Global Information Assurance Certification Paper

GIAC Enterprises eFortune Maker
GIAC Certified Firewall Analyst
Practical Assignment
Version 1.5b
Scott Marshall

Assignment 1 – Security Architecture

Question

Define a security architecture for GIAC Enterprises (GE), a growing Internet startup that expects to earn $200 million per year in online sales

Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access 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).

Answer

Introduction

Much detail is lacking from this question, leaving the network requirements very much open and unspecified. For example:

- transmission or delivery mechanisms for purchases of online fortunes;
- transmission mechanisms of fortunes being translated;
- transmission of data to and from suppliers;
- billing information (suppliers, customers, and partners), electronic, or manual?;
- requirements of customer, partner, and supplier access to the Company's network environment;
- local network traffic and VPN traffic;

General Assumptions

Without knowing the business operations of the Enterprise, we need to make some assumptions:

- GIAC Enterprises is B2B only, but also hosts its own web site including ftp.
- No fail-over/redundancy is directly provided for in the network. However, the hardware and software combination recommended provides these functions.
- Custom integrated software may be developed for delivery and receipt of traffic from customers, suppliers, and partners. No rules are configured for this transfer other than HTTP on the web server and port 1433 (SQL Server) on the database

server

- Standard Internet-connected network services are required, including DNS, email (SMTP through sendmail), HTTP, HTTPS.

To be able to design a solution down to firewall and router rules, this assignment must therefore develop not just a network architecture, but gather some ideas of the software architecture for customer business to operate within these bounds.

Partner Network Requirements

A partner to GE is a company that translates and resells fortunes.

We will provide the following:

- Partners require privileged access to the Private Data Services Network (PDSN) to retrieve and update data and possibly operate other applications through a proxy service.
- No other services on the internal LAN are required. However, the design supports this through a single set of firewall rule modifications;
- No other specific computing services are required of the Company by any Partners;
- Bill presentation and bill payment will not be covered in this document;

A partner will be given access only to update data on particular database servers, but no access, other than access such as that provided for customers and suppliers.

My proposed solution will allow the following services for partners:

- Data upload and download on restricted GE web servers;
- Database access through port 1433 to the database server
- Use of public DNS and web servers and database servers

Customer and Supplier's Service Requirements

A supplier to GIAC Enterprises is an external party that writes fortunes for the Company. A customer to GE is a company that purchases online fortunes.

We assume the following for suppliers:

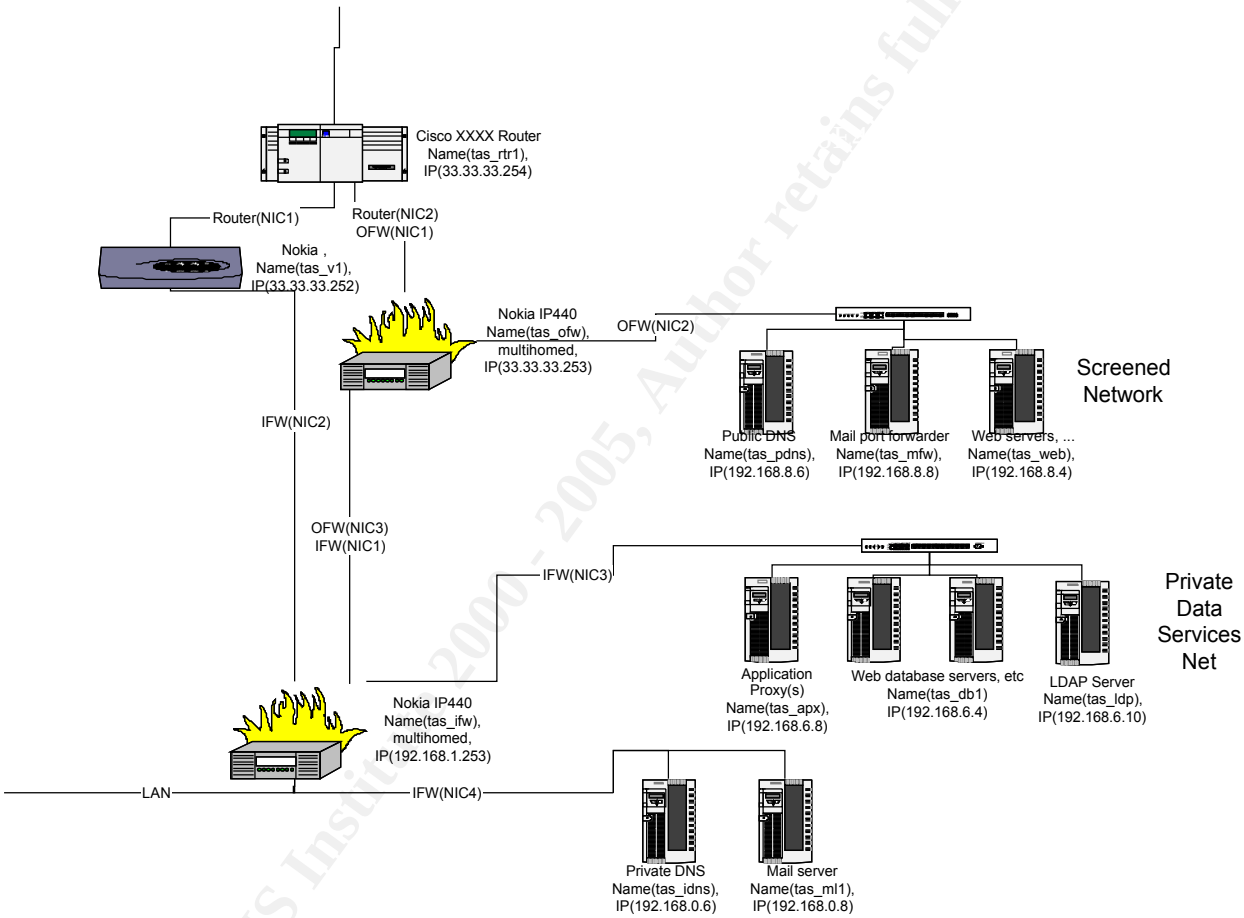
- fortunes will be provided (uploaded or downloaded) electronically through a simple secure Internet method rather than paper-based, or a dial-in method; we assume HTTP and HTTPS is required;
- no access to services on the internal LAN are required;
- no other specific computing services are required of the Company by any Suppliers;

My proposed solution will allow the following services for suppliers:

- File upload and download on access restricted GE web servers;
- XML or text upload of fortune cookies over HTTPS to a designated HTTP server in GE.

Network Architecture Diagram

Below is the proposed network structure. Please see the next section on considerations in designing this network.



Architecture Overview

The solution proposed has been designed with training in mind. It allows many possible expansion options. The solution assumes that partners will access GE's VPN services through the Internet only. Only one connection to GE's network is assumed here. In practice, a additional or redundant link may also be included.

The Cisco 3640 router can have multiple WAN interfaces. It is expandable to quite a large

number of LAN interfaces. Only 2 are used in this solution, leaving future expansion. Expected throughput is significantly larger than the traffic expected for this network.

We will route internet traffic into two sources: Nokia VPN hardware device, and the outer firewall protecting the DMZ and inner network.

The Nokia IP440 firewall device is a rack mount unit easily capable of sustaining throughput for a company such as this. They run a BSD OS implementation customised for the firewall and routing task, and run Checkpoint's Firewall-1. Other nice features of the Nokia devices are:

- Can be clustered
- Use new Intel hot-swappable PCI chipset, so PCI cards can be changed while the firewall is running
- Expandable with additional PCI cards
- Include some built-in log storage
- Easy web interface configuration
- Use Checkpoint Firewall-1 version 4.1 SP2

The outer firewall will be used to:

- Control access from the Internet to the DMZ
- Control access from the Internet to the inner firewall
- Permit access to database services in the Private Data Services Net by servers in the DMZ
- Permit traffic from application proxies in the PDSN to the Internet in order to serve internal LAN requests
- NAT internal addresses to external

The public DNS server will be located in the DMZ. This will publish only required information for Internet services. A split DNS is used, with an internal DNS server described later.

A store-and-forward server will be used for incoming SMTP services coming into our network. A port forward without NAT will be used for POP services. This lets us set up an intermediary between any clients wishing to perform such services and our mail server, hidden behind the second firewall.

GE will run conventional web servers producing HTTP and HTTPS traffic for delivery of fortunes to customers, and upload by suppliers. No other services are provided externally.

