Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.5e
Current as of January 28, 2001 (amended May 22, 2001

Rui Santos

Assignment 1 – Security Architecture

Introduction

The security infrastructure design included in this document, is for GIAC enterprises.

GIAC enterprises main line of business is selling fortune cookies on the Internet. They expect to earn $200 million per year in online sales.
The purpose of this document is to defines perimeter defenses and internal security to protect the access to the business provided by the company and to guaranty that in case of security problems an audit of can be done and swift recovery is possible.

The connectivity to the company is separated into:
- Internet Access: External user possibly not trusted that connects to the web server to download fortune cookie.
- Internal Access: Internal user, they required access to normal day work that might include administration of IT systems and internal administrative work, they require Mail and Internet Access.
- Remote Access from a business partner: Trusted External partner that connects to our system to download or upload fortune cookies.
- Remote Access from a Mobile user: Internal user that might require access to the system when not physically in the company.

External Business partners relationships

GIAC enterprises as three types of business partners:
- Suppliers: Partners that supply fortunes
- Partners: International partners that translate and resell fortunes.
- Clients: Internet users that acquire fortune cookies

Security for these connections is essential as they are critical for the success of the business.

Because of costs all partners connect over the Internet over a VPN connection.
The decision made is to make the VPN on the second border router, which is optimized for VPN traffic.
Suppliers of fortune cookies will connect directly to our Service network; each supplier should have its separate router with VPN.

Other External Connections

Another external connection present on the design is the possibility of connection of users to the internal network from an external location.
This is done through the use of a dial-in solution with strong authentication (Secure Tokens, Secure IDs). The use of strong authentication is required on this link as this can grant direct access to our internal networks from an external user.

Description of components

Firewalls

A Firewall is a set of programs that are located on a gateway server. The purpose of a firewall is to protect resources located on a network from users located on another network. Basically a firewall inspects each network packet against is security policy and makes a decision to forward/drop/deny this to its final destination.

Reverse Proxy Server

A reverse Proxy server is another name given to a proxy server. It will act as an intermediary point between a workstation and the real server so that a enterprise can ensure security, administrative controls and separation between networks with different levels of security when necessary.

