Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.5e

GIAC Enterprises

by Marco Smitshoek
August 2001

Table of contents

1. Assignment 1 – Security Architecture

1.1 Introduction

This chapter describes the design of the infrastructure for GIAC Enterprises.

GIAC Enterprises is a growing Internet Startup that expects to earn $200 million per year in online sales of fortune cookie sayings. The company has just completed a merger/acquisition.

Access will be defined for:

- customers (the companies that purchase bulk online fortunes);
- suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- partners (the international partners that translate and resell fortunes);
- remote access for GIAC Enterprises employees.

1.2 Assumptions and starting points

1.2.1 Infrastructure

GIAC Enterprises has separated the Office LAN from the Portal site.

GIAC Enterprises has separated the Office LAN from the Administration LAN

Administration of the Portal site is done from within the Administration LAN, with dedicated administration workstations

GIAC Enterprises also needs WEB-access from the Office LAN. The mailserver resides in the Office LAN.

All systems should have multiple network interface cards to be able to separate production from administration network traffic.

For further information see the explanatory chapter for the network design.

The Portal LAN is designed according a three layer model:

- WEB zone
- Application zone
- Database zone

In the WEB zone the WEB servers are placed. These servers are the ones interacting with the Portal users. Portal users may only connect to the WEB zone.

In the Application zone the application servers are placed. Dynamic WEB content is provided by these application servers on request of the WEB servers.
Only the WEB servers may connect to the Application zone.

In the Database zone the database servers are placed. Only the application servers may connect to this zone to retrieve necessary data. In the database the most valuable information is stored.

These layers are also implemented in the Administration LAN.

For cost reduction and ease of administration all firewalls are CheckPoint FW-1's. From a security perspective it would be better to use different brands of firewalls and even different kind of firewall technologies (application level proxy firewalls/statefull packet filtering fw's). CheckPoint FW-1 is a statefull packet filtering firewall. To compensate for the disadvantages of statefull packet filtering, a Proxy Server has been implemented for WEB and Mail access.
Also the use of the different branches, i.e. Office Branch and Portal Branch compensates for the disadvantages of using all the same firewalls.

All systems log to the central Loghost in the Administration LAN. Either by using syslog and/or by securely copying (with SSH) logfiles daily.

1.2.2 Authentication

Because GIAC Enterprises is a startup, and has only a few customers, it is not yet affordable to implement authentication by SecureID cards or something alike. Authentication is done by userid/password. The password is generated according GIAC Enterprises' password policy and reset according the policy.

1.2.3 Access

Everyone may connect to the public parts of the WEB server.

Customers may connect to the WEB server and the customers pages.

Suppliers may conect to the public parts of the WEB server and the staging WEB server.

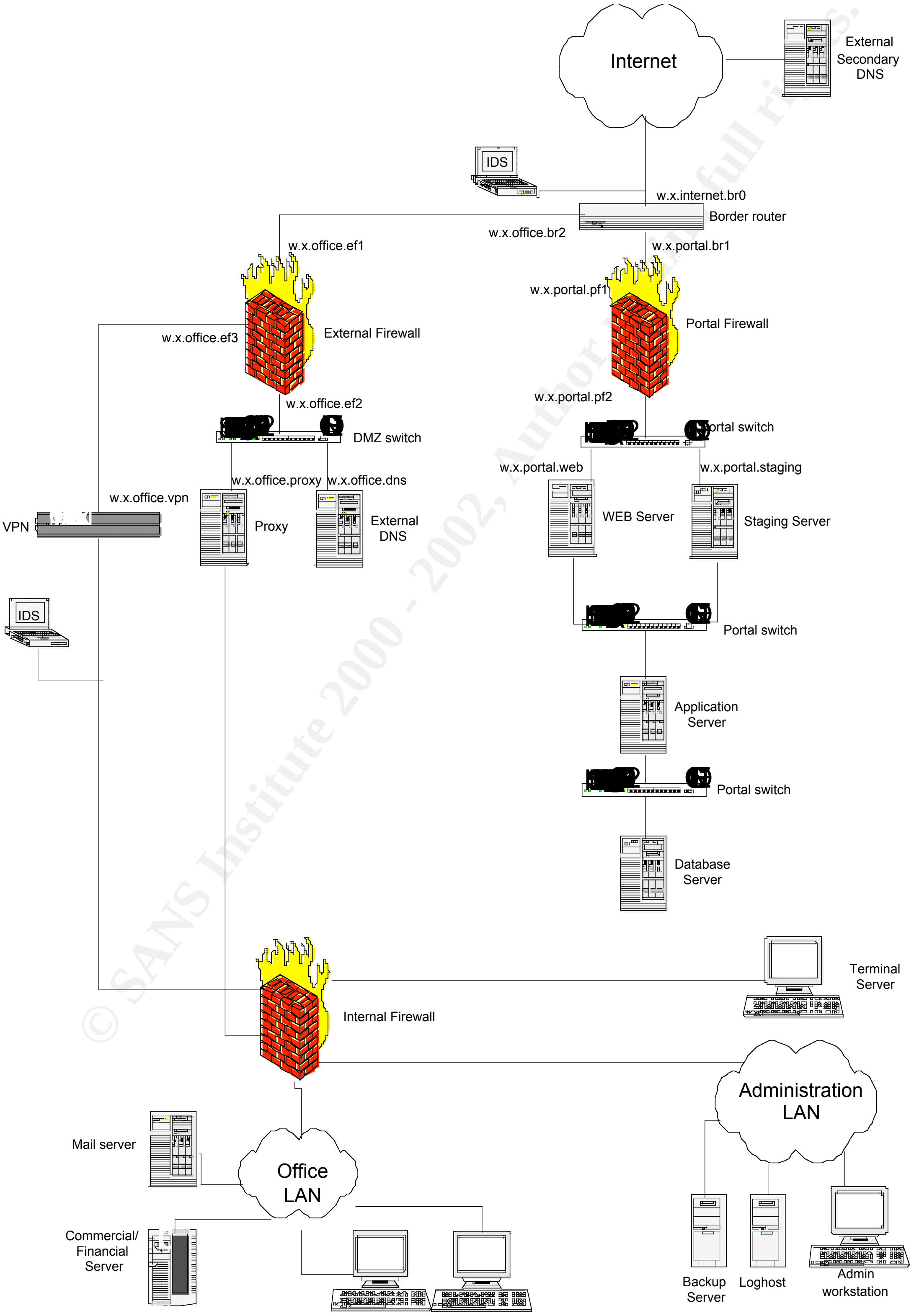
Partners may connect to the public parts of the WEB server and to particular systems in the Office LAN through a VPN connection.

