Global Information Assurance Certification Paper

Assignment 1 - Security Architecture (25 Points)

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acq uisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component. 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).

GIAC Enterprises Business and Systems Environment

As with any security architecture, the first step is to get an understanding of the business an d systems environment to understand what it is we are trying to protect and from whom. During the course of this analysis a number of additional business and technical requirements or constraints were uncovered. These include:

- The fortune cookie manufa cturing industry consists of around 200 organisations world wide – thereby defining the maximum expected number of customers. Most of these are technically advanced, with highly automated manufacturing environments, and are seeking just -in-time delivery of all component parts (including fortune cookie sayings). Thus they require a real -time on-line interface which will allow a variable sized batch of sayings to be delivered on demand. The sayings will be customised for example due to the size of cooki es being produced (larger cookies obviously allow a longer and more profound saying). Customers will be pre -registered by their GIAC Account Executive prior to accessing the site.
- The generation of Fortune Sayings is a cottage industry with tens of thous ands of small producers, most of whom are prepared to pass on their words of wisdom with little or no payment (in fact many are willing to pay for the privilege of having their sayings published).
- The recent merger has been with the Cantonese International Advertising Group (CIAG) - an advertising agency which plans to sell advertising space on the reverse side of fortune cookie sayings. To enable this they require access to the GIAC customer database which is hosted on the GIAC corporate network.
- Remote access to the GIAC network is required for 50 account executives who are highly mobile and technically illiterate. These need full access to the corporate network, but do not need access to the production network. To eliminate the need for modem infras tructure and the cost of international calls, the account executives will use local Internet Service Providers to obtain Internet connectivity, and then VPN based access into the GIAC network.

Security Architecture for GIAC Enterprises

The security archit ecture for GIAC enterprises is shown in Figure 1. It features a separate production e -commerce environment in which the core on -line business functions are implemented, in addition to the corporate network which houses the company's normal internal busin ess functions such as e -mail, payroll, etc.

The e-commerce environment is a three tier application environment using two physically separate firewall devices to separate the three tiers as well as the Internet and the corporate network. Authentication to the e -commerce web server is via client digital certificates for all suppliers, partners and

customers. The web server is configured to require SSL client certificate authentication, thereby reducing the scope of attack of the web server to only pre -registered suppliers, partners and customers. Attack of the SSL establishment phase of the connection is still possible by anyone on the Internet.

The customer and translation partner interfaces – which provide functionality to download the valuable sayings – use digitally signed XML messages to provide additional levels of security and non -repudiation. Client certificates are provided via a Verisign Onsite service hosted by Verisign – this is outside the scope of this discussion.

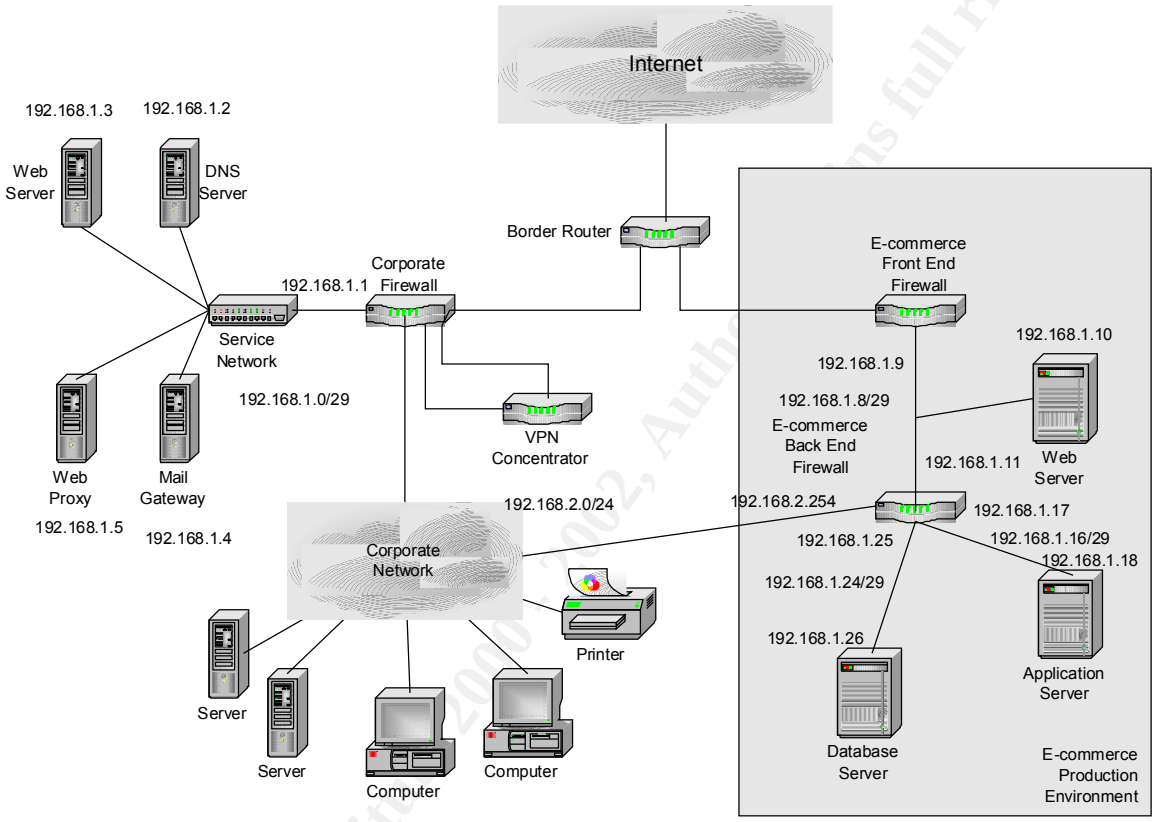


Figure 1 - GIAC Enterprises Security Architecture

The users on the corporate network access the Web via an out bound Web proxy which performs content filtering (eg of Active -X) and also logs usage and sites visited.

The key perimeter devices, are as follows:

Border Router

The border router is a CISCO 7204 router [1], running IOS 12.1. It provides Internet connectivity for both the e-commerce and corporate networks. The main security functions of the border router are to p rovide ingress and egress filtering, and to filter out traffic which is not required into either network, and which may result in excessive "noise" in the firewall logs.

[1] Future plans will provide redundancy of Internet access via two separate ISPs; however these are not detailed here.

Ingress filtering is designed to prevent packets with forged source IP addresses (whic h correspond to addresses within the GIAC networks, as well as other illegal or private address ranges) from entering the GIAC networks.

Egress filtering provides more of a "community service" for the rest of the Internet, rather than providing protection to the GIAC networks. It prevents packets with forged source IP addresses (ie those which do not emanate from the GIAC networks) from leaving the GIACS networks. This prevents denial of service attacks such as smurf attacks [http://www.cert.org/advisories/CA -1998-01.html] from being launched from within the GIAC networks.

