. This vulnerability is assigned name **CAN-2002-0990** for CVE[11]. Further research of this vulnerability, is done with reference to Symantec Security Response, http://securityresponse.symantec.com/avcenter/security/Content/2002.10.11.html, another links from Security Focus, http://www.securityfocus.com/archive/1/295279 and Advance IT-Security, http://www.ai-sec.dk, a security consulting company that reported the vulnerability.

Report on the vulnerability by Advance IT-Security[12] is as follows:

```
Issue:
======
Multiple Symantec Firewall Secure Webserver timeout DoS

Problemdescription:
===================
There exists a problem in "Simple, secure webserver 1.1" which is
shipped with numerous Symantec firewalls, in which an attacker can
connect to the proxyserver from the outside, and issue a HTTP-style
CONNECT to a domain with a missing, or flawed DNS-server. The "Simple,
secure webserver 1.1" appears to wait for a timeout contacting the DNS
server, and while doing so the software does not fork and thereby
queues or drops all requests coming from other clients. The timeout
usually last up to 300 seconds. Sending subsequent requests for other
hostnames in the same flawed domain will force the Simple, secure
webserver 1.1 to stop processing requests for a long time.
```

[9] http://www.securityfocus.com/bid/6389
[10] http://www.securityfocus.com/bid/5958
[11] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0990
[12] http://www.ai-sec.dk/modules.php?op=modload&name=News&file=article&sid=29&mode=thread&order=0&thold=0

```
The exploit works regardless if the domainname in question is allowed
or not in the ACL.
```

From Symantec[13], below is the description of the vulnerability:

```
Advance IT-Security a Scandinavian security consultancy, notified
Symantec of a denial-of-service (D0S) issue they had discovered with
the web proxy component in the Symantec Enterprise Firewall. A
malicious user who is able to establish a remote connection to the
proxy server could, by requesting multiple connections to a non-
existent or erroneous internal URL, cause the proxy server to timeout
for an extended period of time. While timed out, the server fails to
process any subsequent connection requests.
```

To exploit this vulnerability, multiple crafted HTTP GET requests will be sent to the web server protected by the proxy. The HTTP proxy located at the firewall will intercept the requests before pass them to the web server. The GET requests will contain references to non-existent URL. The HTTP proxy will then try to resolve the name contained in the URL. If the firewall is vulnerable, according to the report, it will take a period of time (up to 300 seconds) to wait for the resolution and not processing any subsequent connection requests during that time. Multiple of such request will cause it to deny legitimate connection requests.

The HTTP GET request to be sent to the web server will be in the following form:

```
GET http://notexist.server.com HTTP/1.1
```

Using this form of request, while it is directed to the web server, the proxy will understand that it has to perform the name resolution of *notexist.server.com*.

To launch the request, a small program, **webi.c**, HTTP Request Packet Injection, available at SecuriTeam.com web site, http://www.securiteam.com/tools/5NP0E1P60W.html will be used. This tool will provide easier method in launching multiple requests, although additional simple script is required to run it multiple times. Each execution of the tool will only launch one request.

To check whether the firewall vulnerable to this, a simple request to the web server with browser can be used. If no reply received by the browser after the execution of the tool, then the firewall is vulnerable, or else it is not.

The real identity of the attacker can be covered, by using a remotely controlled compromised host to launch the attack. The tool will have to be transported over to that compromised host. Checking of the firewall status with web browser can be done from any host even by the real attacker machine, as this will be a normal request.

[13] http://securityresponse.symantec.com/avcenter/security/Content/2002.10.11.html

Firewall Attack Execution

Target of the attack is Kevin's web server address, which is 63.100.47.37 and non-existent server, as mentioned above, *notexist.server.com*, is used.