The second firewall allows authorised and valid traffic into the inner networks. It's main uses are:

- Add authenticated and unencrypted VPN traffic (from partners) to the PDSN
- Disallow all VPN sourced traffic from the private LAN
- Duplicate rules of access for VPN users to DMZ as for LAN users
- Allow database traffic from DMZ to enter the PDSN

- Allow internal LAN traffic and VPN traffic to enter PDSN
- Allow traffic from the Internet to return to the application proxies
- Allow administrative access to PDSN and screened net by authorised users.

An IP330 may be suitable for this firewall upgraded with an extra NIC. However, it is recommended that an IP440 be used as downtime of this firewall causes more major network service problems and has better potential capacity. A quick discussion is given later in this assignment.

A short consideration follows on software not yet discussed.

As earlier discussed, data transmission for customers and suppliers is through HTTP and HTTPS. Partners also require such access.

We assume a management TCP port of 8888 for web-managing web servers. Server administration should be accessible only from the LAN.

We will provide SMTP and POP access to partners. This would come under business requirements and may not be required in practise.

The database servers may be running MS SQL Server. (Let's assume this) For queries, etc, TCP port 1433 is used for communications. Other options for SQL Server include named pipes, IPX, … Partners, HTTP servers, and private LAN clients are permitted to access the database server using this method. In practise, the database server may be on Oracle, in which case different database ports are required.

Proxy services are available in the PDSN on port 8080 for HTTP, HTTPS, and FTP.

VPN, customer, partner, and supplier web authorisation uses an LDAP server located in the PDSN.

Partners are using a subnet in the range 192.168.4; if this is not true, firewall NAT-ing can occur. However, this is not covered here. It is assumed that NAT has already occurred to this subnet, so this address space is safe to use internally.

Firewall admin can take place from any internal LAN client. In practice, access would probably be further restricted, possibly through the LDAP server.

This solution has used a simple SMTP store-and-forward and POP port forwarding setup for mail. The internal mail server connects to the screened net mail host to collect new mail. Incoming POP requests work through the port forwarding. To avoid the internal mail server from being connected to from either outside our network or by the mail server, different software will be used on the mail forwarder server. This improves security, but there are also potential vulnerabilities in this additional software too!

Summary

This solution has room to grow into a full, high traffic global network through simple routes. This can occur through adding hardware load balancers or firewalls and upgrading the VPN box. Firewall-1 supports dynamic clustering and failover and this works fine with the Nokia range suggested. Failover occurs in the order of 300ms after a box dies. However, we display here, only a lowly populated network with a single web server and single database server. This can be easily built upon should needs require by simply adding hardware and configuring Firewall-1 to be in a clustered configuration.

Hardware upgrade downtimes are minimal for the firewalls, as NICs are hot-swappable.

Firewall reliability is reportedly high and can be clustered and load balanced, ensuring scalability and reliability. It is further possible to add load balancing web and database solutions with little modification.

Access restriction to the private LAN goes through two firewalls with a port forward for POP and store-and-forward for SMTP, enabling simple hiding of servers.

Because VPN access for partners is probably as important as web or application serving, the PDSN sits on the inner firewall rather than the outer, improving the security to the detriment of network reliability. This of course introduces has multiple failure points. If access from Internet to all services is required in preference, the PDSN may be connected to the outer firewall. This would segregate the screened net and PDSN from the private LAN, and remove all VPN access for partners should the inner firewall go down.

As discussed above, the current network has multiple failure points in the firewalls. Downtime of either firewall results in failure of all web serving activities. However:

- If the outer firewall goes down, the private LAN still functions, machines in the PDSN are still accessible from the LAN, and VPN services to the machines in the PDSN still function. No internet connectivity to the DMZ is available.
- If the inner firewall goes down, the private LAN still functions. Static web serving may still occur. No other services are available.

To improve the VPN hiding, we can move the VPN server to a NIC on the outer firewall (OFW). The VPN server would still connect to the IFW also. This would provide a protected VPN server.

However, in this design, it has been linked to the IFW as:

- The source traffic to the VPN server is encrypted, the end traffic unencrypted.
- The screened net is just that – it contains either public information going to the Internet or only public information from the Internet screened and protected from uncrontrolled viewing. Traffic is generally unencrypted or insecure within the subnet.
- The PDSN contains our more secure service functions required to support less vulnerable services, such as a database server to support the web server. Information, again, is generally unencrypted, but protected by passwords or need-to-know authorisations and services.
- The private LAN is purely private; no traffic is permitted in without passing through another of our controlled subnets.

Therefore, VPN traffic it is logically distinct from the traffic passing through the OFW and has been separated as such. Compromisation of the screened net or PDSN is unlikely to lead to insecurity of either the VPN partners or private LAN.

Assignment 2 – Security Policy

Question

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

Answer

I describe a security policy for:

- Border router
- Outer firewall
- Inner firewall
- Mail forwarding server
- VPN access

The subnets used are:

Subnet	Defined
192.168.8	Screened net
192.168.6	PDSN
192.168.4	VPN subnet
192.168.1	Subnet from firewall to firewall
192.168.0	Private LAN
33.33.33	Internet subnet

Testing is briefly covered of the OFW, as this is most useful to this assignment.

Border router

Two NICs are used on the router:

- eth0 to VPN appliance
- eth1 to outer firewall

IPaddress 33.33.33.254
Local IP address (eth1): 192.168.1.1

The border router will perform ingress and egress rule checking, along with port filtering.

Configuration:
interface Serial 0
ip address 33.33.33.254

Inbound ACLs:

```
!
! Deny local subnet addresses:
!
access-list 101 deny   ip 192.168.0.0 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 10.0.0.0 0.255.255.255 any log
!
! Deny packets with localhost, broadcast, multicast, and
missing destination IP addresses:
!
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny   ip 255.0.0.0 0.255.255.255 any log
access-list 10 deny    ip 240.0.0.0 7.255.255.255 any log
access-list 101 deny   ip 224.0.0.0 7.255.255.255 any log
access-list 101 deny   ip host 0.0.0.0 any log
!
! Prevent spoofing. Deny incoming packets that have
! our internal address:
!
access-list 101 deny   ip  0.0.0.255 any log
!
! More spoofing prevention. Deny any traffic destined for the
router.
!
access-list 101 deny   ip host 33.33.33.254 any log
!
! Allow only ACKed tcp packets to our network:
!
access-list 101 permit tcp any 33.33.33.0 0.0.0.255 gt 1023
established
!
! Allow only specific ICMP:
access-list 101 permit icmp any 33.33.33.0 0.0.0.255 3 0  !
net-unreachable
access-list 101 permit icmp any 33.33.33.0 0.0.0.255 3 1  !
host-unreachable
access-list 101 permit icmp any 33.33.33.0 0.0.0.255 3 3  !
port-unreachable
access-list 101 permit icmp any 33.33.33.0 0.0.0.255 3 4  !
packet-too-big
access-list 101 permit icmp any 33.33.33.0 0.0.0.255 3 13 !
administratively-prohibited
access-list 101 permit icmp any 33.33.33.0 0.0.0.255 4    !
source-quench
access-list 101 permit icmp any 33.33.33.0 0.0.0.255 11 0 !
ttl-exceeded
!
! Allow smtp traffic to mail servers only:
!
access-list 101 permit tcp any host 33.33.33.249 eq smtp pop
```

```
!
! Allow incoming dns traffic to name servers only:
!
access-list 101 permit udp any host 33.33.33.250 eq domain
!
! Allow incoming HTTP, HTTPS, and FTP traffic
!
access-list 101 permit tcp any host 33.33.33.247 eq http
access-list 101 permit tcp any host 33.33.33.247 eq https
access-list 101 permit tcp any host 33.33.33.247 eq ftp
!
! Allow VPN traffic to VPN Server
!
access-list 101 permit tcp any host 33.33.33.252 eq 50
access-list 101 permit ip any host 33.33.33.252 proto eq 500
!
! For ftp clients:
! Not very secure. The alternative is to remove this and
! force clients into passive mode.
!
access-list 101 permit tcp any eq 20 169.254.92.0 0.0.0.255 gt
1023
!
! Log everything that does not meet the above rules.
!
access-list 101 deny   ip any any log
!
! End of access-list 101
```