"Noise" filtering will prevent inbound traffic to services which are commonly used to attack or probe networks, and f or which there is no business need. This includes:

- NetBIOS ports
- Back Orifice
- NetBUS
- Other trojans

This list of blocked ports will be modified based on the ongoing examination of firewall logs. Particular services which are denied by both firewalls, and which result in excessive log entries due to regular probing activity, will also be added to the border router access lists.

E-Commerce Front End Firewall

The E-commerce front end firewall is a Cisco PIX 515 running PIX firewall software version 5.3(1) . This firewall is protecting the front end web server segment of the E -commerce environment. It is dedicated to this task to simplify the rule set thereby minimising the likelihood of configuration errors (which could lead to security exposures).

This firewall allows only two types of traffic into the web server segment regardless of source IP address:

- HTTPS (TCP port 443) to the web server [2];
- ICMP echo requests to the web server (to allow pings to the web server to allow customers, suppliers and partners to test the network connectivity to the web server).

While permitting the ICMP echo requests into the web server segment does marginally increase the scope for attack (particularly denial of service attacks), the business need to provide simple testi ng of network connectivity for customers, suppliers and partners means that this connectivity must be allowed.

The firewall must allow the following traffic outbound from the web server segment:

- Responses over HTTPS (TCP port 443) on the web server;
- ICMP e cho replies

E-Commerce Back End Firewall

The E-Commerce back end firewall is Cisco PIX 515 running PIX firewall software version 5.3(1). This firewall acts as a choke between the web server segment and the application segment, between the application seg ment and the data segment and also to allow management traffic from the corporate network into the three e -commerce segments. The access rules for each of the segments will be discussed in turn.

[2] Netscape Enterprise Server 4.0 on Solaris 2.8 built according to the SANS Solaris step -by-step and running a Web Sphere Applica tion plug in – for those people doing an assignment and wanting to attack this one.

Traffic between the web server segment and the application server segment is restricted to the single port used for the WebSphere Servlet engine – TCP port 8110. This minimises the scope for attack on the application server in the event that the web server is compromised.

Traffic between the application server and the database server is again restricted to the single port that is required to provide the database functionality – in this case the Oracle listener will be configured to use TCP port 1526.

The database server is running on its own segment and will not initiate any outbound connections.

Remote management of the database, application and web servers is performed via SSH from the corporate network. Hence TCP port 22 is allowed into each of these segments from the corporate network. In addition ICMP is allowed between the corporate network and the 3 e-commerce segments via the backend firewall.

Corporate Firewall

The corporate firewall is also a Cisco PIX 515 running PIX firewall software version 5.3(1). It has 5 interfaces, corresponding to the Border Router, the Service Network, the encrypted VPN network, the decrypted VPN network (ie traffic to and from the corporate side of the VPN termination device), and the main corporate network.

Access to each of these network segments is discussed in turn below:

The service network provides the following functions, each of which is hosted on a dedicated server:

- The company's public web server with largely static content. Access to this server is allowed from both the Internet and the Corporate network (via the proxy server) over HTTP and HTTPS (TCP port 80 and 443).
- The external DNS server provides resolution of external DNS names for the internal DNS server, as well as the authoritative source for GIAC public addresses. A secondary DNS server is provided by the ISP. Access to the DNS server is allowed from both the Internet and the internal DNS server on the corporate network to resolve DNS queries (UDP port 53). In addition the secondary external DNS server (hosted by the ISP) is allowed access to perform zone transfers (TCP port 53). To allow external name resolution, the DNS server must also be allowed to initiate outbound queries (UDP port 53).
- The mail gateway handles inbound and outbound mail and provides virus and content checking and filtering. SMTP access to the mail gateway is allowed from both the Internet and the Corporate network (on TCP port 25). In order to relay messages, the mail gateway also needs to be able to establish connections into the corporate network to a single mail server, and outwards to the Internet – in both cases to port 25.
- The outbound web proxy provides logging and content filtering for internal staff to access web sites on the Internet. It is accessible from the Corporate network on TCP port 80, and can initiate outbound sessions to web servers on the Internet.

In addition to the above, each of the above servers needs to be managed from within the corporate network. This will be performed via SSH, and so access to the service network from the corporate network on TCP port 22 is also allowed. As indicated earlier, ICMP echo requests and replies are also supported from the Internet and the Corporate network.

VPN Concentrator

The VPN Concentrator is a Cisco VPN 3015. It provides roaming users with access to the Corporate network (to access e-mail and other services) and also provides access from users from our partner's network to access the Customer database.

Roaming users make use of the VPN 3000 software client to obtain remote access to the GIAC network. Internet connectivity is provided using any available ISP (dial-up, cable or ADSL).

Access from the partner network is via their own Cisco VPN 3000 series gateway.

The VPN concentrator is positioned in such a way as to force all remote traffic through the Corporate firewall after it has been decrypted by the VPN concentrator. In this way a failure or misconfiguration of the VPN concentrator will not lead to traffic bypassing the firewall. In addition, incoming traffic from the Internet to the VPN co ncentrator also passes through the firewall to ensure that only legitimate IPSec traffic is being directed to it.

Assignment 2 - Security Policy (25 Points)

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.

By 'security policy' we mean the specific ACL s, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!

(Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implem ent each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protoc ol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule.

Be certain to point out any tips, tricks, or "gotchas".

The (simplified) syntax of the extended access list on a Cisco router [3] for TCP and UDP protocols is:

access-list *access-list-number* {**deny** | **permit**} {**tcp**|**udp**} source source-wildcard [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**established**] [**log** | **log-input**]

Where:

[3] A fuller discussion of the syntax of Cisco IOS access lists is available from the Cisco web site at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_r/1rprt2/1rip.htm#xtocid223482

access-list-number	Is an integer number for the extended access list in the range 100-199 or 2000-2699.
deny | **permit**	Defines whether traffic matching the rule will be permitted or denied.
tcp|udp	Defines whether TCP or UDP traffic will match this rule (note that **ip** can be used to match all ip traffic including TCP, UDP and ICMP).
source source-wildcard	The source ip address for traffic to match this rule. Note that the source wildcard is the complement of the subnet mask. The keyword **any** can be used as a shorthand for the source address and wildcard combination of 0.0.0.0 255.255.255.255.
[*operator port* [*port*]]	Optionally, the TCP or UDP source port numbers for traffic to match this rule can be specified. The operators **lt** (less than), **gt** (greater than), **eq** (equal to), **neq** (not equal to) can be used in conjunction with a single port number; while the operator **range** can be used in conjunction with two ports to specify a range of port numbers.
destination destination-wildcard	The destination ip address for traffic to match this rule. The syntax is as for the source port.
[*operator port* [*port*]]	Optionally the destination port number, specified in the same way as the source port number.
[**established**]	Optionally used to specify that TCP packets with the ACK or RST bits set will match this rule (but not the initial TCP packet with only the SYN bit set).
[**log | log-input**]	Optionally used to generate log entries when packets match this rule. The **log-input** variant will record the interface number and MAC address in the log entry.