The tool's source code, **webi.c**, is compiled and named as **webi**, prior to be executed. To craft the request, the following syntax is used:

```
./webi –s 63.100.47.37 –u http://notexist.server.com -m GET
```

Options used explained in the following table:

Option	Description
./webi	The executable file
–s 63.100.47.37	Target web server address
–u http://notexist.server.com	URI requested
-m GET	HTTP method used

Running the tool against the web server, intercepted by the firewall proxy, resulting the following response:

```
HTTP/1.1 404 Hostname lookup failure
MIME-Version: 1.0
Server: Simple, Secure Web Server 1.1
Date: Wed, 12 Mar 2003 17:31:34 GMT
Connection: close
Content-Type: text/html

<HTML>
<HEAD><TITLE>Firewall Error: Host name lookup failure</TITLE></HEAD>
<BODY>
<H1>Host name lookup failure</H1>
The host <B>notexist.server.com</B> could not be found. Check the
spelling and try again.
</body></HTML>

webi.c - HTTP Request Packet Injection
(c) 2002 Condor (condor@stz-bg.com)
```

Checking the web server by using web browser shows that the web server is still up and responding to the requests.

On the firewall itself, the logs will show two records for each connection request, one for name lookup failure and one for the connection statistics. These could be used to detect the invalid requests.

Below are two firewall log records:

```
Mar 13 01:31:34.912 THESERVER httpd[800]: 308 Warning: can't lookup
host notexist.server.com

Mar 13 01:31:34.921 THESERVER httpd[800]: 121 Statistics: duration=0.02
id=45Cj sent=1024 rcvd=401 src=100.100.1.5/32800 op=GET
arg=http://notexist.server.com result="404 Hostname lookup failure"
proto=http
```

Running the tool multiple times also resulting the same response and checking with web browser also gives normal response. Apparently the firewall is no longer vulnerable against this exploit.
As earlier prediction, the patch for this vulnerability, provided by Symantec, has already been applied to the firewall.
To be specific, as stated in the link provided above from Symantec[14], this is the hotfix:

> **Symantec Enterprise Firewall V7.0 for Windows 2000**
> **Hotfix:SG7000-20020819-00 - ftpd httpd and axtvpn.sys**

Distributed Denial of Service Attack

DDoS Attack plan

Distributed Denial of Service attack against the chosen site will be done from 50 compromised cable modem/DSL hosts. SYN flood attack method will be used with destination to the web service on TCP port 80. This port is chosen since it is a commonly used service, which most sites will have and then can be easily confirmed by connecting to the site with web browser or telnet to port 80.

The tool of choice to carry out the attack is **TFN2K** created by Mixter (http://mixter.void.ru/tfn2k.tgz). An analysis of this tool can be found in the following URL: http://www.securiteam.com/securitynews/5YP0G000FS.html.

TFN2K consist of client and server components, where one client will issue the attack command to multiple servers. The servers will then perform the attacks against target host. In this case, the servers will be planted into the compromised hosts.
TFN2K offers flexibility because of various platforms that it can support, either Windows or Unix, which make it easier in finding the hosts for its server component.

To make it difficult to trace the attack source, communication between the client and the servers will be using random protocols, which can be UDP, TCP or ICMP. The communication will only be carried out in one direction, from the client to the servers, without requiring any replies. Every command will be sent 20 times by the client, expecting the servers will receive at least one.

[14] http://securityresponse.symantec.com/avcenter/security/Content/2002.10.11.html

When sending the request to the server, client source IP address will be spoofed randomly. Similarly, when the servers execute the attack, they will spoof randomly their source IP addresses. This is the default behavior of TFN2K.

Going further, the client will be run from a compromise host, which remotely controlled by the real attacker machine.

DDoS Attack Execution

Assumption for this part of assignment is that the 50 hosts used as launch pads are already compromised, and TFN2K servers are planted in them. A text file, *servers.txt*, containing IP addresses of the TFN2K servers is created before running the client. The target web server IP address is 63.100.47.37.