Remote employees may connect to the public parts of the WEB server and to the Office LAN through a VPN connection.

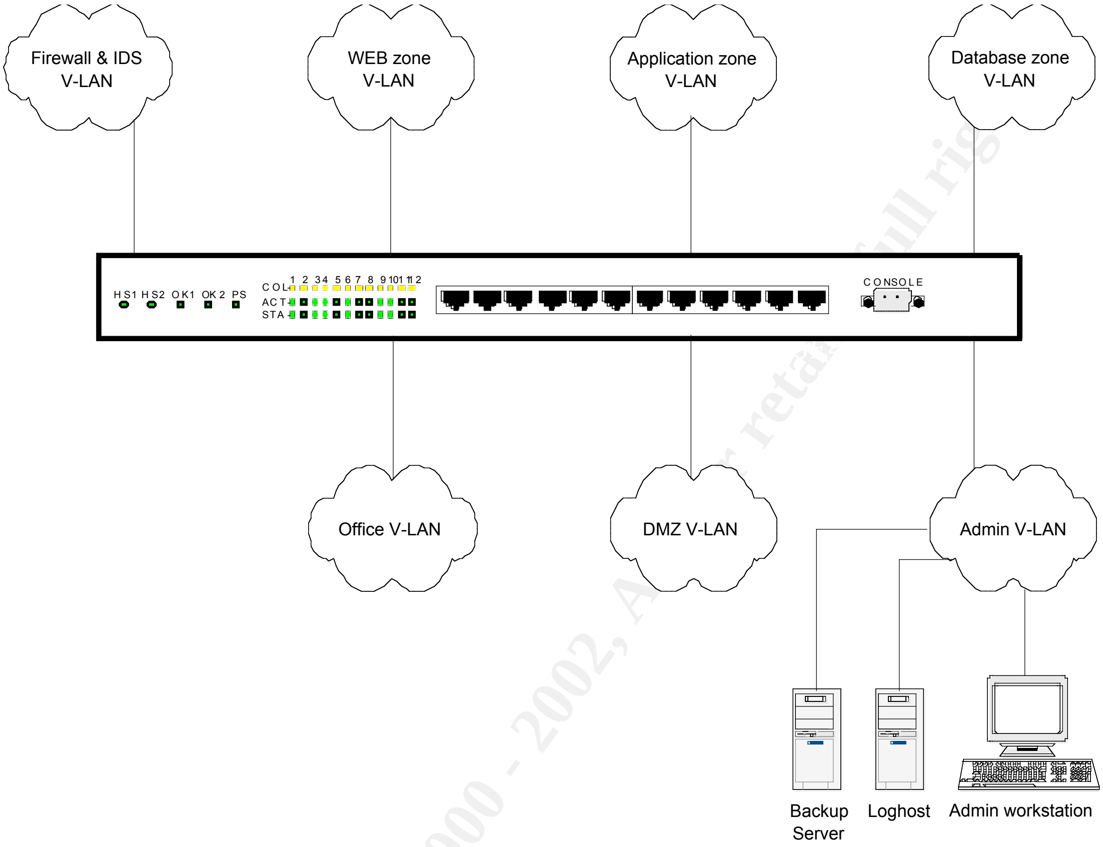
Remote GIAC Enterprises administrators may connect to the public parts of the WEB server and to the Administration LAN through a VPN connection.

1.3 Network diagrams

The following diagram shows the solution chosen for the infrastructure of GIAC Enterprises.



The following diagram shows the V-LAN design for the Administration LAN.



1.4 Explanation of the Network Diagrams

This chapter provides a detailed description of the network design, as shown in 1.3.

The design consists of two branches: one for the Portal and one for the Office connection. Both have their own firewall.

From cost perpective no internal DNS has been set up yet. Because the number of systems is small it is sufficient at this moment to use host files to resolve hostnames to IP-numbers.

For the Office Lan there is a DNS, but this system will not be discussed within this document.

1.4.1 Border router

The function of the border router is provide correct ingress and egress filtering, according to the GIAC Enterprises' security policy. Besides that it is an effective noise filter.

The router has two Ethernet Interfaces, one for the Office Branch and one for the Portal Branch.

The console port is connected to the Administration LAN. The router writes it's logging to the syslogd on the External DNS.

1.4.2 Portal Firewall

The Portal Firewall separates the Internet and the Portal LAN.

The Portal Firewall has three network interfaces:
- for the connection to the Border Router
- for the Portal LAN
- for the Administration LAN

According to the three layer model only connections to and from the WEB zone are allowed by the Portal Firewall to go from the Internet to the Portal LAN. The management interface is only used for management purposes.

The Portal Firewall:
- has OpenSSH2 installed for administration purposes;
- is set up according vendor instructions and has the latest patches installed;
- is backupped through the Administration LAN according policy.

1.4.3 Portal Switch

To minimize costs during the startup phase the three layer model is implemented by using one L3 switch and V-LAN filtering. There is a potential risc of an attacker being able to break out of a V-LAN, but till this day this is only possible with a direct connection to the switch. Users do not have a direct connection to the switch, which minimizes this risc.

In the future if business is going well and budgets expand, this one switch can be completed with two others. This way the layers will be implemented with three separate devices which increases the security level.

The switch is connected to the Administration LAN through the console port.

1.4.4 Portal Servers

WEB zone

There are two WEB servers, one production to which the customers can connect and one staging for the suppliers of the fortune cookies.

Both servers have a SSL certificate to enable encrypted sessions for users to log on and to provide or buy fortune cookie sayings.

On the WEB servers data is static content and most data will be dynamically provided by the application server.

The WEB servers have three NIC's:
- one for the connection to the Portal Firewall (with public address);
- one for the connection to the Application server (with private address);
- one for the connection to the Administration LAN (with private address).

Application zone

On the application server the portal application is running, which provides the functionality needed for the GIAC Enterprises' business. The application retrieves the necessary data from the database server in the Database zone. The application also updates the database with new data. The application communicates with SQL to the database server.

The application server also has three NIC's (all private addresses):
- one for the connection to the WEB zone;
- one for the connection to the Database zone;
- one for the connection to the Administration LAN.

Database zone

The database server is running an Oracle database which will be connected to with SQL by the application as mentioned above.