Our outbound ACLs are relatively lax. This is because the firewalls have already processed all outbound traffic. Allow all traffic originating from a NAT-ed address to exit the network. We explicitly deny any internal or reserved addresses from exiting the network. This ACL acts on the input side of both NIC1 and NIC2 of the router.

```
!
! Beginning of access-list 102
!
!
! Only allow packets from our network.
!
access-list 102 permit ip 33.33.33.0 0.0.0.255 any

!
! Log everything else:
!
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 102 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 102 deny   ip any 192.168.0.0 0.0.255.255 log
!
access-list 102 deny   ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny   ip any any log
!
! End of access-list 102
!
```

Other required settings:

```
! External interface of screening router:
```

```
!
no ip directed-broadcast ! don't send out broadcasts
no ip proxy-arp    ! don't respond to arps
no ip unreachables     ! Don't send icmp for denied items in
access-list.
ntp disable  ! disable network time protocol for the router
!
! Apply access list to external interface:
!
ip access-group 101 in
ip access-group 102 out
!
ip accounting access-violations
```

Mail forwarding server
Default gateway: 192.168.8.254
With Linux, we use:

```
ipmasqadm portfw –a –P tcp –R 192.168.0.8 110
```

Note that we do not perform reverse masquerading. We could easily do this by adding a local address to this command, and modifying the firewall rules. The firewall rules would now need to allow externally addressed traffic from the DMZ into the private LAN, as reverse masquerading port forwarding will rewrite the IP packet headers. This rule simply redirects all traffic to port 110 (POP3) on the internal mail server.

Outer firewall
Three NICs are used on the outer firewall:

- eth0 from router, ip address 33.33.33.253
- eth1 to screened net, ip address 192.168.8.254
- eth2 to inner firewall, ip address 192.168.1.253

Default gateway 33.33.33.254

Routing:

Device	Remote Address
eth0	33.33.33.254 (thru gateway)
eth1	192.168.8
eth2	192.168.1 192.168.6 192.168.0

Routing must occur from the router connection through to the screened net, and the PDSN. No other traffic originating from the Internet will be permitted through the firewall. However, we also need other NIC settings to allow traffic from the screened net to the PDSN, and the IFW to the OFW. Remember that the VPN server is connected between the router and IFW, this is covered here in the rules, but note the options discussed above WRT connecting the VPN server to the IFW. This would require only small changes in rules.
The OFW performs NAT on internal addresses, mapping screened net servers and the application proxy to use static public IP addresses. No other servers should have NAT performed.

The following NAT table should be configured on the firewall:

Host	Public IP	Local IP
VPN server	33.33.33.252	192.168.4.254
Public DNS server	33.33.33.250	192.168.8.6
Mail server	33.33.33.249	192.168.8.8
Web server(s)	33.33.33.247	192.168.8.4
Proxy server	33.33.33.245	192.168.6.8

Suppliers and customers access GE's services through the OFW. Traffic originating from the Internet should have the following general rules applied:

- Allow all inbound UDP DNS requests to the public DNS server
- Allow all inbound FTP, HTTP, HTTPS traffic to the screened net web server
- Allow all inbound POP and SMTP connections to the mail forwarder
- Deny and alert any traffic for private LAN or VPN.

Servers in the screened net require the following connections outside the subnet:

- Web server allowed to connect to database server on TCP port 1433
- Mail forwarding server permitted to connect using POP and SMTP to internal mail server

Services for IFW required:

- Allow TCP and UDP requests from private DNS to either public DNS or secondary internet DNS server
- Allow TCP POP and SMTP connections from private mail server
- Allow all outbound connections by application proxy

Let's summarise this into a table, before finally tightening, merging, and optimising the rule base. Consider the following a starting point:

Action	Source	Destination	Protocol	Service	Track
NIC1 main rules (To Internet/router)					
ACCEPT	ANY	192.168.8.6	UDP	DNS	
ACCEPT	ANY	192.168.8.4	TCP	HTTP HTTPS FTP	
ACCEPT	ANY	192.168.8.8	TCP	POP SMTP	
DROP	ANY	192.168.0	ANY	ANY	Alert
DROP	ANY	192.168.4	ANY	ANY	Long
REJECT	192.168.0	ANY	ANY	ANY	Alert
NIC2 main rules (Screened net)					
ACCEPT	192.168.8.4	192.168.6.4	TCP	1433	
ACCEPT	192.168.8.8	192.168.0.8	TCP	SMTP POP3	
ACCEPT	192.168.8.6	!(192.168)	UDP	DNS	
ACCEPT	192.168.0	192.168.8.4	TCP	8888	

NIC3 main rules (IFW)					
ACCEPT	192.168.0.6	192.168.8.6	ANY	DNS	
DROP	192.168.0.6	ANY	ANY	DNS	Short
ACCEPT	192.168.0.8	192.168.8.8	ANY	SMTP POP3	
ACCEPT	192.168.6.8	192.168.8.4	ANY	HTTP HTTPS FTP	
ACCEPT	192.168.6.8	!(192.168.8)	ANY	ANY	

Now, the final version:

Action	Source	Destination	Protocol	Service	Track
ACCEPT	ANY	192.168.8.4	TCP	HTTP HTTPS FTP	
ACCEPT	192.168.8.4	192.168.6.4	TCP	1433	
ACCEPT	ANY	192.168.8.8	TCP	POP SMTP	
ACCEPT	192.168.6.8	192.168.8.4	ANY	HTTP HTTPS FTP	
ACCEPT	192.168.0	192.168.8.4	TCP	8888	
DROP	ANY	192.168.0	ANY	ANY	Alert
DROP	ANY	192.168.4	ANY	ANY	Long
ACCEPT	192.168.6.8	!(192.168.8)	ANY	ANY	
ACCEPT	ANY	192.168.8.8	TCP	POP3	Short
ACCEPT	192.168.8.8	192.168.0.8	TCP	SMTP POP3	
ACCEPT	ANY	192.168.8.6	UDP	DNS	
ACCEPT	192.168.8.6	!(192.168)	UDP	DNS	
ACCEPT	192.168.0.6	192.168.8.6	ANY	DNS	
DROP	192.168.0.6	ANY	ANY	DNS	Short
ACCEPT	192.168.0.8	192.168.8.8	ANY	SMTP POP3	
REJECT	192.168.0	ANY	ANY	ANY	Long
DROP	ANY	ANY	ANY	ANY	Short

We see that this is a much smaller rule base than the following for the internal firewall. This is because the IFW handles requests from a larger set of sources, whilst the external firewall handles mostly HTTP traffic and responses made from internally. It should be obvious from the table that we value our services more than those of the VPN. We send an alert for any traffic attempting to enter our private LAN, but only a log entry for the VPN.

ACCEPT ANY 192.168.8.4 TCP HTTP HTTPS FTP
This rule allows through the more common requests coming from the Internet, those being the supply of HTTP, HTTPS, and FTP traffic from client requests.
Possible vulnerabilities here are generally the web server application itself or a denial of service attack.

To test, we need to map the three ports specified in this, and attempt to connect using a variety of IP flags. Also, we can try spoofing a return address to test the network structure.

ACCEPT 192.168.8.4 192.168.6.4 TCP 1433
We now allow through database traffic from the web server to the database server. A potential vulnerability exists here if the web server becomes compromised to the extent of leapfrogging vulnerabilities in the database server.
Testing of this is not possible from an uncompromised host, as the rule specifically allows connections between two hosts on a known port. No traffic bound for the destination subnet in this rule is permitted through the router.

ACCEPT ANY 192.168.8.8 TCP POP SMTP
Next, SMTP (for receipt of mail from other mail services) and POP (a user attempting to check mail) are allowed to the mail forwarding server. This server would then redirect the port back through the firewall to our internal mail server on the private LAN.
This represents minimal vulnerabilities since our main mail server is well hidden away behind the two firewalls, NAT-ing of the forwarding server, and throttling settings on the TCP/IP stack port handling whilst processing incoming connections.
This machine may be vulnerable to attack if incorrectly configured. For example, half opening many connections to this host may either cause it or the firewall problems. If the configuration of the server has not allowed throttling of connections, a DDOS opportunity exists here. Similarly, a mail flood may also bring down both firewalls and mail servers.
Destructive testing of this server could use these techniques. Non-destructive testing may involve testing the server's TCP/IP stack remotely for its configuration or flavour.

ACCEPT 192.168.6.8 192.168.8.4 ANY HTTP HTTPS FTP
Next up, connections and traffic are allowed between the application proxy in the PDSN to GE's web server over HTTP, HTTPS, and FTP.
This represents a potential vulnerability if the public web server is compromised – clients accessing GE's web server will be retrieving (through the proxy) potentially compromised data.
Testing of this rule would occur from a client in the LAN or VPN using the proxy server to access the company's web server.