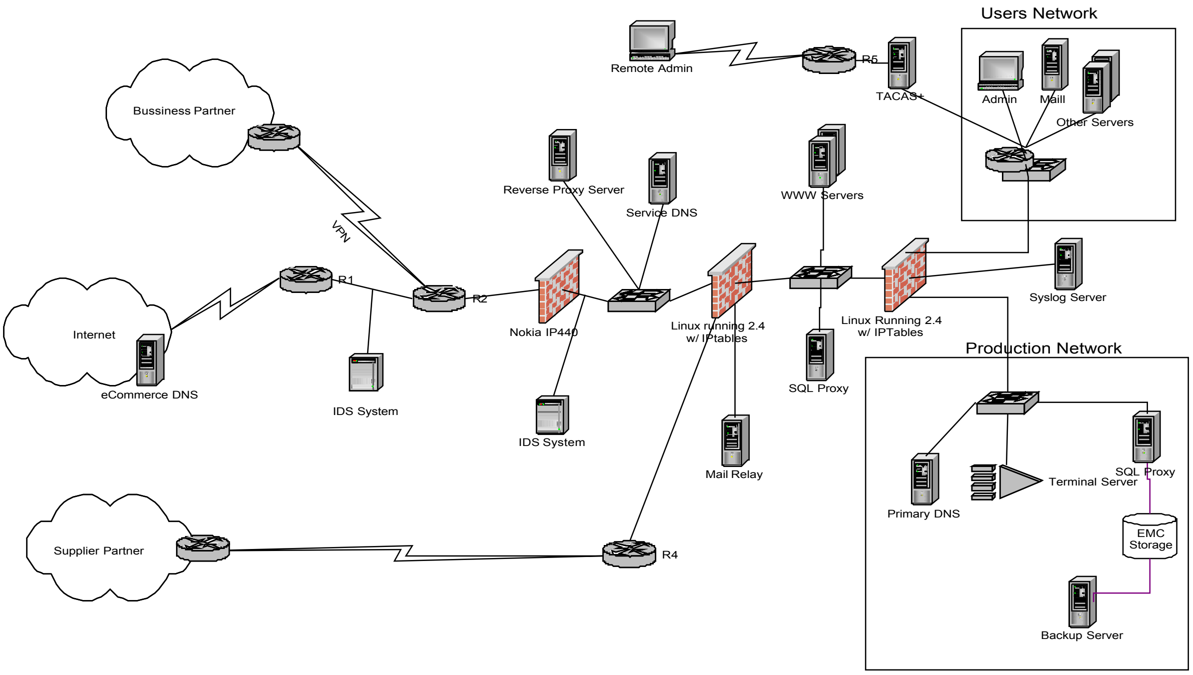
Routers

A router primal purpose is to determine the next network point to which a packet should be forwarded towards to. A router can also perform several other tasks like filtering, Network Address translation and VPN tunnels.

Terminal Server

A terminal server is a device that provides terminals with a common connection point to a local or wide area network.

Network Design



Type of Traffic

Internet Access

HTTP/HTTPS for eCommerce Site access and transactions.

Internal Access

SSH, Firewall-1 protocols for administration of servers (Firewall, Routers, Server, etc).
HTTP/HTTPS for Internet Access
NetBios for access to internal servers for day-to-day work (Mail Server, Print Server, File Server, etc).

Remote Access from business partner

Over a encrypted connection (IPSec, CET, etc)
Access to restricted number of resources related to the business relationship with the Client

Remote Access from Mobile user

HTTP/HTTPS Internet Access
NetBios for access to internal servers for day-to-day work
SSH for administration access based on the level of security of the user

Description of Security

Perimeter defense is implemented with the use of statefull firewalls, routers and proxys,
Two different types of firewall are used. The idea a second line of defense in case of an exploit appears for front end firewall; If this occurs the second firewall should prevent any further access to internal systems from an intruder.

Description	Product
Front End Firewall	Nokia IP440, Checkpoint Firewall 4.1 with SP3
Service Firewall	Linux 2.4.7 bastion host running IPTables 1.2.2 with patches
Internal Firewall	Linux 2.4.7 bastion host running IPTables 1.2.2 with patches

On the routers some filtering is performed (egress, ingress), but they are mostly responsible for VPN and NAT operations.

The proxy servers are responsible for maintaining a separation between possible armful users and the main servers. Their purpose is to protect the main servers of any vulnerability found in them.

Assignment 2 – Security Policy

For the purposes of this work we will use the following NAT translations:

Reverse Proxy	10.1.1.2	x.y.z.10
Service DNS	10.1.1.2	x.y.z.25
Internal DNS	10.1.7.2	x.y.z.26
Web Server	10.1.2.2	x.y.z.1
SQL Proxy	10.1.2.2	x.y.z.2
Normal Users	10.1.3.0	x.y.z.3/7/8/9 (NAT Static /Overload)
Administration User	10.1.4.2	x.y.z.4
Internal Syslog Server	10.1.5.2	x.y.z.6

Configuration of equipment

Border Router
VPN connections from business partners
Egress & spoofing rules to clean all the noise, coming from the Internet.
Drop and logging of connections to the network equipment
Denying and logging of Egress or spoofing attempts

Filtering router
NAT translation
Drop and logging of connections to the network equipment
Denying and logging of Egress or spoofing attempts
Allow traffic only to authorized machines.

Supplier router
NAT translation
Drop and logging of connections to the network equipment
Denying and logging of Egress or spoofing attempts
Allow traffic only to authorized machines.

Front End Firewall
Drop and logging of connections to the firewall
Restrict access to specific business services on DMZ
Denial and logging of all other traffic

Service Firewall
Drop and logging of connections to the firewall
Restrict access to specific business services on Service Network
Denial and logging of all other traffic

Internal Firewall
Drop and logging of connections to the firewall

Routers General Configuration

All routers should have a template for its configuration, as there are some security best practices that should be immediately applied to all the routers wherever they are.