The access lists for the Cisco PIX follow a similar format, except that access lists are named instead of numbered. The default configurations are also dependent on the security level assigned to the interfaces with connectivity allowed by default from interfaces with a higher security level to those with a lower security level, but denied from lower security interfaces to higher security ones. The PIX automatically allows return packets forming an allowed TCP session through the corresponding interface.

More information about configuring the Cisco PIX firewall is available from the Cisco web site at http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/ .

Some general tips that must be observed when configuring access lists on Cisco routers (and also the PIX firewall) are:

- Rules are order dependent – so the first rule that matches a particular packet will be applied. This means that more specific rules need to be listed before general rules. Thus when rules of the nature of permit access to anything but w.x.y.z are implemented, they must be implemented by first denying access to w.x.y.z and then permitting access to any.
- Once access lists (or any other configurations) have been applied to a Cisco device (and tested) it is essential to copy these to memory so that the configurations are not "forgotten" upon rebooting (eg after power failure).
- Access lists on a Cisco router have an implicit deny all as the terminal rule (compared to the permit all default behaviour of the interface prior to the application of the access list).
- When modifying access lists remotely be careful not to cut off your remote access to the device.
- The general router configuration should also be "hardened" to prevent attacks on the router itself. This hardening process should include

- Explicitly turning off IP small services
- Set logon messages
- Set encrypted passwords

The security policies of the following devices are defined below

- Border Router
- Corporate Firewall
- E-commerce Front End Firewall
- E-commerce Back End Firewall Corporate Firewall
- VPN Concentrator

Border Router

The security functions of the border router are ingress and egress filtering as well as filtering out noisy traffic, as described i n Assignment 1.

Ingress filtering is intended to prevent packets with incorrect source addresses from entering the GIAC network from the Internet. Incorrect source addresses would include the local loopback address, private or unassigned addresses, as well as public addresses corresponding to devices within the GIAC network. In this case, the IP address ranges which need to be filtered out are:

Address Range	Reason	Network Address	Subnet Mask
10.0.0.0 – 10.255.255.255	Private Address Range	10.0.0.0	255.0.0.0
172.16.0.0 – 172.31.255.255	Private Address Range	172.16.0.0	255.240.0.0
192.168.0.0 – 192.168.255.255	Private Address Range	192.168.0.0	255.255.0.0
127.0.0.0 – 127.255.255.255	Local loopback address	127.0.0.0	255.0.0.0
224.0.0.0 – 239.255.255.255	Multicast addresses	224.0.0.0	240.0.0.0
0.0.0.0	Invalid address	0.0.0.0	255.255.255.255
99.99.99.0 – 99.99.99.31	Public address space used by GIAC	99.99.99.0	255.255.255.224

Filtering of noisy services is a pragmatic step designed to remove unwan ted noise from the firewall logs. This “noise” results from either misconfigured systems external to the GIAC network or from (semi) malicious activity without a specific target. Initially this will be configured to filter NetBIOS (since it is not required externally and scanning for NetBIOS shares is one of the most popular past -times on the Internet). Similarly, Back Orifice and NetBUS are extremely popular targets due to their high profile, and so these will also be blocked at the border router.

New rules would be added to the filters based on ongoing monitoring of the firewall logs.

Reason	Filtering rules
NetBIOS	TCP and UDP ports 135-139 and 445 (Note although NetBIOS only uses TCP 135 and 139 and UDP 135, 137 and 138 – since there is no need for the remaining ports they will be blocked as well; thereby simplifying the access lists)
Back Orifice	UDP port 31337

NetBUS	TCP port 12345-12346

Other services such as login services, remote procedure calls, network files system, X -windows will not be blocked at the border router since these are not expected to generate a lot of noise in the firewall logs – since few people scan large address ranges looking only for these services. Normally we see these scans of wider port scans, and so in these cas es they will be blocked and logged by the firewalls.

While implementing the ingress filtering could be provided using standard access lists (ie based on source IP address only), the "noise" filtering requires the use of extended access lists since it inclu des destination address/port information. Since only a single access list may be applied to an interface, then all of the rules needed to be provided in a single extended access list.

```
!
! Access List 101 - Ingress and noise filter from Internet
!
no access-list 101
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 99.99.99.0 0.0.0.31 any log
access-list 101 deny tcp any any range 135 139
access-list 101 deny udp any any range 135 139
access-list 101 deny tcp any any eq 445
access-list 101 deny udp any any eq 445
access-list 101 deny udp any any eq 31337
access-list 101 deny tcp any any range 12345 12346
access-list 101 permit ip any any
```

This access list is then applied inbound to the Internet interface of the border router:

```
!
interface Serial 2/0
no shutdown
description connected to Internet
ip address 99.99.99.1 255.255.255.252
ip access-group 101 in
```

Egress filtering is intended to prevent packets with forged source addresses from leaving the GIAC network to the Internet. Based on the security architecture defined in Assignment 1, the only packets leaving GIAC network should have source addresses corresponding to the publicly addressable devices – which are within the 99.99.99.0 -31 range.

Egress filtering can be applied outbound on the Internet interface, using standard access lists.

```
!
! Access List 99 - Egress filter from GIAC Networks
!
no access-list 99
access-list 99 permit 99.99.99.0 0.0.0.31
access-list 99 deny any log-input
```

VPN Concentrator

The VPN concentrator allows the remote access into the corporate network from the Internet, as well as allowing restricted access between the CIAG network into the GIAC corporate network.

Remote access will use IPSec in tunnel mode with an IP address assigned from the 192.168.8.0/24 range. The Encapsulating Security Payload (ESP) protocol (IP protocol 50) will be used so as to provide both confidentiality as well as integrity and authentication. Triple -DES will be used as the encryption algorithm – providing substantially greater level of security than single DES.

Key exchange for IPSec will use Diffie -Hellman to negotiate shared secrets for use to protect the tunneled data.

In order to support a wide range of ISPs – some of whom may require proprietary "heartbeat" mechanisms to ma intain connectivity – the IPSec remote access client must operate in split horizon mode – allowing connectivity both through the tunnel as well as "outside" the tunnel simultaneously.

User authentication for remote access will occur via a SecurID card.

Detailed information about configuring the VPN 3000 Concentrator series can be found on the Cisco Web Site at http://www.cisco.com/warp/public/cc/pd/hb/vp3000/ .