The database server has two NIC's (all private addresses):
- one for the connection to the Application zone;
- one for the connection to the Administration LAN.

ALL servers:
- have OpenSSH2 installed for administration purposes;
- are set up with a hardened OS and have the latest patches installed;
- are backupped through the Administration LAN according policy.

1.4.5 Portal switch

The Portal switch is a L3 switch implementing the three layer model by using V-LAN's and V-LAN filtering. This switch also prevents potential sniffing activities in case an attacker places a sniffer tool on one of the Portal systems.

1.4.6 External Firewall

The External Firewall separates the Internet from the VPN and the DMZ in which the Proxy and the External DNS server are placed.

Main purpose for this firewall is to provide Internet access for the Office Environment and for the VPN connectivity. Also connections to the External DNS are under control of this firewall.

The firewall has four NIC's:

- one for the connection to the Border Router;
- one for the connection to the DMZ;
- one for the connection to the VPN device;
- one for the connection to the Administration LAN.

The External Firewall:

- has OpenSSH2 installed for administration purposes;
- is set up according vendor instructions and has the latest patches installed;
- is backupped through the Administration LAN according policy.

1.4.7 VPN device

The VPN device provides VPN access throught the Internet.

The VPN Device will be used by partners and remote employees.

The VPN device is connected to the Administration LAN with the console port.

1.4.8 Proxy Server

The only way PC's from the Office LAN can access the Internet is through this proxy. Only HTTP/HTTPS is allowed by GIAC Enterprises' policy.
The Proxy Server also serves as a mail proxy which receives mail from the Internet and delivers it to the internal Mail Server and vice versa.

The Proxy Server has three NIC's:

- one for the connection to the External Firewall;
- one for the connection to the Internal Firewall;
- one for the connection to the Administration LAN.

The Proxy Server:

- has OpenSSH2 installed for administration purposes;
- is set up with a hardened OS and has the latest patches installed;
- is backupped through the Administration LAN according policy.

1.4.9 External DNS

The External DNS is authoritative for the GIAC Enterprises' domain. All the public hostnames and IP-adresses of GIAC Enterprises are served by this DNS. A secondary DNS server is hosted at the ISP.

The External DNS is also used by the Proxy Server to resolve hostnames.

The External DNS also serves as a syslog server for the Border Router.

The External DNS has two NIC's:
- one for the connection to the External Firewall;
- one for the connection to the Administration LAN.

The External DNS:
- has OpenSSH2 installed for administration purposes;
- is set up with a hardened OS and has the latest patches installed;
- is backupped through the Administration LAN according policy.

1.4.10 DMZ switch

The DMZ switch prevents potential sniffing activities if an attacker succeeds in placing a sniffer in the DMZ. It also provides the possibility of increasing the number of systems in the DMZ.

1.4.11 Internal Firewall

The Internal Firewall separates the Administration LAN from the Office LAN, the VPN device, the Proxy Server and the Terminal Server.

The firewall has five NIC's:
- one for the connection to the Proxy Server;
- one for the connection to the VPN device;
- one for the connection to the Terminal Server;
- one for the connection to the Administration LAN;
- one for the connection to the Office LAN.

The Internal Firewall:
- has OpenSSH2 installed for administration purposes;
- is set up according vendor instructions and has the latest patches installed;
- is backupped through the Administration LAN according policy.

1.4.12 Administration LAN

The Administration LAN consists of several V-LAN's which are separated by V-LAN filtering rules on the switch. All systems are connected to the switch with their Management Interface.

In the Admin V-LAN the workstations of the administrators are placed. These are dedicated workstations with no Office Applications installed.

Also the central Loghost and the central Backup Server are located in this Admin V-LAN.

To prevent bypassing of the three layer model via the Administration LAN, the several zones are located in different V-LAN's:
- the WEB zone V-LAN, with the WEB and Staging Server;
- the Application zone V-LAN, with the Application Server;
- the Database zone V-LAN, with the Database Server.

All the Firewalls and IDS systems, including their management workstations are located in the Firewall & IDS V-LAN.

In the Office V-Lan the Mail Server and the Commercial/Financial Server are located.

In the DMZ V-LAN the Proxy Server and External DNS are located.

1.4.13 Terminal Server

The Terminal Server is used for administration of the several network components, which are connected to the Terminal Server with their console ports.

Also all the console ports of the other systems are connected to the Terminal Server to be able to connect to the consoles if necessary. (for instance to boot a system)

Because console access should be protected carefully, the Terminal Server is connected to the Internal Firewall on a dedicated interface, so access can be restricted and closely monitored.

1.4.14 Mail Server

The Mail Server is located in the Office LAN because it provides mail functionality to the GIAC Enterprises employees.

It provides SMTP/POP3 access for the users and communicates only SMTP with the mail proxy on the Proxy Server. So no direct connections are made to or from the Mail Server and other mail servers on the Internet.

The Mail Server has two NIC's:
- one for the connection to the Office LAN;
- one for the connection to the Administration LAN.

The Mail Server:
- has OpenSSH2 installed for administration purposes;
- is set up with a hardened OS and has the latest patches installed;
- is backupped through the Administration LAN according policy.

1.4.15 Commercial/Financial Server

This server contains the financial en commercial application of GIAC Enterprises and is the heart of the organization.

The application is managed and used via WEB-interfaces using HTTPS.

GIAC Enterprises employees as well as partners make use of this application.

The Commercial/Financial Server:
- has OpenSSH2 installed for system administration purposes;
- is set up with a hardened OS and has the latest patches installed;
- is backupped through the Administration LAN according policy.

1.4.16 Intrusion Detection (IDS)

Intrusion Detection Systems (IDS) are used to monitor all network traffic at the access points of GIAC Enterprises' infrastructure:
- the Internet uplink
- the VPN connection. Traffic after the VPN device is not encrypted anymore, so this can be monitored by an IDS.

Because GIAC Enterprises is still a small company, with few employees, no IDS is installed in the Office LAN. If GIAC Enterprises will grow and the number of employees increases, it may be a good thing to install an IDS in the Office LAN too, because statistics show that most damage is done from within the organization.

1.5 Hard- and software details

GIAC Enterprises is a UNIX environment. All systems are SUN Solaris, version 8.x.