From the client's host, client is executed to send instruction to the servers to start attacking, using the following command:

```
./tfn –f servers.txt –c 5 –i 63.100.47.37 –p 80
```

The above command options are explained in the table below:

Option	Description
`Tfn`	Executable for TFN2K client
`-f servers.txt`	Obtain the list of TFN2K servers from the servers.txt file
`-c 5`	Select SYN flood as method of attack
`-i 63.100.47.37`	IP address of attack target
`-p 80`	TCP port of attack target

Once the command is executed, the client start to send instruction to the servers, and the servers start sending huge numbers of SYN packets to the web server. Using the command above, the TFN2K servers will send the packets using randomly spoofed source IP addresses. Kevin's web server is protected by HTTP proxy running on the firewall, so this SYN packets will be received by the proxy, which then send the SYN/ACK packets back as replies, and reserves the half open connection in the buffer. Because the senders spoofed their source IP addresses, the proxy will not get any replies, which in turn waste their resources to wait for the connection to complete. If the randomly spoofed IP addresses are non-existing addresses, there will be no replies sent, or else RST packets will be sent which tear down the connections.

With huge number of SYN packets sent, the bandwidth will be fill up with half open connections of web traffic. This will flood the Internet link to the site, considering that the bandwidth of the 50 hosts combined is several times much bigger than the site's link to

its ISP. The result will be disastrous since during this attacks, no legitimate traffic can come in to or go out from the network.

DDoS Countermeasures

As widely known, once occur, distributed denial of service attacks cannot be prevented or recovered completely. Mitigating the attacks is the only action that can be taken. Prevention can be done before the attacks occur. For this specific kind of attacks, the following steps can be taken.

Enabling the SYN flood protection on the firewall
Symantec Enterprise Firewall 7.0 used at the site has a SYN flood protection mechanism that can be enabled on the external interface of the firewall, to reduce the effect of SYN flood attacks. This, however, according to its configuration guide, should only be turned on when such attacks is detected, because it can affect the firewall's performance[15].

Ingress and Egress filtering at the ISP level
Ideally, all ISP should perform ingress and egress filtering on their routers so that no spoofed packets can pass through networks where they are not belongs to. Specifically for the attacks with TFN2K, if filtering has been applied at each of the ISPs, the client and the servers will not be able to spoof their IP with somebody else's because those packets will then be dropped.

Use of virus scanning and personal firewall
These two applications should be used on hosts connected to the Internet, especially those that not protected by network firewall. Virus scanning will detect, prevent and remove any suspicious files matching their signatures, provided that they are always updated. Personal firewall will effectively block attempts to enter or leaving the host using ports that not allowed by it.

Attack to Internal Server through Perimeter

Looking at the network designed by Kevin, several servers are used for public access, accessible from Internet and providing several different services. These servers are protected by the firewall, which are Web server, SMTP Gateway and DNS server. The web server which is using Internet Information Server (IIS) 5.0, running on Windows 2000 Server Service Pack 3 will be the chosen target. The version of Internet Information Server stated in Kevin's practical is 5.5, but since there are no information available on that version, even from Microsoft website, assumption is made that the version is actually 5.0, based on the underlying Operating System used.

[15] Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide, page 98

There are few reasons of choosing this server as the target:

- Quite a number of vulnerabilities have been found for IIS, which will make easier in choosing the type of attack and available exploits. This will also increase the chance of success in attacking it.
- The firewall is using HTTP proxy to protect the web server, enabling traffic inspection up to the application level and increasing the level of security. However, looking at the firewall policy, the proxy is not specifically configured to provide additional protection that it capable to do, such as URL filtering or document content restriction. Default configuration is used for the proxy. This will allow certain types of application level attack on the HTTP protocol to pass through it.

Research from Security Focus website on vulnerability, www.securityfocus.com/bid, several vulnerabilities found on Microsoft IIS 5.0. Among those, the attack of choice will be on **Microsoft IIS Malformed HTTP HOST Header Field Denial Of Service Vulnerability** (http://www.securityfocus.com/bid/5907) which is assigned Bugtraq ID (BID) 5907.
Other references for this vulnerability will be from SecuriTeam.com, **Malformed HOST Header Causes IIS DoS**, (http://www.securiteam.com/windowsntfocus/6C00C1F5QA.html).
This vulnerability is chosen because it was released quite recently and further research shows no known patch has been released for this.