ACCEPT 192.168.0 192.168.8.4 TCP 8888
Connections from inside the LAN are now permitted to the administration port for iPlanet Web Server.

DROP ANY 192.168.0 ANY ANY Alert
DROP ANY 192.168.4 ANY ANY Long
Any traffic is now dropped that's heading directly to our LAN or the VPN. An alert is raised if the connection is going straight to the private LAN. A detailed log entry is recorded if the connection was bound to the VPN.

This rule protects the private LAN at the outermost firewall level, preventing any connections into the LAN. This rule is most likely to occur on a compromised screened net server or possibly an internal intruder physically connected on a subnet. Testing would occur on a similar basis, attempting any sort of connection into the LAN. An alert should be raised within Firewall-1.

ACCEPT 192.168.6.8 !(192.168.8) ANY ANY
The application proxy is now allowed to connect to anywhere outside of the screened net. This rule must go below the above two rules to ensure that the proxy's only allowed destination using the current rule, is heading to less secure areas. Generally, the proxy would be connecting to HTTP, HTTPS, and FTP. However, the company may also use other protocols over the proxy, so we broaden the rule here.
Due to its position in the rule base, this rule will allow the proxy server to connect to anywhere on the internet. As with the corresponding rule for the proxy server to connect to the screened web server, this rule can be tested by using the proxy server to connect to a remote host.

ACCEPT ANY 192.168.8.8 TCP POP3 Short
ACCEPT 192.168.8.8 192.168.0.8 TCP SMTP POP3
POP3 connections are now enabled from anywhere to our mail forwarder. This will generally be from the Internet. We record a short log entry for tracking purposes for this traffic.
Next, the port forwarder is permitted access to the internal mail server. Subject to the notes above regarding SMTP and POP vulnerabilities, it is possible using port forwarding to exploit vulnerabilities in the private mail server.
Testing of the first rule occurs through connecting from the internet to the mail forwarder for a POP3 session (port 110). Ensure that a short log entry is generated for both successful (server running) and unsuccessful connections (eg half-connect with timeout).
The latter rule is tested by connecting to the mail forwarder on SMTP or POP. This should then allow the mail forwarder to connect to the internal mail server to redirect the port.

ACCEPT ANY 192.168.8.6 UDP DNS
ACCEPT 192.168.8.6 !(192.168) UDP DNS
ACCEPT 192.168.0.6 192.168.8.6 ANY DNS
DROP 192.168.0.6 ANY ANY DNS Short
DNS traffic is now handled. We accept any connections to the public DNS server over UDP. This prevents zone transfers.
Next, the public DNS server is allowed to connect outside out network using UDP executing DNS (preventing zone transfers through this server).
We next allow the private DNS server to access our public DNS server using either TCP or UDP. This allows zone transfers of GE's domain records internally. It further, lets the private DNS server as it's secondary name server.
Finally, we drop DNS queries from inside our LAN to any other DNS server.
Testing of the first rule can occur by performing an nslookup on any machine inside or outside our network.
The second rule allows the DNS server to connect to any external DNS server over

UDP. This is looser than most rules. To test, execute a DNS query to a non-cached host (or freshly started DNS server daemon) to the public DNS server. It should then connect to the ISP's or another DNS server to retrieve the network and host information.
The third rule is tested by executing a name lookup (on an unknown host) inside the LAN. The private DNS server then asks the public DNS for the answer.
The final rule forces the dropping of any other connections or traffic from the private DNS server to any other host for DNS information. This would require poisoning of the private DNS configuration to test.
Note that no facility in these rules allows TCP DNS connections. These are untested here, but drop through to the DROP ANY ANY rule.
Use of the split DNS stops GE's private LAN from having a poisoned DNS for any length of time, assuming the private DNS forwards (and doesn't cache) queries for hosts it doesn't know about, but caches local information.

ACCEPT 192.168.0.8 192.168.8.8 ANY SMTP POP3
Next, SMTP and POP connections are permitted from our mail server to the mail forwarder, who can then forward the requests out to the Internet.
Testing of this rule occurs by the internal mail server connecting to the mail forwarder, and sending mail to an external mail server.

REJECT 192.168.0 ANY ANY ANY Alert
DROP ANY ANY ANY ANY Short
Finally, any connections originating in the private LAN to anywhere not already permitted are rejected, and an alert raised. An alert is generated in preference to a log entry, as the IFW has, in this case, allowed traffic out that shouldn't be permitted, indicating a configuration issue. Generally though, no other traffic will use this rule, so we send an alert.
All other connection attempts are dropped and a short log entry generated. This log entry is mainly useful (in this case) for debugging rule sets or for optimisation, to determine what traffic that isn't considered in the rule-base is also on the network.
Testing of the first rule can occur by an internal client telnet-ing to an internet address. No NAT-ing rules are configured for LAN clients, and no direct external access is permitted, testing this rule. An alert should be raised in Firewall-1 if this condition arises.
The final rule drops any other traffic.

Inner firewall
Four NICs are used on the inner firewall:

- eth0 from VPN, ip address 192.168.4.254
- eth1 from outer firewall, ip address 192.168.1.254
- eth2 to PDSN, ip address 192.168.6.254
- eth3 to private LAN, ip address 192.168.0.254

Routing should be configured between all subnets:

Device	Remote Address
eth0	192.168.1 192.168.8
eth1	192.168.4

eth2	192.168.6
Eth3	192.168.0

Note here that we are assuming stateful connections, specifying below only the source of a connection.

Partners access the network through the VPN server. Once processed, the following traffic rules should apply:

- Allow all TCP and UDP DNS requests to screened net
- Allow all TCP HTTP and HTTPS traffic to screened net
- Allow all TCP SMTP and POP traffic to screened net
- Allow TCP 1433 (SQL) to data server
- Allow access to application proxy on TCP 8080
- Allow ICMP(pong, source quench) to screened net and data net
- Deny all traffic to private LAN
- Deny all Internet bound traffic
- Deny remaining traffic

The following traffic rules should apply to traffic originating in the private LAN:

- Allow TCP and UDP traffic from private DNS to public DNS
- Disallow all other DNS traffic from exiting this interface
- Allow all outbound connections on TCP SMTP to public mail forwarder
- Allow all TCP HTTP and HTTPS traffic to screened net
- Allow all TCP 8080 traffic to application proxy
- Allow all TCP SMTP (from internal mail server) and POP traffic to screened net
- Allow TCP 1433 (SQL) to data server
- Allow SSH access to all servers in screened net and PDSN
- Allow pcAnywhere access to all servers in screened net and PDSN
- Allow ICMP(pong, source quench) to screened net and data net
- Deny all traffic to VPN interface
- Deny remaining traffic

On IFW (inner firewall) NIC3 connecting the PDSN, the following traffic rules will be engaged:

- Allow DNS requests from the application proxy to public DNS
- Allow requests from application proxy to all external addresses passing through the outer firewall.

On IFW NIC1 connecting the OFW, the following traffic rules will be engaged:

- Allow TCP port 1433 from web server to database server
- Allow SMTP and POP TCP connections from the port forwarding server in the screened net to the internal LAN
- Allow LDAP connections to the PDSN only originating from either the VPN or either firewall

Implicitly, we also:

- Allow pcAnywhere and OpenSSH TCP return traffic to the private LAN
- Allow return DNS traffic from screened net

- Allow return traffic to the application proxy

Let's translate these into suitable firewall rules. As fitting the architecture, we'll use Firewall-1. Rules are further described later. They are arranged in a particular order; this is described later also. Rules which permit or deny traffic with a minimum of rule match searching assist the performance of the firewall. It is therefore necessary to optimise the rules somewhat, so the above interface based rules are interspersed when designed.
Similarly, some rules must be merged or dropped to cater for other rules' requirements in restricting traffic, and other rules added to provide extra logging where appropriate. Consider the following a starting point:

Action	Source	Destination	Protocol	Service	Track
NIC2 main rules (VPN)					
ACCEPT	192.168.4	192.168.8.6	UDP TCP	DNS	
ACCEPT	192.168.4	192.168.8.4	TCP	HTTP HTTPS	
ACCEPT	192.168.4	192.168.6.4	TCP	1433	
ACCEPT	192.168.4	192.168.6.8	TCP	8080	
REJECT	192.168.4	192.168.0	ANY	ANY	
REJECT	ANY	192.168.4	ANY	ANY	
DROP	192.168.4	ANY	ANY	22 (ssh)	Log
DROP	192.168.8	ANY	ANY	22 23 (telnet)	Log
DROP	192.168.4	ANY	ANY	PcAny	Log
NIC4 main rules (LAN)					
REJECT	ANY	192.168.0.6	TCP	DNS	Log
ACCEPT	192.168.0.6	192.168.8.6	UDP TCP	DNS	
ACCEPT	192.168.0	192.168.8.4	TCP	HTTP HTTPS 8888	
ACCEPT	192.168.0	192.168.6.8	TCP	8080	
ACCEPT	192.168.0.4	192.168.8.8	TCP	SMTP	
ACCEPT	192.168.0.4	192.168.8.8	TCP	POP	
ACCEPT	192.168.0	192.168.6.4	TCP	1433 (sql)	
ACCEPT	192.168.0	192.168.8	TCP	22 (ssh)	
ACCEPT	192.168.0	192.168.8	TCP	pcAnywhere	
REJECT	192.168.0	192.168.4	ANY	ANY	Log
NIC3 main rules (PDSN)					
ACCEPT	192.168.6.8	192.168.8.6	UDP	DNS	

ACCEPT	192.168.6.8	ROUTER	TCP	HTTP HTTPS FTP
NIC1 main rules (OFW)				
ACCEPT	192.168.8.4	192.168.6.4	TCP	1433
ACCEPT	192.168.8.8	192.168.6.4	TCP	SMTP POP
ACCEPT	33.33.33.252	192.168.6.10	TCP	LDAP LDAPS
ACCEPT	33.33.33.253	192.168.6.10	TCP	LDAP LDAPS
ACCEPT	192.168.1.253	192.168.6.10	TCP	LDAP LDAPS
ACCEPT	192.168.8.4	192.168.6.10	TCP	LDAP LDAPS
Default Rule				
DROP	ANY	ANY	ANY	ANY

Merged, optimised for provision of services over the Internet, and tightened, the rule base transforms to:

Action	Source	Destination	Protocol	Service	Track
ACCEPT	192.168.8.4	192.168.6.4	TCP	1433 (sql)	
ACCEPT	192.168.0	192.168.6.4	TCP	1433	
ACCEPT	192.168.4	192.168.6.4	TCP	1433	
ACCEPT	192.168.6.8	ROUTER	TCP	HTTP HTTPS FTP	
ACCEPT	192.168.0	192.168.8.4	TCP	HTTP HTTPS FTP 8888	
ACCEPT	192.168.4	192.168.8.4	TCP	HTTP HTTPS FTP	
REJECT	ANY	ANY		NETBIOS	
ACCEPT	192.168.8.8	192.168.0.8	TCP	SMTP POP3	
ACCEPT	ANY	192.168.8.6	UDP	DNS	
DROP	ANY	192.168.8.6	TCP	DNS	Long
ACCEPT	33.33.33.252	192.168.6.10	TCP	LDAP LDAPS	
ACCEPT	33.33.33.253	192.168.6.10	TCP	LDAP LDAPS	
ACCEPT	192.168.8.4	192.168.6.10	TCP	LDAP LDAPS	

ACCEPT	192.168.1.253	192.168.6.10	TCP	LDAP LDAPS	
ACCEPT	192.168.0	192.168.6.8	TCP	8080	
ACCEPT	192.168.4	192.168.6.8	TCP	8080	
ACCEPT	192.168.0.4	192.168.8.8	TCP	SMTP	
ACCEPT	192.168.0.4	192.168.8.8	TCP	POP3	
REJECT	ANY	192.168.0.6	TCP	DNS	Long
ACCEPT	192.168.0.6	192.168.8.6	UDP TCP	DNS	
ACCEPT	192.168.4	192.168.8.6	UDP TCP	DNS	
ACCEPT	192.168.0	192.168.8	TCP	22 (ssh)	
ACCEPT	192.168.0	192.168.8	TCP	pcAnywhere	
DROP	192.168.4	FIREWALL	ANY	FWADM	Alert
DROP	192.168.8	FIREWALL	ANY	FWADM	Alert
ACCEPT	192.168.0	FIREWALL FIREWALL2	ANY	FWADM	Long
DROP	ANY	FIREWALL FIREWALL2 ROUTER	ANY	FWADM	Long
REJECT	192.168.0	192.168.4	ANY	ANY	Long
REJECT	192.168.4	192.168.0	ANY	ANY	Long
DROP	ANY	192.168.0	ANY	ANY	Alert
DROP	192.168.4	ANY	ANY	22 (ssh)	Long
DROP	192.168.8	ANY	ANY	22 23 (telnet)	Long
DROP	192.168.4	ANY	ANY	PCAnywher e	Long
REJECT	ANY	192.168.4	ANY	ANY	Short
DROP	ANY	ANY	ANY	ANY	Short

This rulebase has been streamed to ensure that network traffic that will occur more frequently occurs earlier in a search for a rule matching an action for the packet.

Here, we are expecting database traffic to be a very major component of traffic on the firewall, followed by HTTP and HTTPS traffic. The remainder of the rules block specific packets and enable some maintenance or system administration traffic.

A brief run-down on rule groups is now given.

ACCEPT 192.168.8.4 192.168.6.4 TCP 1433 (sql)
ACCEPT 192.168.0 192.168.6.4 TCP 1433
ACCEPT 192.168.4 192.168.6.4 TCP 1433
These rules allow clients in the LAN or from the VPN to access the database server. In addition, the web server in the DMZ is permitted access. Note that we allow a specific host in the screened net, versus subnets which are more secure.

This protocol is used for client applications to execute queries on a database server. SQL Server commonly uses this port. Care should be taken, as traffic to and from (ie results) are returned clear-text.
If a server in the screened net is compromised, it may be possible for the intruder to execute SQL commands if authentication succeeds. However, this is the only mechanism by which this can occur except with a physical attack.

ACCEPT 192.168.6.8 ROUTER TCP HTTP HTTPS FTP
ACCEPT 192.168.0 192.168.8.4 TCP HTTP HTTPS FTP 8888
ACCEPT 192.168.4 192.168.8.4 TCP HTTP HTTPS FTP
This group of rules allows any HTTP (port 80), HTTPS (port 443), or FTP (port 21) access to the company's web server, and permits the application proxy access to the router to proxy client requests.
Within the internal firewall, vulnerabilities related to HTTP exist only through the downloading of dangerous code within HTML or through this source, representing a threat to internal business services. Someone may have already penetrated the OFW through a web server vulnerability. The rule set above allows only outgoing HTTP connections.

REJECT ANY ANY NETBIOS
NetBIOS may be used to obtain information about clients on GE's network. There is no need for this to pass through the firewall to any other subnets and so is closed off completely. This is not logged, and may occur relatively frequently.

ACCEPT 192.168.8.8 192.168.0.8 TCP SMTP POP3
This rule allows the mail forwarding machine to forward requests for these mail protocols to an internal server, hiding it from the Internet. It opens up a connection only from the port forwarding machine to particular services on the internal server. This may be a vulnerability if one exists in the port forwarding which may allow a DOS. Alternatively, the store-and-forward SMTP application may have a vulnerability. This may cause a significant problem if the server is compromised.

ACCEPT DROP 8 192.168.8.6 UDP DNS
This rule allows only UDP DNS requests from the application proxy to the public DNS server. Private LAN DNS requests are covered by a separate rule.
By allowing this rule and disabling all other DNS, is not possible to obtain any network information about the private LAN. A TCP DNS request may indicate a zone transfer; this is not possible through the UDP protocol.

DROP ANY 192.168.8.6 TCP DNS Long
This rule goes hand in hand with the above rule, disallowing potential zone transfers. Further, we log any attempted TCP DNS requests.

ACCEPT 33.33.33.252 192.168.8.10 TCP LDAP LDAPS
ACCEPT 33.33.33.253 192.168.8.10 TCP LDAP LDAPS
ACCEPT 192.168.1.253 192.168.6.10 TCP LDAP LDAPS

LDAP is used for authentication on the VPN as well as firewall. It is not used for authenticating users on GE's web site, but the potential exists for this.
LDAP is not considered a critical risk as it is used for specific purposes and contains no customer-sensitive information in the store. LDAPS is LDAP over SSL.