Had a banner for legal reasons and to warn anyone that connects to router without permission and/or by mistake. The information included on this warning is required to be as clear as possible and should not provide any information regarding the equipment being connected.

```
banner /GO AWAY: Authorized access only/
```

Configure a syslog server

```
logging x.y.z.6
```

Stop all services that are not required, and that can either provide a source of attack or of information to potential attackers

```
no service tcp-small-servers
no service udp-small-servers
no finger
no ip http server
no ip bootp server
```

Snmp is not required, GIAC enterprises as decided not use snmp on its infrastructure

```
no snmp
```

Prevent source routing has this is only used usually for connectivity diagnostic and this can be used by an attacker to penetrate your network

```
no ip source-route
```

In order to prevent smurf, and someone of using or networks to initiate a smurf attack, prevent directed-broadcasts. This will have to be done on all network interfaces.

```
no ip direct-broadcast
```

Prevent other usually unnecessary servicies

```
no ip redirects
no ip route-cache
no ip mroute-cache
```

Prevent anyone except the administrators from connecting to the router all virtual terminals should be protected.

```
Ip access-list standard administration
    ! accept Only authorized access
    permit x.y.z.4 log
    deny any log

line vty 0 4
    access-class 11
    login
```

On the internal interface there should also be a rule to allow access from x.y.z.4 to telnet port.

For the logs to be coherent all devices should have their time synchronized.

```
ntp authenticate
ntp authentication-key 1 md5 ntpk3y
ntp trusted-key 1
ntp access-group peer 20
ntp server <ntp_server> key 1 prefer
ntp server <ntp_server_1> key 1
```

Spoofing rules

Prevent someone from spoofing your internal ip addresses by applying and anti-spoofing rules to the external interface.

```
    ip access-list standard spoof
        ! deny internal networks
        deny 10.0.0.0 0.255.255.255 log
        deny 172.16.0.0 0.15.255.255 log
        deny 192.168.0.0 0.0.255.255 log
        ! block loopback and localhost addresses
        deny 127.0.0.0 0.255.255.255 log
        deny 224.0.0.0 7.255.255.255 log
        deny x.y.z.0      0.0.0.32
        permit any
```

Egress rules

Prevent someone from the spoofing address coming from your internal network, this is usual a best practice because of Internet good manners.

```
    ip access-list standart egress
        ! allow only legitime traffic
        permit x.y.z.0 0.0.0.32
        deny any log
```

Border router (R1)

The configuration of the border router is quite simple for performance reasons, and should have little more than then the template used for all the routers.
The router is used to clear out all the “noise” coming from the Internet.

Filter router (R2)

The router will be used to make a bit more specific filtering and to do all the NAT from our internal networks and for the VPN connections of any clients connecting from the outside.

```
! static nat for the Reverse proxy
ip nat inside source static 10.1.1.2  x.y.z.10
! static nat for the Service DNS
ip nat inside source static 10.1.1.2 x.y.z.25
! static nat for the Internal DNS
ip nat inside source static 10.1.1.2 x.y.z.26
! static nat for the administration console
ip nat inside source static 10.1.4.2 x.y.z.4
! static nat for the Log server
ip nat inside source static 10.1.5.2 x.y.z.6

! overload NAT address
ip nat pool nat-pool x.y.z.3 x.y.z.9 netmask 255.255.255.224
ip nat inside source list 1 pool nat-pool overload

! VPN tunnel to an external client
crypto isakmp policy 1
        encr 3des
        hash md5
        ! use a preshared secret
        authentication pre-share
crypto isakmp key r4z0R address z.t.u.y 255.255.255.255
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac

crypto map serial00 1 ipsec-isakmp
        set peer z.t.u.y
        set transform-set rtpset
        match address 115
!
```

More specific rounting can be done as well on this device to take some load off the firewall, but without forgetting that this router is already doing VPN and NAT that are very demanding operations.

```
ip access-list extended filterin
        ! allow access to the Reverse Proxy Server
        permit tcp any x.y.z.10 0.0.0.32 eq www
        permit tcp x.y.z.10 0.0.0.32 eq 80 any gt 1023 established
        ! allow the access from the internal DNS server to make queries
```

```
          permit udp x.y.z.26 0.0.0.32 ant eq 53 reflect dnsfilter
!
evaluate dnsfilter
```

Note: I will not get into much more detail were as the firewall will do the filtering.