Web Server Attack Plan

From Security Focus[16], explanation of the vulnerability is as follows:

> Microsoft IIS is reported to be prone to a remotely exploitable denial of service.
>
> This condition occurs upon receipt of a malformed HOST field in a HTTP request for 'shtml.dll'. It is possible to reproduce this condition by sending a HTTP POST request with a HOST header field that is composed of an excessive number of slashes (/).

The attack is based on crafted HTTP packet sent to the web server. Different from HTTP attack to the firewall previously, which purposely asks the proxy to handle the request, this attack would be HTTP request to the web server. The attack is expected to be valid request from the HTTP proxy point of view, so that it will just pass the request to the web server without performing checking to it.

[16] http://www.securityfocus.com/bid/5907

HTTP request sent to the web server will be the same as explained in the SecuriTeam.com link above[17]:

```
POST /_vti_bin/shtml.dll HTTP/1.0
Host: [32762 '/' characters]
```

The number of '/' in the host field are 32762 characters, which not explicitly shown here for simplicity.

To inject the request to the web server, **netcat**, a famous tool by Hobbit, which can be found at @stake, Inc. website (http://www.atstake.com/research/tools/nc110.tgz), will be used. The HTTP request content will be written in a text file, which then used as input for netcat.

To check whether the attack successful, web browser can be used to connect to the web server right after the launch of the attack. If the web server is not responding then the attack is successful. Another way to check is by observing the output of netcat, which will be the response from the web server or the proxy. However, according to the report, this attack is only temporary disable the service, which then it can recover after several seconds. Repetition of the attack can increase the interruption frequency.

The attack should be carried out from a remotely compromised host in the Internet, so that if the attack is detected, the compromised host address is the one found of launching it.
Prior to launch the attack, netcat and the text file used as input file will be transported to the compromised host.

Web Server Attack Execution

The attack target is the web server at 63.100.47.37. The input file for netcat, named as *host.txt*, is contained with the HTTP commands.

Executing the command to launch the attack, is done as follows:

```
nc 63.100.47.37 80 < host.txt
```

The above command options are explained in the table below:

Option	Description
`Nc`	Netcat executable
`63.100.47.37`	Target IP address (the web server)
`80`	TCP port 80 (HTTP), used for the connection
`< host.txt`	Use host.txt to input the command for the connection

[17] http://www.securiteam.com/windowsntfocus/6C00C1F5QA.html

After the execution, netcat shows the following response:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Sat, 15 Mar 2003 04:42:06 GMT
Content-Type: text/html; charset=windows-1252

<HTML><H2>FrontPage Error.</H2>

<P>
<B>User:</B> please report details to this site's webmaster.
<P>

<P>
<B>Webmaster:</B> please see the server's application event log for
more details.
</P>
```

Checking with web browser shows delay on responding to the request. Repeating the attack several time lengthen the delay of the response.

At the firewall, checking on the logs will show record on the connection, as follows:

```
Mar 15 12:37:12.998 THESERVER httpd[788]: 121 Statistics: duration=8.26
id=4kwK sent=32804 rcvd=323 srcif=EEF4C223-0BC6-4 src=100.100.1.5/32785
cldst=63.100.47.37/80 svsrc=192.168.1.1/1143 dstif=0254FF85-A0D9-4
dst=192.168.1.7/80 op=POST arg=http:///_vti_bin/shtml.dll result="200
OK" proto=http rule=2
```

The firewall is not detecting this connection as any malicious connection, since only statistic of connection is shown, no other alerts on the logs.

On the web server, upon receiving the malicious attack, the CPU usage hits 100% utilization for a few seconds. Repeating the attack will cause it to reach 100% utilization again. By the time this happened, the web server is not responding to other requests, which is why the browser experience delay. Figure 28 shows this statistics.

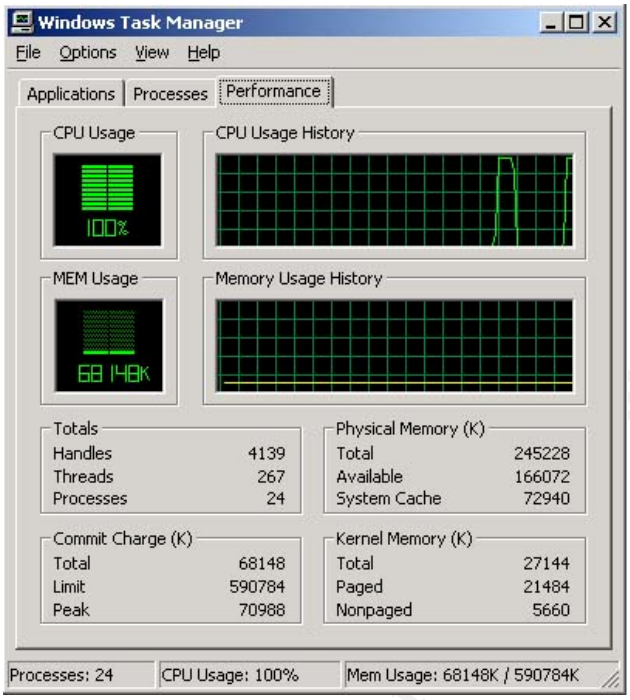

Figure 28: CPU Utilization During The Attack

Overall, the attack has been successfully cause denial of service on the web server.

Web Server Attack Countermeasures

At this point no patch is available from Microsoft that able to fix this problem. Workaround solutions should be used to mitigate the attack.

The IDS should be able to detect the attacks, but it won't be able to react against it. Firewall will log the malicious requests, but it will log it as if they were normal traffic (information event type), which require further analysis of the logs. Without additional protection system, absolute blocking to the IP addresses sending such requests is the solution. But this won't be much effective since these IP addresses, will probably only compromised hosts being used by the attacker.

The other way to prevent this attack to crash the web server, which will be a more effective solution, is to have a web server protection system that able to defend against typical attacks to web servers, especially IIS. Such systems would use web attacks signatures and when there are matching traffic to the signatures, they will drop those connections. Entercept Web Server Edition from Entercept Security Technologies (http://www.entercept.com/products/wse/) and SecureIIS from eEye Digital Security (http://www.eeye.com/html/Products/SecureIIS/index.html) are two examples of systems giving such protection.

References

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

The SANS Institute. Firewalls 101: Perimeter Protection with Firewalls, Track 2.2. Bethesda: SANS Press, 2002.

The SANS Institute. Firewalls 102: Perimeter Protection and Defense In-Depth, Track 2.3. Bethesda: SANS Press, 2002.

The SANS Institute. VPNs and Remote Access, Track 2.4. Bethesda: SANS Press, 2002.

Skoudis, Ed. Counter Hack, A Step-by-Step Guide to Computer Attacks and Effective Defenses. Upper Saddle River: Prentice Hall PTR, 2002.

Zwicky, D. Elizabeth. Cooper, Simon. Chapman, Brent D. Building Internet Firewalls, Second Edition. Sebastopol: O'Reilly & Associates, Inc., 2000.

Microsot Corporation. "Exchange 2000 Windows 2000 Connectivity Through Firewalls". 3 October 2002. URL: http://support.microsoft.com/default.aspx?scid=KB;en-us;q280132 (November 2002).

Microsoft Corporation. "Exchange 2000 Static Port Mappings". 22 January 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;270836 (November 2002).

Microsoft Corporation. "How to Configure a Global Catalog Server to Use a Specific Port When Servicing MAPI Clients". 22 January 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;298369 (November 2002).

Microsoft Corporation. "How to Configure a Firewall for Domains and Trusts" 10 October 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q179442&gssnb=1 (November 2002).

US Department of Energy, Computer Incident Advisory Capability. "DDoS Mediation Action List". 3 April 2000. URL: http://www.ciac.org/ciac/bulletins/k-032.shtml (December 2002).

Cisco Systems, Inc. "Improving Security On Cisco Routers". 29 December 2002. URL: http://www.cisco.com/warp/public/707/21.html (December 2002).

National Security Agency. "Cisco Router Security Recommendation Guide". 24 October 2001. URL: http://www.nsa.gov/snac/cisco/ (December 2002).

Cisco Systems, Inc. “Cisco IOS Release 12.2 Configuration Guides and Command References”. 2002. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm (December 2002).

CyberGuard Corporation. CyberGuard Firewall Manual, Administering the CyberGuard Firewall. CyberGuard Corporation. December 2001.

CyberGuard Corporation. CyberGuard Firewall Manual, Configuring the CyberGuard Firewall. CyberGuard Corporation. December 2001.

CyberGuard Corporation. CyberGuard Firewall Manual, Configuring SmartProxies for the CyberGuard Firewall. CyberGuard Corporation. December 2001.

Spitzner, Lance. “Auditing Your Firewall Setup”. 12 December 2000. URL: http://www.spitzner.net/audit.html (January 2003).

Fyodor. “Nmap network security scanner man page”. 2003. URL: http://www.insecure.org/nmap/data/nmap_manpage.html (January 2003).

Fyodor. “The Art of Port Scanning”. 6 September 1997. URL: http://www.insecure.org/nmap/nmap_doc.html (January 2003).

Van Jacobson. Leres, Craig. McCanne, Steven. “Windump Manual”. 14 March 2002. URL: http://windump.polito.it/docs/manual.htm (February 2003).

Vigilante.com, Inc. “SecureScan™ Vulnerability Test Performed by VIGILANTe.com Support for Sample Report”. 4 October 2001. http://www.vigilante.com/securescan/perimeter/sample_report/scex_classic.zip (February 2003).
Vigilante.com, Inc. Getting Started with VIGILANTe SecureScan NX. Beaverton: Vigilante.com, Inc, May 2002.

Fielding, R. et al. “Hypertext Transfer Protocol -- HTTP/1.1”. June 1999. URL: http://www.w3.org/Protocols/rfc2616/rfc2616.html (February 2003).

Postel, B. Jonathan. “SIMPLE MAIL TRANSFER PROTOCOL”, August 1982. URL: http://www.freesoft.org/CIE/RFC/821/index.htm (February 2003).

Bong, Kevin. “GIAC Certified Firewall Analyst (GCFW) Practical Assignment Version 1.8”. 8 December 2002. URL: http://www.giac.org/practical/GCFW/Kevin_Bong_GCFW.pdf (February 2003).

Advance IT Security. “Symantec Firewall Secure Webserver Timeout DoS”. 14 October 2002. URL: http://www.ai-sec.dk/modules.php?op=modload&name=News&file=article&sid=29&mode=thread&order=0&thold=0 (February 2003).

Security Focus. “Symantec Enterprise Firewall RealAudio Proxy Buffer Overflow Vulnerability”. 13 December 2002. URL: http://www.securityfocus.com/bid/6389 (February 2003).

Security Focus. “Multiple Symantec HTTP Proxy Denial of Service Vulnerability” 14 October 2002. URL: http://www.securityfocus.com/bid/5958 (February 2003)

Symantec Corporation. “Symantec Firewall Secure Webserver timeout DoS”. 13 October 2002. URL: http://securityresponse.symantec.com/avcenter/security/Content/2002.10.11.html (February 2003).

Condor. “HTTP Request Packet Injection”. 16 January 2002. URL: http://www.securiteam.com/tools/5NP0E1P60W.html (February 2003).

Symantec Corporation. “Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide”. 2001. URL: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/manuals/7.0/sef_sevpn_70_config.pdf (February 2003).

Mixter. “Tribe FloodNet 2k edition, Distributed Denial Of Service Network”. URL: http://mixter.void.ru/tfn2k.tgz (February 2003).

Barlow, Jason. “Axent releases a full TFN2K Analysis”. 8 March 2000. URL: http://www.securiteam.com/securitynews/5YP0G000FS.html (February 2003).

Security Focus. “Microsoft IIS Malformed HTTP HOST Header Field Denial Of Service Vulnerability”. 7 October 2002. URL: http://www.securityfocus.com/bid/5907 (March 2003).

Testa, Joe. Aitel, Dave. “Malformed HOST Header Causes IIS DoS”. 15 October 2002. URL: http://www.securiteam.com/windowsntfocus/6C00C1F5QA.html (March 2003).

Hobbit. “Netcat 1.10 for Unix”. 20 March 1996. URL: http://www.atstake.com/research/tools/nc110.tgz (March 2003).

Appendix A: Router Configuration