The key security configurations for our deployment are as follows:

1. Tunnel Modes - Both PPTP and L2TP will be disabled since all remote access will be required to use IPSec (which will be enabled);
2. IKE Proposals – Two IKE Proposals will be active to support remote users and LAN to LAN connections respectively. Remote users will make use of the Cisco VPN 3000 series client and will be configured to use CiscoVPNClient -3DES-MD5 for IKE. This uses a pre -shared secret (configured as a password) for initial authentication, but then require s the users to provide individual authentication credentials (which will be configured to use SecureID cards). Our partner network will be configured to use IKE -3DES-MD5-RSA. This authentication mode uses a digital certificate for authenticating the pe er gateway.
3. LAN to LAN IPSec Tunnel Properties – This will explicitly define the local and remote networks by IP address and wildcard mask, as well as defining the packet level security parameters. In this case the ESP/MD5/HMAC -128 authentication mechani sm will chosen along with 3DES -168 encryption.
4. User Configuration - User authentication will be configured to use an external SDI Server (which will reside on the Corporate Network). The VPN concentrator must be configured with the IP address and UDP port number (default 5500) to use for the SDI server. IP addresses for remote clients will be assigned by the VPN Concentrator from a configured pool (with starting IP address of 192.168.8.1 and a finishing IP address of 192.168.8.254). A shared group account name and password must be set for remote users. This is in addition to the individual authentication provided by the SecureID card.

Corporate Firewall

The corporate firewall is the most complex configuration due to the wide variety of functions it is performing.

Firstly the interfaces are named and assigned a security level. These affect the default permissions, in that unless otherwise specified access is denied from an interface with a lower security level to an interface with a higher sec urity level, and access is allowed from a higher security level interface to a lower one. The Corporate Network is assigned the highest security level, while the Internet has the lowest. The assignment of the security levels for the services LAN, and t he two VPN LANs is somewhat arbitrary, except that the corporate side of the VPN should be higher the service network, to prevent a compromised server in the services network from gaining access to our partner (CIAG).

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 services security 40
nameif ethernet3 vpn_internet security 20
nameif ethernet4 vpn_corporate security 60
```

To facilitate understanding of the access lists we will use names for common servers, including b oth their public and private addresses.

```
name 99.99.99.2 pub_dns_server
name 99.99.99.3 pub_web_server
```

```
name 99.99.99.4 pub_mail_server
name 99.99.99.5 pub_proxy_server

name 99.99.99.17 pub_vpn
name 192.168.1. corp_vpn

name 192.168.1.2 dns_server
name 192.168.1.3 web_server
name 192.168.1.4 mail_server
name 192.168.1.5 proxy_server

name 192.168.2.123 internal_mail
name 192.168.2.124 internal_dns
name 192.168.2.125 indernal_sdi

name 88.88.88.88 isp_dns

name 66.66.66.66 ciag_vpn_gw

name 192.168.2.99 customer_database
```

We need to provide static Network Address Translation to allow the servers on the services network to be accessible from the internet:

```
static (services,outside) pub_dns_server dns_server netmask 255.255.255.255
static (services,outside) pub_web_server web_server netmask 255.255.255.255
static (services,outside) pub_mail_server mail_server netmask 255.255.255.255
static (services,outside) pub_proxy_server proxy_server netmask 255.255.255.255
```

The Internet interface must allow access to the DNS, Web and Mail servers on the services network from anywhere on the Internet – but only on the port(s) corresponding to their services. In the case of the DNS server zone transfers are only allowed from a single secondary DNS server hosted by the ISP and so this is the only server which requires TCP port 53 access, while all other addresses on the Internet can resolve names (using UDP port 53). The Internet side of the VPN concentrator must be accessible for IKE (UDP port 500) and ESP (IP protocol 50) – again from anywhere on the Internet to support our roaming users. Our policy of supporting ping to assist in fault resolution means echo requests are allowed from anywhere on the internet to any publicly addressable host.

```
access-list acl_outside permit udp any host pub_dns_server eq 53
access-list acl_outside permit tcp host isp_dns host pub_dns_server eq 53
access-list acl_outside permit tcp any host pub_web_server eq 443
access-list acl_outside permit tcp any host pub_web_server eq http
access-list acl_outside permit tcp any host pub_mail_server eq smtp
access-list acl_outside permit udp any host pub_vpn eq 500
access-list acl_outside permit 50 any host pub_vpn
access-list acl_outside permit icmp any any echo
access-list acl_outside deny ip any any
```

The services network must be provided with connectivity between the internal and services DNS and mail servers. The DNS server must also be able to resolve names from DNS servers external to the company (UDP port 53), and the proxy server must be able to initiate connections to Internet based web servers on TCP ports 80 and 443, but not to internal web servers. This is an example where access lists must be constructed paying careful attention to ordering.

```
access-list acl_services permit tcp host mail_server host internal_mail eq smtp
access-list acl_services permit udp host dns_server host internal_dns eq 53
access-list acl_services deny udp host dns_server 192.168.2.0 255.255.255.0 eq 53
access-list acl_services permit udp host dns_server any eq 53
access-list acl_services deny tcp host proxy_server 192.168.2.0 255.255.255.0 eq 80
access-list acl_services deny tcp host proxy_server 192.168.2.0 255.255.255.0 eq 443
access-list acl_services permit tcp host proxy_server any eq 80
access-list acl_services permit tcp host proxy_server any eq 443
access-list acl_services permit icmp any any echo-reply
access-list acl_services deny ip any any
```

The Internet facing interface of the VPN concentrator must be allowed to initiate ESP traffiic (IP protocol 50) as well as IKE (UDP port 500). It can also be pinged to help diagnosis. All other traffic is denied.

```
access-list acl_vpn_internet permit 50 host pub_vpn any
access-list acl_vpn_internet permit udp host pub_vpn any eq 500
access-list acl_vpn_internet permit icmp host pub_vpn any echo_reply
access-list acl_vpn_internet deny ip any any
```

The corporate network facing interface of the VPN concentrator will forward traffic from remote users (with a source address within 192.168.8.0/24) which can have full access t o the corporate network. VPN access from the CIAG network is allowed. This network uses the 10.1.1.0/24 private address range, and hence does not require address translation. Access from this network is only allowed to the customer database. Echo r eplies are allowed from the VPN concentrator, and the VPN concentrator is allowed to communicate to the internal SDI server to allow SecureID authentication of remote users. No other access is allowed.

```
access-list acl_vpn_corporate permit ip 192.168.8.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list acl_vpn_corporate permit tcp 10.1.1.0 255.255.255.0 host customer_database 1526
access-list acl_vpn_corporate permit icmp host corp_vpn 192.168.2.0 255.255.255.0 echo-reply
access-list acl_vpn_corporate permit udp host corp_vpn host internal_sdi eq 5500
access-list acl_vpn_corporate deny ip any any
```

The main access from the corporate network is to the outbound web proxy in the service network. In addition the internal mail system and the internal DNS n eed to access the corresponding hosts in the service network. Management of all the service network hosts and the VPN concentrator is via SSH (TCP port 22), and ICMP echo is also allowed. Access to the remote users (on the 192.168.8.0/24 network) is al so required from systems on the corporate network. All other access is denied.