Supplier router (R3)

The router will be used to connect to another router over a ISDN line and a small the channel will be encrypted using IPSec. Some NAT and filtering will be done as well.

```
! static nat for the administration console
ip nat inside source static 10.1.4.2 x.y.z.4.
! static nat for the SQL proxy
ip nat inside source static 10.1.2.2 x.y.z.2
! static nat for the Log server
ip nat inside source static 10.1.5.2 x.y.z.6

crypto isakmp policy 1
          encr 3des
          hash md5
          ! use a preshared secret
          authentication pre-share
crypto isakmp key r00t address z.t.u.f 255.255.255.255
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac

crypto map serial00 1 ipsec-isakmp
          set peer z.t.u.f
          set transform-set rtpset
          match address 115
!
```

Front End firewall

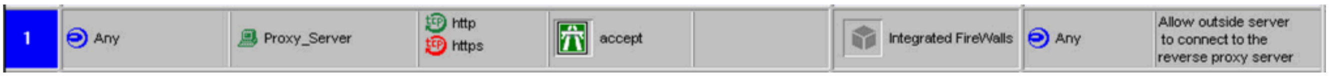
This will be the first line of defense. There should be very few rules on the firewall, for the maximum performance, and the rules that have more frequent access should be placed in the beginning of the policy so that the firewall doesn't need to go through the entire security policy from the firewall to make a decision.

We are using a Nokia IP440 Firewall with Checkpoint Firewall 4.1 SP6 for this function.

Services allowed through the firewall

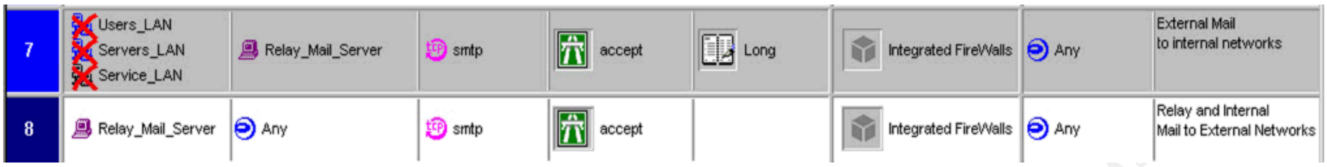
HTTP

Allow access to the reverse proxy server



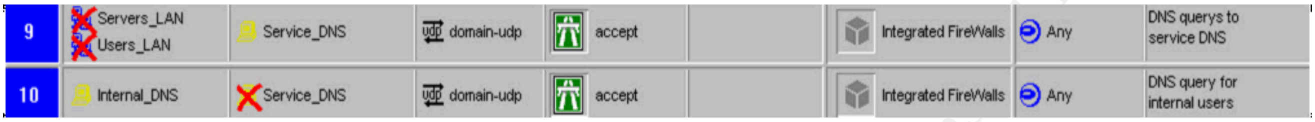
1	Any	Proxy_Server	http https	accept		Integrated FireWalls	Any	Allow outside server to connect to the reverse proxy server

SMTP
Allow mail to reach the relay and to go out



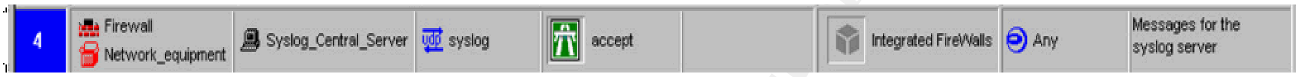
7	Users_LAN Servers_LAN Service_LAN	Relay_Mail_Server	smtp	accept	Long	Integrated FireWalls	Any	External Mail to internal networks
8	Relay_Mail_Server	Any	smtp	accept		Integrated FireWalls	Any	Relay and Internal Mail to External Networks

DNS
Allow Internet users to query our service dns server, and for primary dns server to query the Internet for internal Internet access.



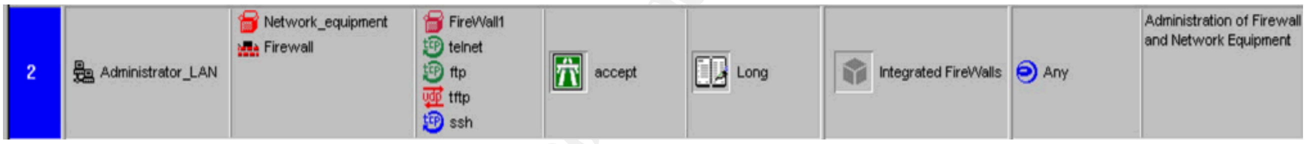
9	Servers_LAN Users_LAN	Service_DNS	domain-udp	accept		Integrated FireWalls	Any	DNS querys to service DNS
10	Internal_DNS	Service_DNS	domain-udp	accept		Integrated FireWalls	Any	DNS query for internal users