```
version 12.2
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname Router
!
aaa new-model
!
!
aaa authentication login default local enable
aaa session-id common
enable secret 5 $1$Y50C$hL511CVH8jt9tPJtHk70W/
!
username admin1 password 7 023A02305E741D1B
username admin2 password 7 BA50773493C21216
memory-size iomem 25
ip subnet-zero
no ip source-route
!
no ip bootp server
!
!
!
interface FastEthernet0
 ip address 100.1.1.17 255.255.255.240
 ip access-group 100 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 speed auto
!
interface Serial0
 ip address 100.1.1.34 255.255.255.252
 ip access-group 101 in
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no fair-queue
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.33
no ip http server
!
!
logging 100.1.1.21
access-list 100 deny ip any 0.0.0.0 0.255.255.255 log
access-list 100 deny ip any 10.0.0.0 0.255.255.255 log
access-list 100 deny ip any 127.0.0.0 0.255.255.255 log
access-list 100 deny ip any 169.254.0.0 0.0.255.255 log
access-list 100 deny ip any 172.16.0.0 0.15.255.255 log
access-list 100 deny ip any 192.0.2.0 0.0.0.255 log
access-list 100 deny ip any 192.168.0.0 0.0.0.255 log
access-list 100 deny ip any 224.0.0.0 15.255.255.255 log
access-list 100 deny ip any 240.0.0.0 7.255.255.255 log
```