Component	Brand and version
Border Router	Cisco 3640, IOS 11.x
Portal, External, Internal Firewall	CheckPoint Firewall 1, version 4.x
IDS	CheckPoint RealSecure, version 5.x
Switches	Cisco Catalyst 4000
Proxy	Squid, version 2.4
VPN device	Cisco 3030

2. Assignment 2 – Security Policy

In this chapter the security policies will be decribed and explained of:

- Border Router
- Portal Firewall
- VPN Device

Technical measures on systems are based on a written security policy, which describes what is allowed and what not and why. This security policy has to be signed off by upper management of GIAC Enterprises.

It is beyond the scope of this assignment to provide a complete security policy for GIAC Enterprises. The implemented policies described in this chapter are to be considered technical translations of the written GIAC Enterprises' security policy.

2.1 Border Router

2.1.1 General

Since the Border Router is not the main line of defense, the security policy is not too tight. Everything is allowed, except what is explicitly denied. Everything definitively NOT wanted is blocked.

GIAC Enterprises wants to be a good Internet neighbour, so correct egress filters will be applied.

To drop the obvious noise from the Internet as soon as possible, ingress filtering rules will be applied on the incoming interface from the Internet.

According the security policy the following banner needs to be shown at logon:
Warning: unauthorized access strictly prohibited. Any use of this system may be logged or monitored without further notice.

Access lists are processed top -> down. At the first encountered match the specified action (permit/deny) is applied to the packet. Then the next packet is checked, starting at the top of the accesslist again. If no match is found in the access list, a default deny will be applied.

For performance it's best to put ACL rules which are likely to be hit most at the top. This saves CPU cycles.

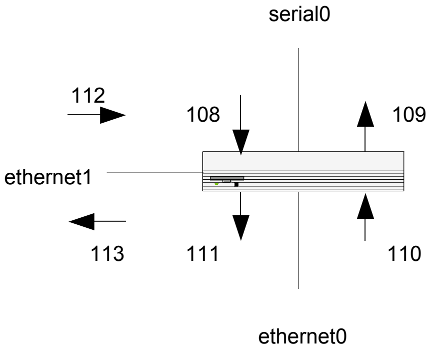
It is important to find a balance in what to log and what not. Too much logging costs resources and important entries may disappear between all the others.
Too little logging can make troubleshooting and incident handling a difficult task.
It's a continuous practice to optimize logging for a specific site.

Filtering can be done either on the router's input or ouput interface. To be as efficient as possible with the CPU cycles filters will be applied to the input interfaces so packets don’t have to go through the packet forwarding process only to get filtered out…

2.1.2 Configuration

Interface Serial 0 is the connection to the Internet.
Interface Ethernet 0 is the connection to the Portal Branche.
Interface Ethernet 1 is the connection to the Office Branche.

See figure:



Defining the IP Addresses to the interfaces and definition and assignment of the access-groups:

```
        interface Serial 0
                ip address w.x.internet.br0
                ip access-group 108 in
                ip access-group 109 out

        interface Ethernet 0
        ip address w.x.portal.br1
                ip access-group 110 in
                ip access-group 111 out

        interface Ethernet 1
        ip address w.x.office.br2
                ip access-group 112 in
                ip access-group 113 out
```

Allow only console logins to the router:

```
                line console 0
                login
                password <password>
```

Disabling unnecessary services which reduce security. Enable password disguising:

```
service password encryption
enable secret <password>
no service tcp-small-servers
no service udp-small-servers
no service finger
no service cdp
no ip bootp server
no ip http server
```

Limiting ICMP. Prevent layer 3 -> 2 mapping and smurf amplification:

```
no ip direct-broadcast
```

Stop ICMP unreachables; prevent network mapping:

```
no ip unreachables
```

Set the banner:

```
banner /
***Warning: unauthorized access strictly prohibited. Any use of this system
may be logged or monitored without further notice.***
/
```

Disable SNMP:

```
no snmp
```

Loose Source Route:

```
no ip source-route
```

Keep MAC addresses secret:

```
no ip proxy arp
```

Log information to the External DNS as previously mentioned:

```
logging w.x.office.dns
```

Ingress ACL on Interface Serial 0.
Deny non routable source IP spoofed packets:

```
access-list 108 deny ip 0.0.0.0 0.255.255.255 any log
access-list 108 deny ip 10.0.0.0 0.255.255.255 any log
access-list 108 deny ip 172.16.0.0 0.15.255.255 any log
access-list 108 deny ip 192.168.0.0 0.0.255.255 any log
access-list 108 deny ip 224.0.0.0 15.255.255.255 any log
access-list 108 deny ip 240.0.0.0 7.255.255.255 any log
access-list 108 deny ip 248.0.0.0 7.255.255.255 any log
access-list 108 deny ip 255.255.255.255 0.0.0.0 any log
```

Block tftp at the router:

```
access-list 108 deny udp any any eq 69 log
```

Block ICMP queries that may be used to enumerate the environment:

```
access-list 108 deny icmp any any 13
access-list 108 deny icmp any any 17
```

Block internal address space

```
access-list 108 deny ip 127.0.0.0 0.255.255.255 log
access-list 108 deny ip w.x.portal.0 0.255.255.255 log
access-list 108 deny ip w.x.office.0 0.255.255.255 log
```

Finally the last rule allows everything else:

```
access-list 108 permit any
```

Testing of these rules can be done by using a tool (like nmap) and spoofing the addresses with the correct ports for which the rules apply and send the packet to the router. Check the logging to see if the proper action is taken by the router.
This can be done by using a system and a dialup account with an ISP, because the test machine should be connected to the Internet and not reside in the GIAC Enterprises network.

Now the egress ACL's will be applied to the correct interfaces. To save CPU cycles the egress ACL's will be applied to the ethernet interfaces of the router, instead of the serial interface.

The purpose of the egress ACL is to prevent spoofed packets of leaving GIAC Enterprises' network. This prevents the network of being used as a DDoS source.

The following rules will be applied:

```
access-list 110 permit ip w.x.portal.0 0.255.255.255 any
access-list 110 deny ip any any

access-list 112 permit ip w.x.office.0 0.255.255.255 any
access-list 112 deny ip any any
```

Because filtering is done at the other interfaces the following access lists can be very simple:

```
access-list 109 permit ip any any
access-list 111 permit ip any any
access-list 113 permit ip any any
```

Testing of these rules can be done by placing a test system on the GIAC Enterprises networks connected to each interface and send packets with other source ip addresses than the ones allowed. Check the logging for the deny entries. Also send packets from the allowed hosts and check if these packets are permitted.