Syslog
Allow the firewall and the external network equipment to send syslog messages into the central syslog server



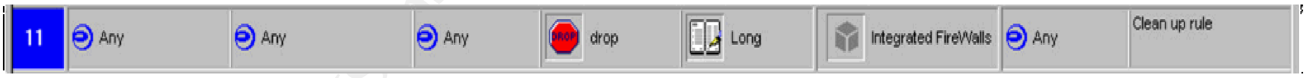
4	Firewall Network_equipment	Syslog_Central_Server	syslog	accept		Integrated FireWalls	Any	Messages for the syslog server

Administration
Allow administration of the firewall and network equipment



2	Administrator_LAN	Network_equipment Firewall	FireWall1 telnet ftp tftp ssh	accept	Long	Integrated FireWalls	Any	Administration of Firewall and Network Equipment

Clean up rule
Drop everything else, as it is either forbidden or unnecessary and log our send an alert if someone is trying to access the network equipment and the firewall



11	Any	Any	Any	drop	Long	Integrated FireWalls	Any	Clean up rule

Proxy server
This will translate any request made to it into a request to the real web server, this way we can protect the web server from direct attacks coming from the Internet.

Service Firewall
This is the second line of defense this firewall will in fact protect the servers that store all the information as the two servers in front of it will not have much information stored on them.

We are using iptables 1.2.2 on a Linux box with 2.4.7 kernel with all the latest patches the latest patches.

HTTP
Allow http and https from the proxy server to the web server

```
$IPTABLES –A FORWARD –o outside_interface –p tcp –s proxy_server –d web_server –dport 80 –j ACCEPT
$IPTABLES –A FORWARD –o outside_interface –p tcp –s proxy_server –d web_server –dport 443 –j ACCEPT
$IPTABLES –A FORWARD –i internal_interface –p tcp -s 10.1.3.0/24 –dport 80 –j ACCEPT
$IPTABLES –A FORWARD –i internal_interface –p tcp -s 10.1.3.0/24 –dport 443 –j ACCEPT
```

SMTP
Allow mail from the relay to the internal mail server

```
$IPTABLES –A FORWARD –p tcp –s smtp_relay –d internal_mail_server –dport 25 –j ACCEPT –j LOG
```

DNS
Allow the DNS server to make queries to the Internet

```
$IPTABLES –A FORWARD –i internal_interface –p udp –s primary_dns –dport named –j ACCEPT
```

Syslog
Allow the entire server to send messages to the central syslog server

```
$IPTABLES –A FORWARD –p udp –s <network_equipment> –d syslog_server –dport 524 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p udp –s frontend_firewall –d syslog_server –dport 524 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p udp –s proxy_server –d syslog_server –dport 524 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p udp –s smtp_relay –d syslog_server –dport 524 –j ACCEPT –j LOG
$IPTABLES –A OUPUT –p udp –s service_firewall –d syslog_server –dport 524 –j ACCEPT –j LOG
```

SQL
Allow the access to the SQL proxy server

```
$IPTABLES –A FORWARD –p tcp  -d sql_proxy–dport <sql_port> –j ACCEPT
$IPTABLES –A FORWARD –p tcp  -d sql_proxy–dport <sql_port> –j ACCEPT
```

Administration
Allow administrators the manage all the equipment

```
$IPTABLES –A FORWARD –i internal_interface –s administration  -d frontend_firewall -dport <firewall-1 services> –j ACCEPT –j LOG
```

```
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d frontend_firewall -
dport 22 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d <network_equiment> -
dport 22 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d smtp_relay -dport 22
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d proxy_server -dport
22
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d <network_equiment> -
dport 21 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p udp –i internal_interface –s administration –d <network_equiment> -
p 21 –j ACCEPT –j LOG
$IPTABLES –A INPUT –p tcp –s administration –dport 22 –j ACCEPT LOG
```

State full Rules

Allow all established and related traffic to go through

```
$IPTABLES –A FORWARD –m state –state ESTABLISHED,RELATED –j ACCEPT
$IPTABLES –A INPUT –m state –state ESTABLISED, RELATED –j ACCEPT
$IPTABLES –A OUTPUT –m state –state ESTABLISED, RELATED –j ACCEPT
```

Clean up rule

```
$IPTABLES –A FORWARD –j  DROP
$IPTABLES –A INPUT –j DROP
$IPTABLES –A OUTPUT –j DROP
```

Internal Firewall

This firewall will protect internal systems and will in fact enforce a separation between the Users network and the production network.