ACCEPT 192.168.0 192.168.6.8 TCP 8080
ACCEPT 192.168.4 192.168.6.8 TCP 8080
Here, we specifically allow connections to the application proxy on port 8080 using TCP.That is, proxy services are available only to partners and internal employees. This is not considered a security risk and serves to improve security.

ACCEPT 192.168.0.4 192.168.8.8 TCP SMTP
ACCEPT 192.168.0.4 192.168.8.8 TCP POP3
SMTP and POP are used for mail transfer; our rule pair here allows connections from the internal mail server outwards to the port forwarding server, to send outgoing email, or for the mail server to connect outwards to gather mail.
On the internal LAN, this is not considered a risk.

REJECT ANY 192.168.0.6 TCP DNS Long
This rule rejects any TCP DNS requests to the internal DNS server. No connections are permitted into the private DNS server from outside the LAN. Allowing this traffic may allow a party external to the LAN to gather network information.

ACCEPT 192.168.0.6 192.168.8.6 UDP TCP DNS
ACCEPT 192.168.4 192.168.8.6 UDP TCP DNS
Now, however, we allow requests from the private DNS server to the public DNS sever, and VPN users to access the public DNS server.

ACCEPT 192.168.0 192.168.8 TCP 22 (ssh)
ACCEPT 192.168.0 192.168.8 TCP pcAnywhere
Allow system administration traffic into the screened net from the private LAN. We allow two services only, ssh and pcAnywhere. pcAnywhere allows remote GUI administration of a Microshaft server using encrypted transmission. Ssh traffic is also encrypted. All management traffic to and from the screened net must be encrypted as the screened net is potentially unsafe.

DROP 192.168.4 FIREWALL ANY FWADM Alert
DROP 192.168.8 FIREWALL ANY FWADM Alert
ACCEPT 192.168.0 FIREWALL FIREWALL2 ANY FWADM Long
DROP ANY FIREWALL FIREWALL2 ROUTER ANY FWADM Long
These rules allow only firewall administration. We specifically drop all traffic from the VPN to the firewall for administration, and raise an alert to the administrator.
Similarly, raise an alert for any traffic to the firewall originating from the screened net to the firewall.
However, we also allow traffic from the private LAN to either firewall for administration.
All other traffic firewall administration traffic is dropped.

Cleanup rules now are appended, raise more alerts and logging and traffic denials

REJECT 192.168.0 192.168.4 ANY ANY Long
REJECT 192.168.4 192.168.0 ANY ANY Long
Disallow any traffic from the internal LAN to the VPN, and vice versa. Add a long log entry when this occurs. We consider these two networks completely disjoint, and consider any attempted traffic between the two to be a possible violation.

DROP ANY 192.168.0 ANY ANY Alert
Any other clients attempting to connect to the private LAN are dropped, and an Alert raised, but the traffic dropped, rather than alerted.

DROP 192.168.4 ANY ANY 22 (ssh) Alert
DROP 192.168.4 ANY ANY PCAnywhere Alert
DROP 192.168.8 ANY ANY 22 23 (telnet) Long
Any management traffic coming from the VPN is explicitly denied and an alert raised. Telnet traffic to the screened net is logged and dropped.

REJECT ANY 192.168.4 ANY ANY Short
This rule catches any other traffic not handled by the above stateful rules denying traffic into the VPN. Response traffic is still allowed through, but anyone attempting to connect into the VPN will be denied. A short log entry is generated.

DROP ANY ANY ANY ANY Short
Final rule; drop any other traffic we haven't explicitly handled.

VPN access
VPN access occurs through the Nokia CC2500 VPN server (suitable for a regional office gateway traffic load). Currently, it connects directly to the inner firewall from the router. Ideally, this should probably be connected between the two firewalls to protect the server. As noted initially in this assignment, customers on the VPN have possible already been NAT-ed to 192.168.4; no traffic is permitted from the VPN to any other traffic.
To ensure adequate and standard security, we'll use an IPSEC VPN. ESP (Encapsulated Security Payload) will be used. This encrypts normal traffic and wraps it into another packet. AH can also be used, but this is an message authentication methodology only. We prefer encrypted traffic whenever possible, so will stick to ESP. One thing to note with using the two protocols is:

- ESP, since is encapsulates traffic, the original address, before being encrypted for the VPN must be NAT-ed to 192.168.4;
- AH, as it includes an authentication header, cannot have a NAT-ed address, as rewriting the address would modify the required authentication header.

This is not a serious issue, as from with partners, private addresses could be NAT-ed

before being passed to the VPN gateway. However, as noted, encrypted traffic is preferred.

Although the traffic isn't greatly privileged (eg we're not transmitting personal information), we still use encryption. We can, in theory, therefore perform key exchange infrequently if desired. However, considering the small overheads in renegotiating keys on a well utilised network, we cause little extra traffic by increasing key negotiation periods. I therefore choose to renew keys every 84 hours, guaranteeing a key exchange twice a week.
Encryption and authentication will use triple DES (3DES), with MD5 hash for authentication of the message

IPSEC security negotiation requires the following ports and protocols:

- TCP Port 500 (key exchange)
- IP Protocol 50 (data traffic)

Assignment 3 – Audit your Security Architecture

Question

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

- Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
- Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
- Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Answer

Plan the assessment

An assessment is planned for the network structure. To perform a formal network security audit, we need to analyse a number of different areas of the network:

- Test viewing of the network from outside of GE's
- Test connections from subnets
- Check appropriate hardening of relevant servers
- Analyse redundancy, scalability of network
- Analyse administration and data handling processes
- Analyse risks
- Determine vulnerabilities of installed components

Given that there's no coversion needed here, we can plan the attack here without consequences except GE's potential downtime. Where necessary, I note possible times for analysis where risks may be high or the time of day assists the testing.

Cost Estimate

The cost estimate is broken down according to times required. Two cost estimates are given, that of an assessment similar to that performed in this assignment, and a full formal assessment. Times and costs could still be significantly higher if we're permitted to attempt deep penetration of the network.

Brief Assessment

Note that these times represent a middle-ground for a cheap consultancy of a fairly basic analysis, recommendations, and documentation of structures and findings.

Item	Time

Analysis of network	13 hours
Analysis of hosts	5 hours
Investigation of vulnerabilities	5 hours
Analyse risks	6 hours
Total	29 hours

Based on a rate of $120 per hour for this type of consultancy, the cost would be approximately $3480. (Figures in Australian dollars)
These figures also purely note the work of the contractor; a network administration resource would also be required on behalf of the company for approximately 40% of the time.

Formal Assessment
A formal assessment covers the same tests as the brief assessment, but performed by a well respected consultancy, and includes more invasive testing. It is hard to predict, without including specific requirements, top and bottom end amounts. For example, a free reign may be given on attempting to penetrate a network.
A middle-ground is therefore presented allowing some investigation of some potential weaknesses that may be found. Also, in practice, a broader consultancy may occur including discussions with management affected by DRP, deeper risk analysis, and security policy, password, access, and physical security policies, server examinations and hardening, etc. Again, we restrict the time recommended for this item.

Analysis of network (testing and gathering from subnets, internet reconnaissance, some covert testing, alert testing)	18 hours
Analysis of hosts (hardening, access and configuration)	12 hours
Investigation of vulnerabilities (including invasive testing)	14 hours
Risk analysis (externally and network)	8 hours
Security policy and procedures examinations	10 hours
Total	62 hours

Based on a rate of $150 per hour for this type of consultancy, the cost would be approximately $9300. A full consultancy testing and covering all of the network operations is likely to take approximately 3-6 times this period and cost, depending on the level of assurance and independent testing required.
These figures also purely note the work of the contractor; a network administration resource would also be required on behalf of the company for approximately 50% of the time.

A significant risk exists in performing extremely invasive penetration testing of the network. Such testing may include exposing vulnerabilities which would disrupt the company's normal network operations. If this is to be attempted in the analysis it is recommended that company subnets be made unavailable for short periods of time at the least disruptive time. If covert intrusion is attempted, much of this would need to be non-disruptive, and possible log generating activities would be planned for times when other similar messages are likely to appear. Hackers are also likely to perform their activities between 9PM and 6AM, outside of common working hours, or the weekend.
For an international eCommerce business, much of the traffic is probably generated during US business hours, but with a general spread around the day. Some log messages may occur at times of day suiting the average hacker who uses these methods.