```
access-list 100 deny ip any 248.0.0.0 7.255.255.255 log
access-list 100 deny ip any 255.255.255.255 0.0.0.0 log
access-list 100 permit tcp host 100.1.1.18 any eq 20
access-list 100 permit tcp host 100.1.1.18 any eq 21
access-list 100 permit tcp host 100.1.1.18 any eq 53
access-list 100 permit udp host 100.1.1.18 any eq 53
access-list 100 permit tcp host 100.1.1.18 any eq 80
access-list 100 permit tcp host 100.1.1.18 any eq 443
access-list 100 permit udp host 100.1.1.18 any eq 500
access-list 100 permit 50 host 100.1.1.18 any
access-list 100 permit tcp host 100.1.1.19 any eq 25
access-list 100 permit tcp host 100.1.1.19 any gt 1023
access-list 100 permit tcp host 100.1.1.20 any gt 1023
access-list 100 permit tcp 100.1.1.21 100.1.1.17 eq 23
access-list 100 deny any any log
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log
access-list 101 deny ip 192.168.0.0 0.0.0.255 any log
access-list 101 deny ip 224.0.0.0 15.255.255.255 any log
access-list 101 deny ip 240.0.0.0 7.255.255.255 any log
access-list 101 deny ip 248.0.0.0 7.255.255.255 any log
access-list 101 deny ip 255.255.255.255 0.0.0.0 any log
access-list 101 deny ip 100.1.1.16 0.0.0.15 any log
access-list 101 permit tcp any host 100.1.1.18 gt 1023
access-list 101 permit tcp any host 100.1.1.18 eq 53
access-list 101 permit udp any host 100.1.1.18 eq 53
access-list 101 permit udp host 100.1.1.18 any eq 500
access-list 101 permit 50 host 100.1.1.18
access-list 101 permit tcp host 100.1.1.19 any gt 1023
access-list 101 permit tcp host 100.1.1.19 any eq 25
access-list 101 permit tcp host 100.1.1.20 any eq 80
access-list 101 permit tcp host 100.1.1.20 any eq 443
access-list 101 deny any any log
no cdp run
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