We are using iptables 1.2.2 on a Linux box with 2.4.7 kernel with all the latest patches the latest patches.

HTTP/HTTPS

Allow http and https to all the servers

```
$IPTABLES –A FORWARD –i users_interface -s 10.1.3.0/24 –dport 80 –j ACCEPT
$IPTABLES –A FORWARD –i users_interface -s 10.1.3.0/24 –dport 443 –j ACCEPT
```

SMTP

Allow mail from the relay to the internal mail server

```
$IPTABLES –A FORWARD –p tcp –s smtp_relay –d internal_mail_server –dport 25 –j ACCEPT –j
LOG
```

DNS

Allow the DNS server to make queries to the Internet

```
$IPTABLES –A FORWARD –i users_interface -s 10.1.3.0/24 –p udp –s primary_dns –dport named
–j ACCEPT
```

SQL

Allow all the servers to send messages to the central syslog server

```
$IPTABLES –A FORWARD –p tcp  -s sql_proxy -d sql_server –dport <sql_port> –j ACCEPT
$IPTABLES –A FORWARD –p tcp  -s 10.1.3.0/24 -d sql_server –dport <sql_port> –j ACCEPT
```

Syslog

Allow all the servers to send messages to the central syslog server

```
$IPTABLES –A FORWARD –p udp –s <network_equipment> –d syslog_server –dport 524 –j
ACCEPT –j LOG
$IPTABLES –A FORWARD –p udp –s frontend_firewall –d syslog_server –dport 524 –j ACCEPT
–j LOG
$IPTABLES –A FORWARD –p udp –s proxy_server –d syslog_server –dport 524 –j ACCEPT –j
LOG
$IPTABLES –A FORWARD –p udp –s smtp_relay –d syslog_server –dport 524 –j ACCEPT –j
LOG
$IPTABLES –A FORWARD –p udp –s service_firewall –d syslog_server –dport 524 –j ACCEPT –j
LOG
$IPTABLES –A OUTPUT –p udp –s backend_firewall –d syslog_server –dport 524 –j ACCEPT –j
LOG
$IPTABLES –A FORWARD –p udp –s web_server –d syslog_server –dport 524 –j ACCEPT –j
LOG
$IPTABLES –A FORWARD –p udp –s sql_proxy –d syslog_server –dport 524 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p udp –s tacas_server –d syslog_server –dport 524 –j ACCEPT –j
LOG
$IPTABLES –A FORWARD –p udp –s sql_server –d syslog_server –dport 524 –j ACCEPT –j LOG
```

Administration

Allow administrators the manage all the equipment

```
$IPTABLES –A FORWARD –p tcp –I internal_interface –s <administration_lan> -d
<terminal_server> -p 1494 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –i internal_interface –s administration  -d frontend_firewall -dport
<firewall-1 services> –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d frontend_firewall -
dport 22 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d <network_equiment> -
dport 22 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s <terminal_server> –d smtp_relay -dport
22 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s <terminal_server> –d proxy_server  –j
ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s <terminal_server> –d web_server  –j
```

```
ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s <terminal_server> –d sql_proxy  –j
ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s <terminal_server> –d service_dns  –j
ACCEPT –j LOG
$IPTABLES –A FORWARD –p tcp –i internal_interface –s administration –d <network_equiment> -
dport 21 –j ACCEPT –j LOG
$IPTABLES –A FORWARD –p udp –i internal_interface –s administration –d <network_equiment> -
p 21 –j ACCEPT –j LOG
$IPTABLES –A INPUT –p tcp –s administration –dport 22 –j ACCEPT –j LOG
```

State full Rules
Allow all established and related traffic to go through

```
$IPTABLES –A FORWARD –m state –state ESTABLISHED,RELATED –j ACCEPT
$IPTABLES –A INPUT –m state –state ESTABLISED, RELATED –j ACCEPT
$IPTABLES –A OUTPUT –m state –state ESTABLISED, RELATED –j ACCEPT
```

Clean up rule

```
$IPTABLES –A FORWARD –j  DROP
$IPTABLES –A INPUT –j DROP
$IPTABLES –A OUTPUT –j DROP
```

SQL proxy

This will prevent any direct access to the Database and will protect the database servers.