```
access-list acl_inside permit tcp 192.168.2.0 255.255.255.0 host proxy_server eq 80
access-list acl_inside permit tcp 192.168.2.0 255.255.255.0 host proxy_server eq 443
access-list acl_inside permit tcp host internal_mail host mail_server eq smtp
access-list acl_inside permit udp host internal_dns host dns_server eq 53
access-list acl_inside permit udp host internal_sdi host corp_vpn eq 5500
access-list acl_inside permit tcp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.248 eq 22
access-list acl_inside permit icmp 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.248 echo
access-list acl_inside permit ip 192.168.2.0 255.255.255.0 192.168.8.0 255.255.255.0
access-list acl_inside deny ip any any
```

These access lists then need to be applied to the appropriate interfaces:

```
access-group acl_outside in interface outside
access-group acl_inside in interface inside
access-group acl_services in interface services
access-group acl_vpn_corporate in interface vpn_corporate
access-group acl_vpn_internet in interface vpn_internet
```

E-Commerce Front End Firewall

The e-commerce front end firewall will filter out all traffic from the Internet to the Web server LAN apart from HTTPS (TCP port 443) and ICMP. Return traffic is allowed from the Web Server (which will also originate from port 443, as are ICMP echo replies. While allowing ICMP into and out of the Web server LAN is an increased security risks, the business benefit it provides in ter ms of easier configuration of customer sites means that it is required.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100

static (inside,outside) 99.99.99.10 192.168.1.10 netmask 255.255.255.255

access-list acl_outside permit tcp any host 99.99.99.10 eq 443
access-list acl_outside icmp any host 99.99.99.10 echo
```

```
access-list acl_inside permit icmp host 192.168.1.10 any echo-reply
access-list acl_inside deny ip any any

access-group acl_outside in interface outside
access-group acl_inside in interface inside
```

E-Commerce Back End Firewall

The e-commerce back end firewall acts as a choke between the different segments of the e-commerce production network, as well as allowing remote management access via SSH, and ICMP pings to the production servers.

First define the different interfaces and their relative security levels. In this case the outside interface is actually the web LAN, while the inside interface is the data LAN. While these set the default traffic flows, in practice we will explicitly override these for this device.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 corporate security30
nameif ethernet3 application security60
```

To improve the readability of the access control lists we will assign meaningful names to the key servers:

```
name 192.168.1.10 web_server
name 192.168.1.18 app_server
name 192.168.1.26 database_server
name 192.168.2.0 corporate_network
```

The access list for the interface connecting to the web LAN needs to allow access from the web server to the application server on a single Web Sphere port (TCP 8110). In addition, we will allow operations staff on the corporate network to ping the web server, and so we need to allow the echo replies back to the corporate network. No other traffic is allowed.

```
access-list acl_web permit tcp host web_server host application_server eq 8110
access-list acl_web permit icmp host web_server corporate_network 255.255.255.0 echo-reply
access-list acl_web deny ip all all
```

The access list for the interface connecting to the corporate network needs to allow operations staff to manage the different servers, using SSH (TCP port 22). In addition, we allow them to ping the servers to ensure that they are alive – hence ICMP echo requests are allowed. All other traffic is explicitly denied.

```
access-list acl_corporate permit tcp any web_server eq 22
access-list acl_corporate permit icmp any web_server echo
access-list acl_corporate permit tcp any application_server eq 22
access-list acl_corporate permit icmp any application_server echo
access-list acl_corporate permit tcp any database_server eq 22
access-list acl_corporate permit icmp any database_server echo
access-list acl_corporate deny ip any any
```

The application must be able to initiate connections to the Oracle database on TCP port 1526, and again must be able to respond with echo replies to the corporate network.

```
access-list acl_application permit tcp app_server database_server eq 1526
access-list acl_application permit icmp app_server corporate_network 255.255.255.0 echo-reply
access-list acl_application deny ip any any
```

The only traffic initiated out of the database LAN are echo replies.

```
access-list acl_database permit icmp database_server corporate_network 255.255.255.0 echo-reply
access-list acl_database deny ip any any
```

The above access lists then need to be applied to the relevant interfaces:

```
access-group acl_web in interface outside
access-group acl_data in interface inside
access-group acl_corporate in interface corporate
access-group acl_application in interface application
```

Assignment 3 - Audit Your Security Architecture (25 Points)

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:

1. 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.
2. 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.
3. 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.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

Scope of Audit

To be effective, the security audit should examine not just the current technical configurations, but also the underlying operational and management processes which will maintain and update these configurations.

The first part of the assessment will be a review of the security management framework against an accepted standard such as AS-4444 or BS-7799, and will be based on interviews with key operational and management staff. This part will determine the existence and adequacy of processes such as:

- Password management
- Key management (for SSH for example)
- Change control
- Proactive Patching
- Incident response
- Documented policies
- Security Awareness
- Back up

This part of the assessment is not described in detail here.

The second phase will examine the current configurations of the technical infrastructure to try to identify any weaknesses that could be exploited by an attacker. This assessment will be confined to just the e-commerce environment – not the corporate network. The assessment will include

- A perimeter assessment identifying the connectivity from outside the production environment;
- An assessment of firewall configurations to ensure that they meet the stated policy;
- An assessment of operating system configurations to ensure that they are sufficiently secure;
- An assessment of the application components to ensure that they are sufficiently secure;

1. Assessment Planning

The technical assessment does, by its nature, involve subjecting the production environment to potentially hostile traffic (particularly if resilience to denial of service attacks is going to be tested). Such testing

should be scheduled so as to minimise the chance of disrupting service to customers – and so it is desirable to perform the testing during a period of light load. However, should somethin g go wrong, it is important for operations (and potentially second or third level support staff) to be either on site or at call to quickly assist in rectifying any faults which occur during testing. For this assignment – which deals with a mission criti cal system - a weekend would be the preferred time, with some operational staff scheduled to be on duty.

The approach to be taken for the testing is as follows (note only the network/firewall components are described in any detail):

1. Define the scope of the review based on documented architecture/network diagrams. Define all in scope and out of scope devices including identifying their designed IP address(es), the type of device, the operating system version and patch level. This information is provided in part in Assignment 1 which would need to be supplemented with the detailed application architecture.

   (Requires access to documentation which should be provided before engagement. Estimate 2 hours)

2. Initial information gathering about the GIAC environme nt from the Internet.

   This stage would use a generic Internet connection to scan the production environment from the Internet using nmap (or nmapnt on a Windows platform - note that the Windows port of nmap does not work with dial up connections). The full TCP and UDP port ranges (1 -65535) would be scanned. A TCP SYN scan would be used initially as it is substantially quicker than a TCP connect scan.

   In addition, some querying of the DNS server will be undertaken to determine whether excessive information is being provided.

   The results of this phase should just confirm the accuracy of parts of the architecture identified in step 1. The estimated time for this phase is 2 staff hours of manual effort and 2 -3 hours of unattended scanning.

3. The next phas es of testing require direct physical access to the production network. The actual operation of the firewall can be tested by probing (again using nmap) from each of the network segments in turn, and running TCPdump on the other segment to check whether traffic has made it through. We will also check the firewall logs to ensure that corresponding log entries are being generated.

   This phase of the assessment requires 2 laptops (to run nmap and TCPdump), and approximately 1 -2 staff hours per interface – so around 8 staff hours for the production environment.

4. The next phase will require local access to the individual firewall or network devices to review configurations. This will look at the overall device set up, as well as manually checking the access lists to ensure that they are appropriate. Time estimate is 1 -2 hours per device depending on the complexity of the access lists.

5. The previous phases have concentrated on the network devices. Of equal – if not more – importance is the configuration of the servers and applications which provide the business functionality. This phase would look at the operating system configurations to validate that they have been appropriately hardened, as well as the application components, such as the web server, database server and the business application (including any middleware such as Websphere in this instance).

   The operating system would be analysed against a hardened build standard (such as that defined in the SANS Step by Step series [http://www.sans.org/newlook/publications/solaris_toc.htm]. Again nmap can be used to determine which ports are open on the server, and this compared with the system design to determine whether or not the y are necessary. Allow 1 -2 hours per server for this phase.

6. Other tools (either open source or commercial) may be used to identify possible misconfigurations on the different services that are required. Of critical importance is to test the Web Server configuration – as this will be in the front line of attack. Open source tools available to assist with this include Nessus [http://www.nessus.org] as a general purpose vulnerability scanning tool, Whisker [

http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2] to concentrate on active content and scripting vulnerabilities on the Web Server, and Cerberus [http://www.cerberus -infosec.co.uk/cis.shtml] which covers much of the same ground as Nessus. Commercial tools such as ISS Internet Security Scanner and Cybercop from Network Associates may also be used. These tools do – in general – provide better reporting functions, with greater consistency in description of the cause and impact of the problems as well as the recommended fixes. However, their use does incur a substantial licensing cost.

While Nessus and Cerberus include some testing f or database vulnerabilities, significant additional benefit can be obtained from examining the database using a dedicated database scanning tool. The ISS Database Scanner is probably the most advanced in this area, and will identify a wide range of datab ase configuration vulnerabilities.

4 hours

7. The final stage is to bring the results of all of the previous phases together and analyse and document the results, identify and describe and vulnerabilities and recommend any improvements. The amount of effort required at this stage depends largely on the results of the previous stages. Allow around 10 hours.

Total engagement estimate: 32 -35 hours = $8000.

2. Assessment Implementation

This section will only focus on items 2 and 3 of the above list, as the oth ers are really dependent on the application environment.

2. The initial perimeter assessment will validate that the actual infrastructure in production corresponds to what has been designed. An nmap scan from the Internet (ie from the Internet side of the b order router will be used to identify open ports).

```
C:\> Nmapnt -sS 99.99.99.1-30

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org ( www.insecure.org/nmap/ )


All 65535 scanned ports on  (99.99.99.1) are: filtered
All 65535 scanned ports on  (99.99.99.2) are: filtered
Interesting ports on  (99.99.99.3):
(The 65533 ports scanned but not shown below are in state: filtered)
Port       State       Service
80/tcp     open        http
443/tcp    open        https

Interesting ports on  (99.99.99.4):
(The 65534 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp

All 65535 scanned ports on  (99.99.99.5) are: filtered
All 65535 scanned ports on  (99.99.99.6) are: filtered
All 65535 scanned ports on  (99.99.99.7) are: filtered
All 65535 scanned ports on  (99.99.99.8) are: filtered
All 65535 scanned ports on  (99.99.99.9) are: filtered
Interesting ports on  (99.99.99.10):
(The 65534 ports scanned but not shown below are in state: filtered)
Port       State       Service
443/tcp    open        https

All 65535 scanned ports on  (99.99.99.11) are: filtered
All 65535 scanned ports on  (99.99.99.12) are: filtered
All 65535 scanned ports on  (99.99.99.13) are: filtered
All 65535 scanned ports on  (99.99.99.14) are: filtered
All 65535 scanned ports on  (99.99.99.15) are: filtered
All 65535 scanned ports on  (99.99.99.16) are: filtered
```

```
All 65535 scanned ports on  (99.99.99.17) are: filtered
All 65535 scanned ports on  (99.99.99.18) are: filtered
All 65535 scanned ports on  (99.99.99.19) are: filtered
All 65535 scanned ports on  (99.99.99.20) are: filtered
All 65535 scanned ports on  (99.99.99.21) are: filtered
All 65535 scanned ports on  (99.99.99.22) are: filtered
All 65535 scanned ports on  (99.99.99.23) are: filtered
All 65535 scanned ports on  (99.99.99.24) are: filtered
All 65535 scanned ports on  (99.99.99.25) are: filtered
All 65535 scanned ports on  (99.99.99.26) are: filtered
All 65535 scanned ports on  (99.99.99.27) are: filtered
All 65535 scanned ports on  (99.99.99.28) are: filtered
All 65535 scanned ports on  (99.99.99.29) are: filtered
All 65535 scanned ports on  (99.99.99.30) are: filtered

Nmap run completed -- 30 IP addresses scanned in 10204 seconds
```

3. In this phase we verify the behaviour of the key security devices. Again nmap provides a useful tool for scanning the devices. As an example we will describe the testing for the e -commerce front end firewall – although the same bas ic methodology would be used to validate the other firewalls.

   To begin we need to obtain access to the network outside the firewall, either by using a spare port on the border router, or by temporarily installing a hub or switch between the border router a nd firewall. Similarly access to the webLAN is also required for a PC running tcpdump or WinDump.

   We begin by testing the required connectivity – in this case by telneting or directing a browser to port 443 on the web server. The browser will prompt for a client digital certificate indicating that the connection was successful.

   This interaction will generate traffic similar to that shown below in the WinDump output, indicating that the firewall allowed the connection through (and that our test set -up is working).