Test viewing of the network from outside of GE's
This can take place on multiple levels:

- Determining publicly available network information

- Scanning of our network
- Intrusion of our network

Through www.arin.net we can find out the public IP address range, company information, and support contact information about the network. This gives us a start with possible email addresses and number of hosts publicised.
Continuing with public information, DNS queries will expose the IP and external hostname of the web server, mail server, and router.

Intrusion of our network is not covered in this section.

Scanning of our network will use two tools:
- Ping and traceroute
- Nmap

Ping will tell us if we can get an ICMP echo request and echo reply message to hosts we're interested in or not. This is handled by the nmap covered later.
Traceroute potentially shows us the path to the server we're interested in, include routers and firewalls that traffic must pass through to the host.

Let's probe firstly, with a full ping scan GE's whole public IP address range with nmap. We could also try the broadcast and multicast addresses, and all of these would be in a full network audit. In our configuration, the multicast addresses would be blocked by the router. Testing might raise alarms, but that's okay, and we're not being destructive or disruptive to the network… ☺ As we're likely to raise alarms, testing would be performed during normal business hours, to avoid unnecessary callouts. If we were trying to be covert, randomised and time-fed map attempts would be included to avoid IDS tripping.
The first nmap should show which hosts are accessible through public IP addresses.

Secondly, we run an nmap ACK scan against the router and firewall. This will show ports that are open on these two devices, with no application listening for that port.

A full nmap is now attemped against all servers discovered above.
That nmap command is likely to show up most services available from the outside on GE's public IP range! What we'd expect to see here includes:
- All ports listening for TCP on accessible hosts
- No response on the ports listening for UDP
- ICMP Admin Forbidden on TCP ports blocked by the router

Continuing, try nmap-ing over UDP and a half-open TCP scan. These, again, will return similar results to the above.
Given this and using simple DNS queries to determine mail hosts, web servers, etc, we can then use techniques to determine the server version running. For example, server headers are returned from a web server stating the server type. Mail servers can also return their version to a client connection.
As most successful intrusions occur due to configuration errors, it's more than likely a vulnerability can be found in either a server software application (eg web server, mail forwarder, DNS), it's configuration, or data available on the server.

Test connections from subnets
Connections should be tested from all subnets:
- VPN
- Private LAN
- Screened net host

- PDSN host

This gives us a picture of the traffic permitted throughout GE's network. For this assignment, we will cover only the private LAN and a screened net host. The other perspectives are behind the inner firewall. They would, however, be tested in a full network audit. Here, we are interested mainly in perimeter defense.
Techniques used here will be similar to those used to test connectivity from the internet, using nmap to determine listening sinks. However, we will mainly be interested in ensuring that specific traffic is or isn't permitted to specific target ports.

Analyse redundancy, scalability of network
We determine the paths into the network, determine failure points and how redundancy can be implemented, and determine how the network should scale. GE is expecting business to grow to $200m this year, amounting to a large number of fortunes and traffic.

Analyse business processes and procedures
We do not cover this in this assignment. The assignment deals with perimeter defence, rather than disaster recovery procedures, etc. In a formal network audit, processes and procedures such as the following would be examined:

- Disaster recovery procedures
- Intrusion detection and incident handling methods
- Support contacts and information, including network appliance support information
- Procedures for maintaining and administering the firewall
- Physical security
- … the list goes on

Determine vulnerabilities of installed components
The following components have been installed on the network.

- Version of Firewall-1 4.1 SP3
- Router Cisco 3640 router
- iPlanet Web Server Enterprise Edition 4.1 SP7
- iPlanet Directory Server 4.13

It is not uncommon for web and ftp servers to have vulnerabilities, so we will research potential known vulnerabilities of these components.
Also, the web server above uses an administration server port, by default, 8888. Testing from the outside should include an attempt to get to this port to check for misconfiguration. Directory Server uses 389 for normal queries, and 636 for SSL tunnelled queries.

Implement the assessment
This section is kept brief, and along the lines of testing from subnets and from the internet, above. Generally, the other sections above are covered in the perimeter analysis in the following section.

Public Information
Public information that will be gleaned includes:

- Mail server: 33.33.33.249
- Web server: 33.33.33.247
- DNS server: 33.33.33.250

As well as the company's IP range (eg 33.33.33.240/16).

Internet Scanning

1. Traceroute

It is possible for the effects of a traceroute to be different between different operating systems. For example, Windows uses only ICMP, whilst Unix uses both ICMP and UDP for a traceroute.

In our case, an ICMP Echo Request is not permitted into our network. We will therefore see a traceroute to the request server, but with the last hop being the last router before GE's outer router.

2. nmap ping scan

An nmap ping scan over the entire network will be blocked at the router, as ICMP is restricted.

Nmap would report that ping (echo request) is administratively prohibited at the router.

Now, unfortunately, without performing more intrusive testing, we're limited to the IP addresses that we gleaned gathering public information. The brief scan would continue based on these known addresses.

3. ACK scan of router

The ACK scan of the router will show open or non-blocked ports:

Port	Status	Service
25/tcp	open	SMTP
110/tcp	open	POP3
53/udp	open	DNS
80/tcp	open	HTTP
443/tcp	open	HTTPS
21/tcp	open	FTP
XXXXX IPSEC	open	key exchange

4. ACK scan of outer firewall

The ACK scan of the OFW will show open or non-blocked ports:

Port	Status	Service
25/tcp	open	SMTP
110/tcp	open	POP3
53/udp	open	DNS
80/tcp	open	HTTP
443/tcp	open	HTTPS
21/tcp	open	FTP

5. ACK scan of DNS server and mail server:

The DNS server scan reports:

Port	Status	Service
53/udp	open	DNS

The mail server scan reports:

Port	Status	Service
25/tcp	open	SMTP
110/tcp	open	POP3

Subnet Scanning
Subnet scanning is similar to the above, but occurs from each interesting subnet. Here, I cover only from the screened net, and the private LAN.

We can try a number of things here:

- Plug in a new host with a different IP address. This should allow scanning of the firewall only on network rules, rather than host-based rules.
- Scan from an existing machine. This may disrupt services and requires security to be opened on the server temporarily to allow the testing to take place.

1. Screened net
On a new host with new IP:

With a new host, the following ports should be open for transmission f. From this interface, we'd expect the following:

Port	Status	Service
80/tcp	open	HTTP
443/tcp	open	HTTPS
21/tcp	open	FTP
1433/tcp	open	SQL Server
25/tcp	open	SMTP
110/tcp	Open	POP3

This list is similar to that found above from externally. However, we now also see the SQL Server query port. It should also be noted that from particular hosts in the screened net, this list would be reduced, as the host doesn't have access to all ports.

Nmap-ing the IFW will return a very small number of open ports, including proxy server and database server access.

2. Internal net
Scanning from the internal net should give a very restricted number of services available. The mail server has access to the mail server in the screened net. All other clients have access to specific servers, such as:

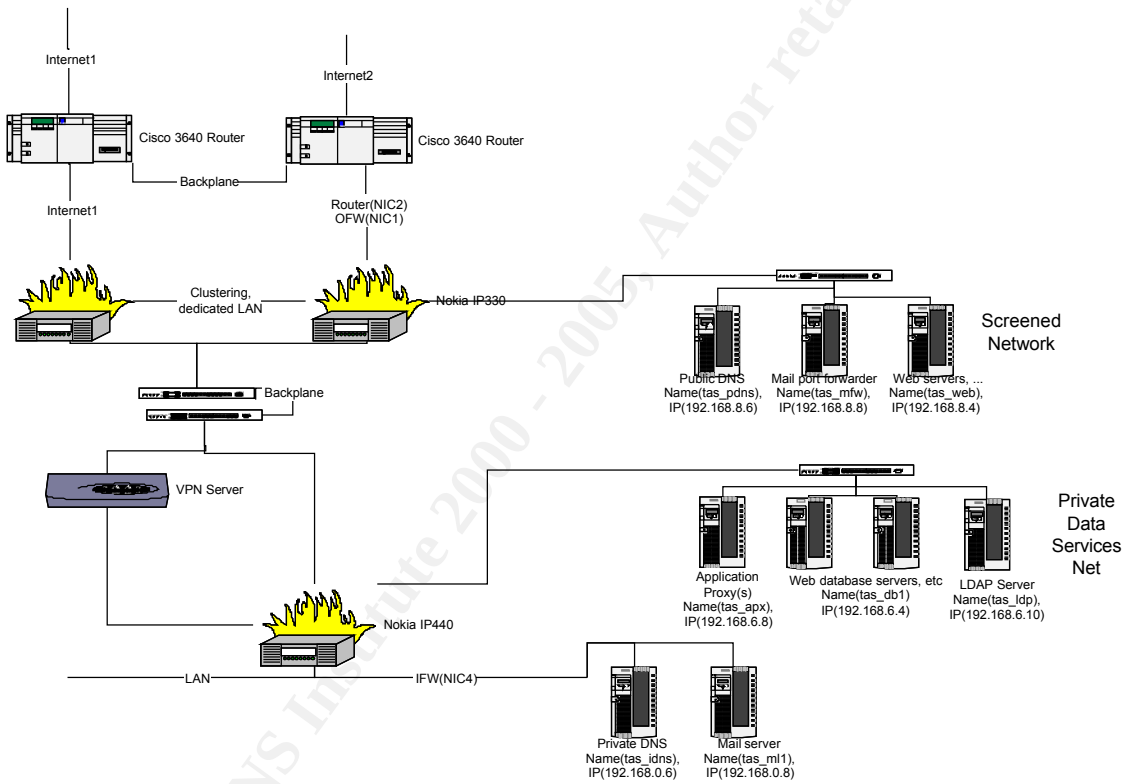
- Internal mail server
- Proxy server in the PDSN
- Web server in the Screened net
- DNS access should be permitted from inside
- SQL Server port on the database server