2.2 Portal Firewall

2.2.1 General

All firewalls in the GIAC Enterprises' infrastructure are CheckPoint FW-1's.

From a security point of view this is not the best choice. It would be more safe to use different brands and technologies.

The infrastructure has been divided in two branches, the Portal and the Office branch, both with their own firewall. For the Internet connectivity from within the Office LAN a proxy is used to improve security. These additional points compensate for using all the same firewalls.

By default FW-1 has the following ports opened:
ICMP, DNS (TCP/UDP), RIP and the FW-1 management ports (256, 257, 258)
This can be changed by editing the default properties.

FW-1 uses only the IP addresses and ports to maintain state of the sessions.

To prevent errors in the rulebase, the rulebase will have to be kept simple: no more than 30 rules. Specific rules will be placed before general rules, because otherwise the general rules migth overrule the specific ones. For performance reasons the commonly rules will be used first.

All logging will be done in the LONG format to log as much information as possible. No name resolution will be used for the logs to increase throughput. Logfiles will be rotated daily.

According policy the default rule for the firewalls is "drop all/log". All firewalls should have a firewall lock down rule, only allowing specific administration access and dropping all other connections.

2.2.2 Configuration

The Portal Firewall is protecting the services of GIAC Enterprises.

The firewall has to permit only the following services:
- http/https traffic to the WEB server for anyone
- http/https traffic to the Staging server for suppliers
- admin access from the administration LAN

The default settings will be changed by selecting Policy -> Properties and unchecking the following items:
- Accept Outgoing Packets
- Accept RIP
- Accept Domain Name Queries (UDP)
- Accept Domain Name Queries (TCP)
- Accept Domain Name Download

The following objects by example are defined:
Networks: Administration, Supplier
Services: http, https, syslog
Routers: FW1
Hosts: WEB server, Staging server, Loghost

The rulebase for the firewall will be as follows:

#	Source	Destination	Service	Action	Track
1	Any	WEB server	http	Accept	Long
2	Any	WEB server	https	Accept	Long
3	Supplier	Staging server	http	Accept	Long
4	Supplier	Staging server	https	Accept	Long
5	Administration	FW1	Any	Accept	Long
6	FW1	Loghost	syslog	Accept	Long
7	Any	Any	Any	Drop	Long

Explanation of the rulebase:

#	Explanation of the rule
1	First the rule which will be used most, the access rule for anyone to connect to the WEBserver on http.
2	This rule allows anyone access to the more protected part of the WEB site on https.
3	Only suppliers are allowed access to the Staging server on http. The network object "Supplier" contains all the IP addresses of the suppliers.
4	Only suppliers are allowed access to the Staging server on https. The network object "Supplier" contains all the IP addresses of the suppliers.
5	This rule allows only access to the firewall from within the Administration LAN
6	This rule allows the firewall to log on the internal Loghost on syslog
7	This rule drops all other, non authorized, traffic

The rules can be tested with a tool like nmap from within the different connected networks.

Http/https connections to the WEB server from any address should be accepted and logged. Any other connection should be dropped, i.e. no answer back to the sender and a log entry in the firewall log stating the drop action.

Only connections from an originating IP address of a supplier will be accepted for the Staging server on http/https. All other connections and from other IP addresses will be dropped and logged.

Only connections from within the Administration LAN to the firewall will be accepted. All other connections will be dropped and logged.

Only the firewall may connect to the Loghost on syslog. All other connections from the firewall or to the Loghost will be dropped by the firewall. (connections from other hosts to the Loghost will go through the Administration Lan and not through this firewall. So this rule is not disabling other hosts to connect to the Loghost through the Administration LAN!)

2.3 VPN Device

2.3.1 General

The VPN Device will be configured through the console. (by using the Terminal server from within the Administration LAN)

It will be configured and managed by using the command line interface (CLI)

The device has the following interfaces:

- Ethernet 1 (Private) is the interface to your private network (internal LAN).
- Ethernet 2 (Public) is the interface to the public network.
- Ethernet 3 (External) is the interface to an additional LAN.

Since it has an internal interface with an internal IP address it will log to the Loghost directly through the Internal Firewall.

The VPN device will provide access through the Internet.

According security policy only IPSec connections are supported. The policy also prescribes at least the support of ESP, because AH does not function well wit NAT and this could cause some compatibility problems with partners. (AH is also allowed)

Cisco client software will be used to connect to the VPN Device.

The VPN Device will use an internal database for authenticating users. This is no problem, because the number of partners is small. Each user will have an specific IP address assigned. This makes tracing activities from logging easier.

2.3.2 Configuration

The first steps of configuring the VPN Device are setting the passwords for it, setting time & date, configuring the interfaces, etc. . These will not be described. Only the relevant configuration items for this assignment will be described using Quick Configuration.

PPTP an L2TP will be disabled and IPSec enabled.

At the CLI the following info will be shown:

```
-- : Configure protocols and encryption options.
-- : This table shows current protocol settings

        PPTP        |        L2TP        |
-----------------------------------------------
```

```
|      Enabled       |       Enabled       |
| No Encryption Req  | No Encryption Req  |
--------------------------------------------

1) Enable  PPTP
2) Disable PPTP

Quick -> [ 1 ]
```

Enter 2.

The next step is to disable L2TP:

```
1) Enable  L2TP
2) Disable L2TP

Quick -> [ 1 ]
_
```

Enter 2.

Next the system will prompt with the following:

```
1) Enable  IPSec
2) Disable IPSec

Quick -> [ 1 ] _
```

Enter 1.

Now PPTP and L2TP are disabled and IPSec is enabled.

Configure address assignment.

The VPN device will be configured to use only Per User address assignment. (a server assigns IP addresses on a per-user basis)

All other methods will be disabled. Only the enabling of the Per User option will be described here:

```
1) Enable Per User Address Assignment
2) Disable Per User Address Assignment

Quick -> [ 2 ] _
```

Enter 1.

Configuring authentication.

The systems prompts for the following:

```
-- : Specify how to authenticate users.
```

```
1) Internal Authentication Server
2) RADIUS Authentication Server
3) NT Domain Authentication Server
4) SDI Authentication Server
5) Continue

Quick -> _
```

Enter 1.

Configure users and assign specific IP addresses to them.