Design Notes

No connections are granted to the syslog server, any administration or work on this server should be done on the console. Specific events are automatically written to a printer so that they cannot be destroyed if the server is compromised.

Testing the firewalls and routers

Testing all the rules is essential and for this we have built a table with tests that need to be performed, the results of the tests are referenced on the table.

Scan For open ports	Everywhere	Network devices	No opens Doors	Firewall Logs are created
Scan For open ports	Everywhere	Firewalls	No open Doors	Firewall Logs are created
Scan For open ports	Internet/ Business Partners	Service DNS	53/udp	Logs are created for other ports
Scan for open ports	Internet/ Business Partners	Proxy	80/TCP 443/TCP	Logs are created for other ports

Scan for open ports	Internet/ Business Partners	Mail relay	25/TCP	Firewall Logs are created
Scan for open ports	Internet/ Business Partners	SQL Proxy Web Server Mail Server Primary DNS	No open doors	Firewall Logs are created
Scan for open ports	Suppliers	SQL Proxy	SQL Port/TCP	Logs are created for other ports
Scan for open ports	Suppliers	Web Server	80/TCP 443/TCP	Logs are created for other ports
Scan for open ports	Suppliers	Mail Server DNS Server Proxy Server Database Server	No open doors	Firewall Logs are created
Ping	Everywhere	All		Logs are created

Assignment 3 – Audit your security architecture

Approach

The approach to the audit should follow the following approach:

1. Try to getter as much information as possible about the network design of the infrastructure.
2. Assess the business requirements and the business risks
3. Find a Period of low firewall use, for any penetration testing, as this is a critical assessment that might involve down time.

Cost

The cost of auditing a firewall are not only of personnel level, the risks of downtime have to be considered as well as there is a big risk of down time on the assessment.

Personnel costs are as follow

- Review Security Policy – **1 man/day**
- Execute Security policy tests – **1 man/day**
- Look for vulnerabilities on equipment found – **1 man/day**
- Generate a report – **1 man/day**
- Act to correct any problems found – **1 man/day**

Implementation

The first thing to achieve is to gather as much information about what to scan. A good starting point is the DNS server. Try to perform a DNS zone transfer, if the DNS server and the network equipment are not properly configured you can get a lot of information by performing this task.

If you are unable to do a DNS zone transfer to get information about the GIAC infrastructure, you should query other DNS servers. They will give information about the DNS server responsible by GIAC domain and this is a critical point on any infrastructure.

In the event that this should fail the next thing you should try is to scan the address space assign to the GIAC. For this operation you can use nmap (http://www.insecure.org/) or hping (http://www.hping.org/). These tools will give you a lot of information from where to work.
With these tools in can do not only normal ICMP ping, but you can also do TCP ping enabling you to find any machine on the GIAC subnet.

A small script can be built to scan for the normal services normally provided: http, https, dns, smtp.
The syntax for the TCP ping using the nmap tool is: nmap –0 –PT<port> <host>

The –0 option on the Nmap tool will also try to identify the type of operating system running on the other side giving you this way even more information for other phases of the audit.

The second thing to do is to use the information gathered on the first step and look for open doors on each server found, these way you will in fact test each firewall rule, to do this the list of tests included on **Assignment 2 – Security Policy, Testing the firewalls and routers** should be used to test this.

Scan all ports	nmap –sS –p1-65535 –P0 <host> nmap –sU –p1-65535 –P0 <host>
Scan specific tcp port	nmap –sS –p<port> -P0 <host>
Scan specific udp port	nmap –sU –p<port> -P0 <host>

Finally with the information gathered on the previous tests, exploits scanning tools can be used to gathered information about possible vulnerabilities or missing patches on the services found during the previous test.

There are several good tools to perform this task, preference goes to Nessus (http://www.nessus.org), reasons for this:

- It's a free (as free beer).
- Security tests more or less up-to-date
- Possibility of building your own tests.