```
...
21:35:17.417184 99.99.99.37.3177 > commerce.giac.com.443: S 2648095133:2648095133(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
21:35:17.498431 commerce.giac.com.443 > 99.99.99.37.3177: S 2260748142:2260748142(0) ack
2648095134 win 33580 <mss 1460> (DF)
21:35:17.498579 99.99.99.37.3177 > commerce.giac.com.443: . ack 1 win 17520 (DF)
21:35:17.499774 99.99.99.37.3177 > commerce.giac.com.443: P 1:107(106) ack 1 win 17520 (DF)
21:35:17.519485 commerce.giac.com.443 > 99.99.99.37.3177: . ack 107 win 33580 (DF)
21:35:17.523388 commerce.giac.com.443 > 99.99.99.37.3177: . 1:1461(1460) ack 107 win 33580
(DF)
21:35:17.524263 commerce.giac.com.443 > 99.99.99.37.3177: P 1461:2494(1033) ack 107 win 33580
(DF)
21:35:17.524351 99.99.99.37.3177 > commerce.giac.com.443: . ack 2494 win 17520 (DF)
21:35:17.547651 99.99.99.37.3177 > commerce.giac.com.443: P 107:311(204) ack 2494 win 17520
(DF)
21:35:17.616364 commerce.giac.com.443 > 99.99.99.37.3177: . ack 311 win 33580 (DF)
21:35:17.899538 commerce.giac.com.443 > 99.99.99.37.3177: P 2494:2500(6) ack 311 win 33580
(DF)
21:35:17.899695 commerce.giac.com.443 > 99.99.99.37.3177: P 2500:2561(61) ack 311 win 33580
(DF)
21:35:17.899769 99.99.99.37.3177 > commerce.giac.com.443: . ack 2561 win 17453 (DF)
21:35:17.910937 99.99.99.37.3177 > commerce.giac.com.443: P 311:726(415) ack 2561 win 17453
(DF)
21:35:17.955907 commerce.giac.com.443 > 99.99.99.37.3177: P 2561:2586(25) ack 726 win 33580
(DF)
21:35:17.957514 99.99.99.37.3177 > commerce.giac.com.443: P 726:816(90) ack 2586 win 17428
(DF)
21:35:17.974578 commerce.giac.com.443 > 99.99.99.37.3177: . 2586:4046(1460) ack 816 win 33580
(DF)
21:35:17.975778 commerce.giac.com.443 > 99.99.99.37.3177: P 4046:5506(1460) ack 816 win 33580
(DF)
21:35:17.975938 commerce.giac.com.443 > 99.99.99.37.3177: P 5506:5631(125) ack 816 win 33580
(DF)
21:35:17.976033 99.99.99.37.3177 > commerce.giac.com.443: . ack 5631 win 17520 (DF)
21:35:18.005564 99.99.99.37.3177 > commerce.giac.com.443: P 816:1075(259) ack 5631 win 17520
(DF)
21:35:18.075711 commerce.giac.com.443 > 99.99.99.37.3177: . ack 1075 win 33580 (DF)
```

. . .

Similarly pinging the web server should be successful, with the traffic being visible in the WinDump output:

```
21:46:11.119863 99.99.99.37 > commerce.giac.com: icmp: echo request
21:46:11.160603 commerce.giac.com > 99.99.99.37: icmp: echo reply (DF)
21:46:12.119045 99.99.99.37 > commerce.giac.com: icmp: echo request
21:46:12.138448 commerce.giac.com > 99.99.99.37: icmp: echo reply (DF)
21:46:13.130683 99.99.99.37 > commerce.giac.com: icmp: echo request
21:46:13.166313 commerce.giac.com > 99.99.99.37: icmp: echo reply (DF)
21:46:14.132713 99.99.99.37 > commerce.giac.com: icmp: echo request
21:46:14.156063 commerce.giac.com > 99.99.99.37: icmp: echo reply (DF)
```

We now begin testing the serv ices we believe should be disallowed