The systems prompts with the usermanagement menu:

```
Current Users
------------------------------------------------------------------------
                              No Users
------------------------------------------------------------------------
1) Add a User
2) Delete a User
3) Continue

Quick -> _
```

Enter 1 and provide the username and password after the prompts that follow.
The following limitiations apply:
Username:	max. 32 characters and case-sensitive;
Password:	min. 8 characters, max. 32 characters, case-sensitive.

The password will have to be entered a second time for verification.

After this an IP address must be assigned to this user. The systems prompts for an IP address and a subent mask.

At the end you will return to the usermanagement main menu. From here the other users can be created, as many as needed.

Configuration of the IPSec Group.

The remote-access IPSec client connects to the VPN Device via this group name and password, which are automatically configured on the internal authentication server. This is the IPSec group that creates the tunnel. Users then log in, and are authenticated, by means of their usernames and passwords.

The system prompts with the following:

```
> IPSec Group Name

Quick -> _
```

Enter the IPSec group name. Maximum is 32 characters, case-sensitive.

The system prompts to enter the group password.

> IPSec Group Password

Quick -> _

Enter a unique password for this group. The minimum is 4, and the maximum is 32 characters, case-sensitive. For verification the system prompts again for the password.

Reset the admin password according policy.

The system prompts for the password:

> Reset Admin Password

*Quick -> [*****] _*

Enter the new password and reenter it for verification.

The last step is to save the configuration.

1) Goto Main Configuration Menu
2) Save changes to Config file
3) Exit

Quick -> 2

Additional configuration items.

LogToSyslog = On
SyslogIPAddress = <Loghost address>

This enables logging to the internal Loghost. And save the configuration again…

Testing of the VPN Device.

Testing of the VPN Device can be done by installing the Cisco Client Software. Information from the Cisco WEBsite:

"Cisco VPN Client

Simple to deploy and operate, the Cisco VPN Client is used to establish secure, end-to-end encrypted tunnels to compliant Cisco Remote Access VPN devices. This thin design, IPSec-compliant implementation is available via CCO download for use with any compliant Cisco Remote Access VPN product and is included free of charge with the Cisco VPN 3000 Concentrator. The client can be pre-configured for mass deployments and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management. The Cisco VPN client provides support for Windows 95, 98, ME, NT 4.0, and 2000."

Once installed and configured, the VPN Device can be tested by connecting through the Internet and check:

- if the expected functionality/connectivity to the GIAC Enterprises' internal network is available
- check the logging of the VPN Device to see if connecting/authentication/IP address assignment is done correctly.
- check by analysing the IDS logging if the traffic from the Internet to the VPN Device is indeed encrypted.

3. Assignment 3 - Audit Your Security Architecture

3.1 Assessment planning

The basis of the audit is the GIAC Enterprises' Security Policy. The goal is to determine if the firewall implements this policy correctly. These audits should be performed twice a year. The recommendations of these audits are binding, i.e. if any flaws are discovered, they should be fixed. All information regarding to this audit is confidential and should be used accordingly.

Important is to have a written authorization of upper management to perform the audit.

The audit should take place at a time that it has least impact on the business. This means that the audit should take place at off-hours or in a weekend. Statistics of system usage can help determine the best time to perform the audit. One should keep in mind the worst case possibility that the audit can (partly) disturb services. It's important to have good backups and proper restore procedures at hand.

This assessment is an audit, no hacker penetration test! As mentioned before, the goal is to determine if the firewall is compliant to the security policy. This means that the tools used may not be destructive, or should not be used in such manner.

It is recommended to perform this audit with at least two people, one system administrator who is very familiar with the system(s) and one auditor. All superuser and/or administration passwords should be reset after the audit.

The following tasks can be defined, with an estimation of the time needed:

#	Task	Time (hrs)
1	Get written authorization of upper management	1
2	Get a copy of the written GIAC Enterprises Security Policy and read it carefully. Make a checklist for the audit from this policy.	4
3	Get a copy of the written Operational Handbooks of the Firewall and review this document. (check if it's up-to-date, in line with the policy etc.)	4
4	Verify backup by restoring the latest backup on a test machine	2
5	Do the "external" tests with nmap and Nessus from all sides of the firewall. (external, internal, administration LAN)	4
6	Do the "internal" system checks. Check: - config files - filesystem setup and security (access rights) - rulebase - accounts - password strength (with the tool Crack) - patchlevel of the system and the software - check if logging is correctly written to the Loghost	5
7	Analyse the results and write a report with recommendations if necessary.	8

Total time needed is 28 hrs for the auditor and 11 hrs for the system administrator (for the actual tests): total 39 hrs. At a rate of $2000/day this means the total costs for this audit is: $9750. (This is exclusive the possible overtime rates)

3.2 Implement the assessment

Tasks 1, 2, 3 and 4 are considered to be clear and do not need further explanation.

Task 5:
nmap is run against the firewall from all three connected networks: external (Internet), internal (WEB zone) and the administration LAN.

The firewall logs as much as possible. Logging will be analysed after each test to verify the correct functioning of the firewall.

Commands used with nmap:
- full UDP port scan: nmap –sU –p 1-65535 –P0 <IP address>
- full TCP SYN port scan: nmap –sS –p 1-65535 –P0 <IP address>
- ICMP ping: nmap –sP –P0 <IP address>

Now the Nessus scans are run. Latest stable version of Nessus is 1.0.9. Nessus can be obtained from http://www.nessus.org.
Nessus has a graphical user interface from which it is run. It consists of a server part and a client part, which can be run on separate systems.

At this point a copy of all the firewall logging of today is made for further analysis.

Task 6:
In this step the audit is performed on the system itself instead of scanning it from the outside. Copies of config files can be saved to be included in the final report if needed.

A lot of relevant information is provided by organizations like SANS and CERT like Step-by-step guides and checklists. This way one knows what files to check.

A copy of the password file is saved to be crunched by Crack to see it the passwords are strong enough. Crack is available from:
ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack
All passwords need to be reset after the audit.

Also the rulebase is checked for misconfigurations or possible optimizations. The order of the rules is for example a very important issue. See assignment two for the rulebase of the Portal Firewall of GIAC Enterprises.

A very important and in practice often neglected issue is to keep the system on the latest (stable) patch level. On the other hand it is important to only patch if necessary, and not to blindly apply all patches. It is important to check if all necessary patches have been tested and applied according policy.

Another important issue is to check whether the logging is also correctly written to the Loghost. Copies of this logging are saved for further analysis too.

Step 7:
Finally all test results need to be analysed and compared to each other to be matched. Recommendations can be made to improve the security of the system, both on technical and procedural level.