Other tools available for this purpose are:
Sara (http://www.www-arc.com/sara)
ISS Internet Scanner (http://www.iss.net)
Cisco Secure Scanner (http://www.cisco.com)

Improvements

One of the improvements that can be done to the design is, to include a Proxy server for Internet access from internal users, this will take some pressure off the routers, by the removal of NAT overload, and it will include a point where all internet downloads can be scanned for viruses and Trojans.

As web servers exploits can be run on HTTPS there is always a risk that someone will attack our web server and go unnoticed, this way if we un encrypting all the traffic this would enable us to have an early warning system, to do this we would use the reverse proxy server to translate all HTTPS traffic to HTTP by installing the certificate on the reverse proxy server. This would make the presence of an IDS system between the two systems an option to monitor all the traffic.

Assignment 4 – Design under fire

The design I have select is the one from Jeff Stelzner.
http://www.sans.org/y2k/practical/Jeff_stelzner_GCFW.doc

On its paper he states that is core firewall is a Cisco PIX 10000 firewall running 5.3-1.

The attack used on this firewall is describe on the BugTraq mailing list, and can be found on the following URL:

http://cert.uni-stuttgart.de/archive/bugtraq/2001/03/msg00146.html

This URL contains a description of some tests made to this Cisco PIX firewall; one of its tests is a DoS attack. For the attack to be successful the following information is required:

1. The IP address of a service on the other side of the firewall.
2. A syn-flood tool for the attack

This attack will not grant us access to any resources of GIAC but will exploit the firewall to perform a DoS. This attack will enable us to stop the firewall from working properly, this way in fact stopping GIAC as its entire network is depending on its core firewall.

The first thing to do in this attack is to find a service that we can attack this can be done easily if the enterprise as a Web server as is the case for GIAC enterprises.

Using a syn-flood tool freely available on the Internet (synk4[1]) an attack is performed on the Web Server that will.

To start the attack we run the command:

```
./synk4 10.10.10.10 200.200.201.18 80 80
```

If everything goes well the web server should stop responding to requests in a few seconds, notice the fact that a spoof ip address was used for obvious reasons.

This will prevent any other connections to the web server. Making this a very effective way of disturbing the company main business function.

As describe in the URL this will leave a number of ports opened that will not be closed by the firewall as no RST of FYN reply is sent. So the firewall will not open any other connection until, either the default timeout for a connection as been reached or a cleanup of the PIC connection table as been made.

Dos Attack using 50 DSL/Cable Modem

The attack describe previously can be used for the DoS attack required by this test. But if the attack was unknow or not documented this might not even be necessary. If someone had control of 50

---

[1] This tool can be download from several sites I have found it in http://www.netflood.net/download.php?op=getit&lid=5

DSL/cable modem a DoS attack would be quite difficult to prevent and little could be done.

If we consider that a DSL/Cable modem as a possible bandwidth of 128kps upload, and if we multiply this by 50, we would have a possible attack of 128kps 50 bandwidth. This would be more than enough to stop must eCommerce sites, or to at least make this site to be /. (Slashdoted[2]).

To prevent this specific DoS attack the solution is to either timeout to clean up a connection or like stated on the mail on bugtraq to implement a working “tcp intercept” feature.

To prevent the second attack little could be done, as this would flood our network.

Potential point of attack

The preferential point of attack in my opinion would be the DNS server , this is must of time the must critical point of any infrastructure and if this server is located on the same subnet as other servers, it can be used as a point of attack to other servers that can be protected by reverse proxy servers or load balancers.

Bind as had security advisories recently, and this attack would depend on the ability of the GIAC enterprises to have their DNS servers updated. Exploits for bind are generally easy to find on the Internet, on sites like packestorm, netflood.

In fact the best point of attack is not a server but the firewall, because it will grant us access to the entire structure of the organization. This network design shows that firewalls should not be the only line of defense in any organization.

---

[2] A Friendly DoS attack

References

Mastering Cisco Routers. Written by Chris Brenton ISBN 0-7821-2643-X

SANS. http://www.sans.org/

Jeff Stelzner Certification Paper. http://www.sans.org/y2k/practical/Jeff_stelzner_GCFW.doc

Security Focus. http://www.securityfocus.com/

Nettools. http://www.nettools.com/

Bugtraq Mailing list

Acknowledgements

To my girlfriend Carla for having the patience to cope with me.
To SANS for delaying the deadline.