```
nmapnt -sU -p1-65535 99.99.99.0/27
nmapnt -sS -p1-65535 99.99.99.0/27
```

Observation of the WinDump logs resulting from these scans would show that only traffic to TCP port 443 of the web server appears on the web server LAN.

3. Perimeter Assessment

Assessment of the e -commerce production environment indicates that the system is well secured against direct attack.

One of the main recommendations would be to reconsider the policy of allowing ICMP echo requests into the GIAC network.

Additional protection against some forms of denial of service attack – in particular SYN floods – could be gained by implementing the TCP intercept functions on the PIX firewall. This is most critical for the front end e-commerce firewa ll.

Another item that has not been explicitly covered previously is the use of warning banners on the border router and firewalls (and for that matter on the servers).

Assignment 4 - Design Under Fire (25 Points)

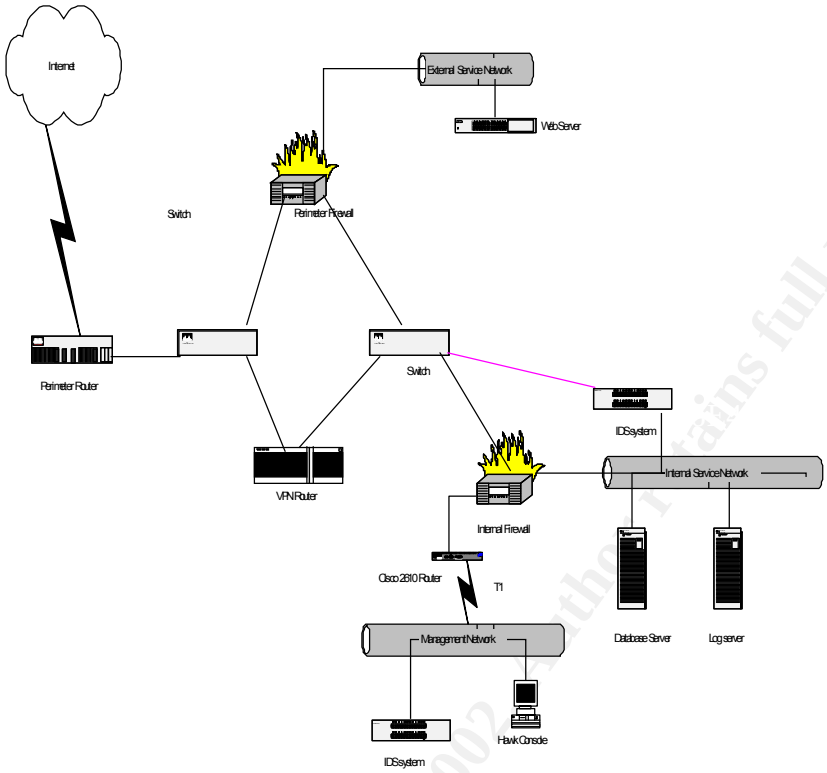
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

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:

1. An attack against the fi rewall 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.
2. A denial of service attack. Subject the design to a theoreti cal 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.
3. 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.

Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand -waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand tha t firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

For this question I will look at the practical assignment submitted by Tamara Bowman (which is available at http://www.sans.org/y2k/practical/Tamara_Bowman_GCFW.doc). The security architecture is shown below:



1. Attack Against Firewall

In general the firewall is probably the most difficult component to attack, so if the goal was gaining access to the fortunes database the most likely path for attack would be via the web server or some other application which requires Internet access.

The two main firewall devices used in this design are a Cisco PIX 525 ver 5.3 (1) and a Raptor 6.4 on Solaris 2.8. Both of these are very up -to-date configurations and so there are no widely reported weaknesses. However, there appears to be anecdotal evidence that there are certain problems with the Cisco PIX with regard to excessive fr agmentation.

(see http://www.nexial.com/cgi -bin/firewallsbodyview?h=3&d=92649&q=fh%5finsertb).

This problem has been acknowledged by Cisco on their web site, alt hough there does not appear to be any fix nor any information about the performance impact.

Hence we will use this as the basis of a denial of service attack against the firewall – noting that by degrading the performance of this device to a sufficient ext ent will impact all network traffic except for the VPN. The attack would involve generating large numbers of heavily fragmented (ie fragmented into 13 or more parts) packets.

Fragrouter (http://www.anzen.com/research/nidsbench/fragrouter.html) can be used to help implement this attack, by configuring it to fragment packets (eg into 8 or 24 byte IP fragments) and forward them to an IP address beyond the firewall.

Another host on the same network as the fragrouter host must be configured to route traffic to the target server via the fragrouter.

Then it is simply a matter of generating packets which are large enough to fragment into more than 12 fragments (ie packets of more than 96 or 288 bytes). Various traffic generators can be used for this, or most simply the ping command could be used (ping –l 300 www.giac.com)

2. Denial of Service Attack

With 50 cable modems (assuming 500 kbps each upstream) at one's disposal, one has a ready made bandwidth of around 25 Mbps available. This is enough to flood many organisation's communications links, without even resorting to any fancy techniques.

An attacker can leverage their available bandwidth in a number of ways:

- Directed broadcasts can be used to amplify traffic volumes. The simplest form of attack is the smurf attack. A ping (ICMP echo-request) to a broadcast address can yield many replies. If the source IP address of such a ping can be forged to correspond to the victim's IP address, the resultant flood of ICMP echo-replies can flood the communications bandwidth of the victim. There are numerous web sites that provide details of the worst offenders with respect to directed broadcast amplification. Currently, these include (http://www.pulltheplug.com/broadcasts2.html):

NETWORK	RESPONSES
63.84.239.255	7239
213.11.125.255	2272
210.240.250.127	1486
167.7.21.64	1184
208.20.112.224	1148
207.102.63.191	758
200.39.219.32	611
207.51.55.159	577
204.113.16.31	462
206.66.134.63	457
194.177.100.127	446
207.252.215.127	406
210.241.236.191	358
216.63.164.191	331
38.167.73.255	320
24.48.37.255	310
207.193.206.64	291
200.215.130.0	280
203.75.25.63	277
193.95.112.63	241

  While these figures drop off, it must be expected that one can easily obtain a 10:1 average amplification of traffic. Hence, with 50 compromised cable modem machines, each capable of generating at least 500 kbps of upstream traffic, the resultant flood of traffic to the victim's IP address could be around 50*500*10 = 250 000 kbps = 2.5 Gbps. This is easily enough to flood the total bandwidth that most organisations have to their Internet Service Provider – and in fact is enough to flood most Internet Service Providers.

  There is no direct defence against such an attack, as it is flooding the communications link coming *into* the devices that you have control over. The only hope is to discover the attack (by observing the high traffic levels through your network and the 100% bandwidth utilisation of your communications links) and to request that your ISP block traffic further upstream (or that their wholesale ISP does the same). Their ability to do this will depend on the location of the compromised cable modem systems and the location of the directed broadcast amplifiers.

- Even without this traffic amplification, 250 Mbps is enough to saturate the raw communications capacity of most organisations. This could be done by directing any manner of traffic at any of the publicly addressable servers. Again, there is no direct defence – other than requesting upstream ISP's detect and block the traffic before it enters your network. Varying the types of traffic, and potentially forging the source IP addresses, will make tracking down and filtering the attack traffic extremely difficult.

- The way to leverage bandwidth is to inject traffic that requires greater resources to process at the victim's side than it does to generate at the attacker's side. This can be done by a variety of ways as we move up the protocol stack:
  - Insert TCP SYNs which cause the server to allocate resources for the expected TCP session. The number of "half open" TCP sessions that many operating systems support is very low, and hence they are unable to respond to legitimate requests to establish a TCP session. Thus a small number (eg around 300 per minute) of TCP SYNs (without corresponding ACKs) is sufficient to fully disable a server.
  - Requesting a transaction that requires server side processing is another way of leveraging bandwidth to create a denial of service attack. Security protocols can be prime subjects of this sort of attack due to the processing overheads associated with cryptographic operations. For example, during the SSL establishment phase [http://home.netscape.com/eng/ssl3/draft302.txt], replaying the initial messages (client hello and client key exchange) with a randomly generated value for the Encrypted Pre Master Secret will cause minimal load on the attacker's machine, but will require the server to perform a computationally expensive private key operation each time.
  - Exploiting bugs in the application code that may cause the server to crash or hang thereby preventing it from servicing other legitimate requests. An example of such a bug is described at http://www.securityfocus.com/bid/2282 and consists of generating GET requests with a large number of "../"'s.

3. Internal System Attack

If we are looking to attack the critical fortune cookie database in this architecture then the easiest approach would be to attack an accessible server which itself would have access to the database contents. The perfect victim is the web server, which by its nature must be accessible to anyone on the Internet. In this instance the Web Server is a Netscape Enterprise server – although the version number is not provided. In this case we will assume that it is Netscape Enterprise server version 3.6.

Looking for exploits against Netscape servers we discover a number of possibilities, including this one: http://xforce.iss.net/alerts/advise39.php . This vulnerability allows an attacker to execute arbitrary code on the web server under the same permissions as the web server process (usually *nobody* on a Unix platform).

Using this vulnerability we can execute commands to upload and execute any utilities we require to further infiltrate the system. For example we could use tftp (or even normal ftp) to load netcat (http://www.l0pht.com/~weld/netcat/readme.html) onto the web server host and run it to listen on port 22, 80 or 443. The Perimeter firewall will allow the outgoing "session" since it is being initiated from a higher security interface to a lower security one. It will also allow the subsequent connection to ports 22,80 or 443 which are used to get a shell on the web server machine, as it has been configured to do so.

At this point we have a Unix shell on the web server host. This web server also has access to the database server, and all the client software and configuration information required to generate SQL requests to the Oracle server (including any account names and passwords needed for authentication). These can be used to browse the fortune database, download the sayings, and overwrite them with "y0r c00ki3 w4z h4cked !!!"