3.3 Conduct a perimeter analysis

The results of the audit show that the Portal Firewall is functioning as expected and is implementing the GIAC Enterprises' Security Policy correctly.

On the other hand, the overall audit results in some recommendations.

First of all, all the firewalls are of the same technology and from the same vendor. It would be better to differentiate on this: use different technologies and different vendors. This will improve security, but on the other hand this will increase the cost of administering the infrastructure. The proxy server compensates for this disadvantage, so this is not a critical recommendation, but one for the future. It is recommended to replace the External firewall of the Office Branche by an Application Level Firewall like Raptor.

Regarding the IDS infrastructure some improvements can be made too. Statistics show that 70 – 80% of misuse/hacks are the responsiblility of internal employees instead of external hackers. It is strongly recommended to implement an IDS in the Office LAN too.

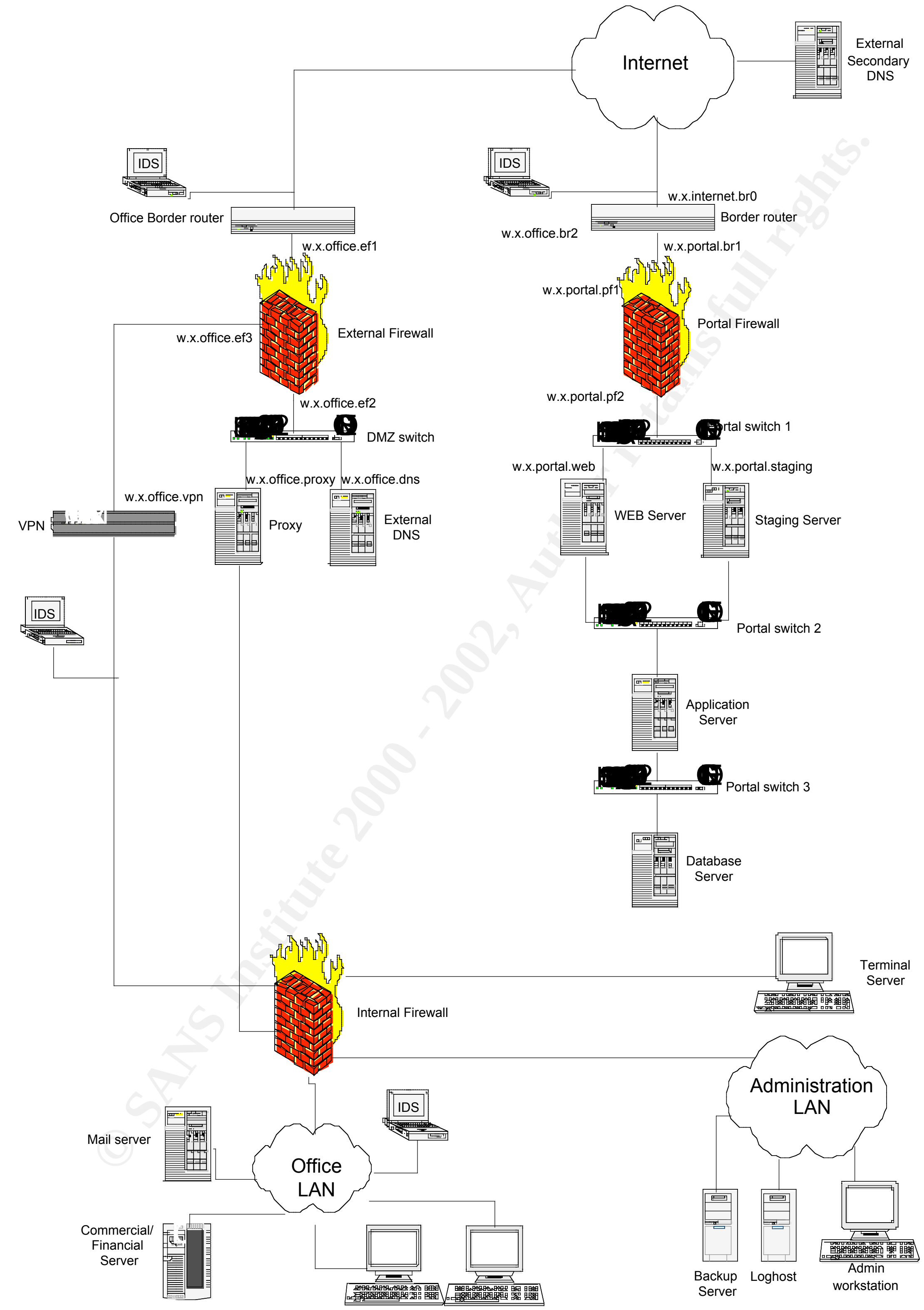
To separate traffic to the Portal and from/to the Office LAN it is recommended to implement another uplink to the Internet from another provider. This extra uplink prevents Office traffic to disturb Portal traffic and vice versa. This uplink can also be used as a backup link for the Portal in case of an emergency, or the Portal link can be used as a backup link for the Office. This also means another IDS.

A recommendation for the future is to think about implementing redundancy into the infrastructure. A second uplink for the Portal Branche with loadbalancing firewalls (StoneBeat) and loadbalancing WEB severs can increase availability of the infrastructure. This is only possible if the business is blooming and the costs can be justified.

At this moment the Portal Branche is separated into it's Zones by using a L3 switch and V-LAN filtering. This means the internal security of the Portal Branche is implemented by just one device. It is recommended to add two more devices to implement this separation. The same goes for the Administration LAN.

Implementation of these recommendations will result in the following diagram. (The recommendations for the future are not yet taken into account.)