Appendix B: Firewall Packet-Filtering Rules

Type	Service	Source	Destination	Option
# Packet Filter rules section				
# Internal users to access giac-db				
permit	1433/tcp	giac-users	giac-db	
# Internal users to access giac-mail				
permit	135/tcp	giac-users	giac-mail	
permit	1026/tcp	giac-users	giac-mail	
permit	1027/tcp	giac-users	giac-mail	
permit	1028/tcp	giac-users	giac-mail	
# giac-mail to access domain controllers				
permit	53/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	53/tcp	giac-mail	giac-dc	
permit	88/tcp	giac-mail	giac-dc	
permit	88/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	123/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	135/tcp	giac-mail	giac-dc	
permit	389/tcp	giac-mail	giac-dc	
permit	389/udp	giac-mail	giac-dc	ENABLE_REPLY
permit	445/tcp	giac-mail	giac-dc	
permit	3268/tcp	giac-mail	giac-dc	
permit	1025/tcp	giac-mail	giac-dc	
# giac-web to access giac-db				
permit	1433/tcp	giac-web	giac-db	
# router to send syslog to giac-log				
permit	514/udp	giac-router	giac-log	
# giac-log to perform remote access to router				
permit	23/tcp	giac-log	giac-router	
# VPN rules section				
# VPN users to connect to giac-db				
permit	1433/tcp	giac-vpnhosts	giac-db	
# VPN users to connect to giac-mail				
permit	135/tcp	giac-vpnhosts	giac-mail	
permit	1026/tcp	giac-vpnhosts	giac-mail	
permit	1027/tcp	giac-vpnhosts	giac-mail	
permit	1028/tcp	giac-vpnhosts	giac-mail	
# VPN users to connect to domain controllers				
permit	1029/tcp	giac-vpnhosts	giac-dc	
permit	53/tcp	giac-vpnhosts	giac-dc	
permit	53/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	88/tcp	giac-vpnhosts	giac-dc	
permit	88/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	123/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	135/tcp	giac-vpnhosts	giac-dc	
permit	389/tcp	giac-vpnhosts	giac-dc	
permit	389/udp	giac-vpnhosts	giac-dc	ENABLE_REPLY
permit	445/tcp	giac-vpnhosts	giac-dc	
permit	3268/tcp	giac-vpnhosts	giac-dc	
# Split DNS rules				
permit	domain/tcp	ALL_EXTERNAL	EXTERNAL_INTERFACES	

permit	domain/tcp	EXTERNAL_INTERFACES	ALL_EXTERNAL	
permit	domain/udp	ALL_EXTERNAL	EXTERNAL_INTERFACES	ENABLE_REPLY
permit	domain/udp	EXTERNAL_INTERFACES	ALL_EXTERNAL	ENABLE_REPLY
permit	domain/tcp	ALL_INTERNAL	INTERNAL_INTERFACES	
permit	domain/tcp	INTERNAL_INTERFACES	ALL_INTERNAL	
permit	domain/udp	ALL_INTERNAL	INTERNAL_INTERFACES	ENABLE_REPLY
permit	domain/udp	INTERNAL_INTERFACES	ALL_INTERNAL	ENABLE_REPLY
deny	domain/tcp	EVERYONE	EVERYONE	
deny	domain/udp	EVERYONE	EVERYONE	
# CVP rule				
permit	18181/tcp	FIREWALL	giac-avs	
# Firewall logging to Syslog				
permit	syslog/udp	FIREWALL	giac-log	
# Proxy rules				
# SSL Proxy rules				
proxy	https/tcp	ALL_EXTERNAL	giac-web	
proxy	https/tcp	giac-users	giac-web	
proxy	https/tcp	giac-users	ALL_EXTERNAL	
# SMTP Proxy rules				
proxy	smtp/tcp	ALL_EXTERNAL	giac-mail	
proxy	smtp/tcp	giac-mail	ALL_EXTERNAL	
# FTP Proxy rules				
proxy	ftp/tcp	giac-users	ALL_EXTERNAL	
# HTTP Proxy rules				
proxy	http/tcp	ALL_EXTERNAL	giac-web	
proxy	http/tcp	giac-users	giac-web	
proxy	http/tcp	giac-users	ALL_EXTERNAL	
proxy	http/tcp	giac-avs	ALL_EXTERNAL	
# Last deny rule				
deny	ALL	EVERYONE	EVERYONE	ENABLE_REPLY