Conduct a perimeter analysis
Public Reconnaisance
Our public reconnaissance showed us the publicly accessible servers such as mail, web, and dns. Also, our IP range was discovered.

Internet Scanning
Internet scans have shown the publicly available services and no more. Access to the PDSN or private LAN requires compromising of a server in the screened net. The most likely cause of any intrusion is by misconfiguration or vulnerabilities in software components. iPlanet Enterprise Server is by far the most vulnerable component, with close to a dozen vulnerabilities reported in the last six months.

The software chosen (and properly upgraded) is resilient to most protocol attacks.

Recommendations
The network's single-point of failure is it's biggest drawback. The network can be made to be resistant to most attacks, but a DDoS will significantly reduce network throughput.
A recommended improvement to the structure is:



This network will cater well to most attacks:

- VPN traffic goes through the outer firewall, with unencrypted traffic separated
- DDoS traffic must be sufficient to saturate the two internet connections, the two routers (on two public IP addresses) and two clustered outer firewalls
- Internal traffic must still traverse two firewalls to the LAN

The results would be discussed with major stakeholders and responsible network administrator(s) regarding any problems discovered. Follow-up checks are also advised. A regular audit should also be performed to ensure that procedures are followed, sign-offs are performed on network modifications, etc.

It is probably also recommended that TCP Wrappers be used to further hide the mail server

to scans.

Assignment 4 – Design Under Fire

Question

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

- An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
- A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
- An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Answer

For this assignment, I'll operate on Dave Chen's design (see http://www.sans.org/y2k/practical/Dave_Chen_gcfw.zip).

His network design is shown below:

This network has been designed as a full-failover hot site if either of the internet connections fall over, rather than a redundant connection. It is not clear what is in the Services Segment. The Cisco IP tunnel router connection I believe is a VPN connection through the internet to the opposite network. No allowance is made for the duplication (or replication) or the private sharing of internet, services, and data at both sites, although possibilities exist in configuration of various network components to do this.

Effectively, these are two separate public networks connected to another WAN. The two Firewall-1 components protect in to this WAN.

Attack and compromise of either side of the internet connection will lead to effects on the other.

Three attacks are attempted:

- Determine vulnerabilities of firewall and attack the firewall
- A denial of service attack
- An attack plan for compromising an internal host.

Vulnerabilities

Assume that the software is the latest, so:

- NAI Gauntlet for Solaris version 6.0
- Checkpoint Firewall-1 Solaris version 4.1 SP3.

Firewall-1 had exposed a number of security holes at the BlackHat conference in 2000 (see slides at http://www.dataprotect.com/bh2000/. The hole were discovered in version 4.0 SP5 running on an Nokia IP440. Tests repeated later on version 4.1 SP1 indicated that some attacks were still possible, whilst some were fixed. Reportedly, although this hasn't been confirmed, subsequent releases fixed these problems. See www.phoneboy.com for more information.

The latest vulnerability reported for Firewall-1 on January 17, 2001 and is related to a Denial of Service. This vulnerability is applicable to this firewall. It causes high load on the firewall CPU when a large number of source routed packets from invalid IP addresses are permitted into a firewall interface. (See www.securityfocus.com for more info). No other reported vulnerabilities are still outstanding on a well-configured Firewall-1 installation.

A search reveals no vulnerabilities have been reported for the latest version of NAI Gauntlet, version 6.0.

We therefore come across the situation where there are no known vulnerabilities in the firewall we can exploit in the first stage.

However, unless one is attempting to cause a DOS, it is usually more useful to penetrate the firewall and compromise an internal host. This allows much greater hiding of the hacker's activities. Attempting to muddle with the firewall from outside the network will generally give us more information about the protected hosts, without causing as many alarms. A compromised host is less likely to be noticed than a firewall being tampered with.

Other possible attempted intrusion points include the VPN (external clients), VPN server, and router.

A denial of service attack

Here, I choose the TFN2k remote DDOS tool to perform an attempted denial of service attack.

This is capable of performing ICMP, UDP, and TCP floods. It is controlled by a master program, with clients installed on other machines, often compromised. A DDoS can be triggered at the master's will, interspersing traffic and sending decoy traffic.

The effects of an attack are difficult to predict with perfect accuracy without physically attempting this with a replica network. However, we can build some expectations based on how the routers and firewall should be configured. Remember that attacking either of the east or west zones would be expected to yield the same results, given the mirror image. However, in practice, some settings may or may not have been replicated correctly.

To minimise the effects of a flood and generally improve security, as a minimum, some ICMP traffic must be restricted at the router. This is a two way stick. By restricting ICMP, some network functions are limited slightly. Some should be disabled as they're not really needed, such as redirects. One of the most important methods is to disallow private network addresses into the firewall to minimise spoofing. Disabling of router direct broadcasts is essential. Some ICMP traffic is useful, such as the ping and ping response. However, these typically open up DDoS opportunities.

Most DDoS attacks are caused by script kiddies, as in reality, it's pretty pointless. Writing the code to do an attack is quite trivial. Once a new vulnerability is discovered, most vendors react fairly quickly to release a patch to cover the hole, or an advisory on how to fix the problem. However, this is too late in the wild. As discovered above, a DoS opportunity exists in Firewall-1 currently. Always keeping up to date with patches helps to maintain the network integrity.

Given that the selected answer in this assignment blocks all ICMP traffic, the network will be relatively unaffected by a DDoS attempt. The internal firewalls restrict the level of penetration of any amplified attack. However, with only particular UDP and TCP ports available through thr router, we'd need very high numbers of packets to saturate the company's links and affect the services segment significantly.

An attack plan for compromising an internal host

A number of commercial software products may be used in the network. Unfortunately, this was outside the scope of Dave Chen's network.

There are three layers of security in this network:

- Router
- Outer firewall
- Inner firewall

In this assignment, I cover only compromising a machine in the services segment.

A number of small investigations uncover much information about the company's public network, including the IP addresses for the public servers (mail, dns, ftp, http), and the IP range allocated to the organization (through *whois*).

As discussed elsewhere in my practical, web servers can return a version number in headers, and some mail programs will happily report a version number to the outside world. Any number of sources on the Internet will display a list of known vulnerabilities of the software discovered. Vulnerabilities are common:

- It is extremely difficult to maintain software versions and upgrades in a production environment, giving falling security confidence over time;
- Errors in configuration of routers, firewalls, or service hosts is very possible;
- Custom software operating with (eg web servers) allows programmer introduced vulnerabilities to occur;
- An attacker needs only find one vulnerability, whilst network administrators need to close all, including many they don't know about.

Vulnerabilities may include:

- Buffer overflows
- Misconfigurations
- Back-doors
- Path handling errors

- Root shells
- Authentication responses and interpretations
- …, it's a long list

With sufficient time it's possible to penetrate many network structures. The structure analysed here is well resistant to DDoS attacks, as they're located on different sides of the country, ensuring fully redundant traffic paths to any server. However, to do this, more hardware would be required to operate correctly. Router rules and firewall rules are tight enough to limit most nasty traffic, so we should aim for vulnerabilities in the network.