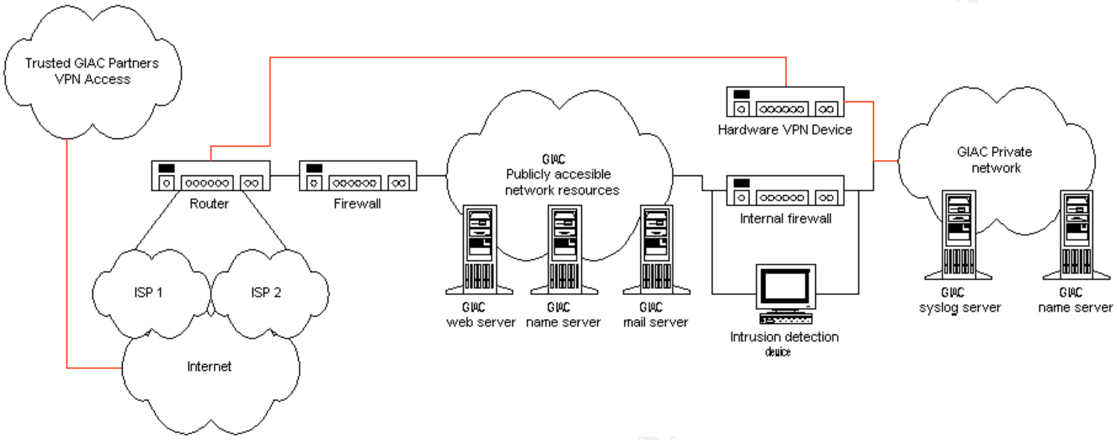
Improved network design for GIAC Enterprises.



4. Assignment 4 – Design Under Fire

For this assignment the GCFW Practical of Ken Colson has been chosen:
http://www.sans.org/y2k/practical/ken_colson_gcfw.doc

The network design is as follows:



4.1 Attack against the firewall

The firewall is a Linux machine with Ipchains as firewall software.

There are several ways to attack the firewall system:

- through the OS
- through the firewall software/rules (in this case very much integrated with the OS)
- through additional tools/software like OpenSSH.

First a nmap scan can be performed to scan the firewall for any misconfigurations. Misconfigurations can occur on OS-level or within the rulebase of the firewall software. If one is found the exploit for using this misconfiguration can be used to attack the firewall system.

If the SSH 1 protocol is used, the following deficiency might be exploited: “OpenSSH has the SSH 1 protocol deficiency that might make an insertion attack difficult but possible. The CORE-SDI deattack mechanism is used to eliminate the common case. Ways of solving this problem are being investigated, since the SSH 1 protocol is not dead yet.” See http://www.openssh.org/security.html

If the Firewall is correctly installed, it’s difficult to gain privileges on this system. On the other hand some DoS attacks can be launched against the firewall, causing all services of GIAC Enterprises to be unavailable, except for the VPNdevice.

One recent DoS attack, for which no patches are available yet, is the “Multiple Vendor Small TCP MSS Denial of Service Vulnerability”. This issue is discussed on BugTraq, identification number 2997. See http://www.securityfocus.com/.

Darren Reed provided an exploit:
http://www.securityfocus.com/data/vulnerabilities/exploits/maxseg.c

After compilation this code can be run against the firewall to use the exploit.

The idea of this attack is the following, citing a part of Darren's original posting on BugTraq:

"What's this mean? Well, if I connect to www.microsoft.com and set
my MSS to 143 (say), they need to send me 11 packets for every one
they would normally send me (with an MSS of 1436). Total output
for them is 1876 bytes - a 30% increase. However, that's not the
real problem. My experience is that hosts, especially PC's, have
a lot of trouble handling *LOTS* of interrupts. To send 2k out
via the network, it's no longer 2 packets but 20+ - a significant
increase in the workload."

Since the firewall is a low end solution, probably a PC with Linux, this firewall could be suffering easily from this attack. By sending lots of small packets the workload for the firewall gets too high and it will slow down very much, denying normal services to the customers.

4.2 DoS attack

A search on BugTraq resulted in the following possible attack:

"A potential denial of service vulnerability exists in the Linux Kernel.

The problem occurs when a large number of UDP packets are sent to a
Linux system. This can cause the system to use all available CPU
resources and thus become unresponsive.

The attack can be performed by sending UDP packets to any port on
the system, regardless of whether a service is listening on that port. The
system may have to be reset manually if the attack is successful."

The attack is described in the following BugTraq archive entry:

To: *BugTraq*
Subject: *UDP packet handling weird behaviour of various operating systems*
Date: *Tue Jul 24 2001 23:36:39*
Author: *Stefan Laudat < stefan@mail.allianztiriac.ro >*
Message-ID: *<20010724233639.A5717@allianztiriac.ro>*

The following tool can be used to perform the attack:
http://www.securityfocus.com/external/http://rootshell.com/archive-j457nxiqi3gq59dv/199803/biffit.c

When this tool is run from all 50 compromised systems to attack the WEBserver, the WEBserver will probably die…

Which steps will have to be performed?

- compile the tool for the OS of the compromised hosts
- distribute the program to the compromised hosts
- start the program and send a UDP flood to the GIAC Enterprises WEB server

Cisco IOS seems to be vulnerable too, so probabaly the border router will “hang” first. If not, the WEB server will and will probably have to be restarted manually.

How can this attack be mitigated? Since there’s no patch available yet, it is difficult to prevent this attack. One possible solution is to use a bandwith controller, like a PacketShaper to limit the bandwidth for UDP traffic, so the flood will be bound to a maximum at which the infrastructure has no problems. See http://www.packeteer.com/products/packetshaper/ for additional information.

4.3 Internal System Attack

Financial and business information systems reside in the GIAC Private Network. This is the most interesting information for a hacker. To avoid as many security devices as possible, my first target would be the VPN Device.

If I could gain control over the VPN device I would bypass both firewalls and the IDS system and connect directly to the GIAC Private Network. From here I could find out which internal system holds the information I want to have for example by sniffing network traffic. Probably the internal hosts are not too well protected (probably Micosoft OS) and the information I want can be retrieved.

First step is to find as much information on the Cisco VPN5000 device, especially the security issues.

Secondly if an exploit can be found, use it against the VPNdevice and gain control. If possible monitor the network traffic on the GIAC Private Network.

Try to gain access to the system containing the information wanted and send a copy of this info to an anonymous mailbox. (special hotmail account or something alike) Get the information from the mailbox.

5. References

- Help Defeat Denial of Service Attacks: Step-by-Step, SANS, http://www.sans.org/dosstep/index.htm

- Using the Command-Line Interface for Quick Configuration, Cisco, http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/3_1/getting/gs4cli.htm#xtocid63130

- Building Internet Firewalls, Second Edition, Zwicky, Cooper and Chapman, O'Reilly

- Readers of the SANS course "Firewalls, Perimeter Protection and VPN's" , SANS 2001

- Nessus, http://www.nessus.org

- nmap, http://www.nmap.org

- Crack, ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack

- Practical of Ken Colson, SANS GCFW, Ken Colson, http://www.sans.org/y2k/practical/ken_colson_gcfw.doc

Other references are mentioned in the text when appropriate.