Global Information Assurance Certification Paper

SANS Certification
Level Two Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment

Tim Alton

April 2001

Assignment 1 – Security Architecture

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/acquisition. 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).

Solution

1.1 Business Model

The business model is assumed to be the following:

GIAC Enterprises is a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings.

The enterprise has just completed a merger/acquisition with AFC (Asia Fortune Cookies) which translates the sayings into various Asian languages and resells throughout Asia. AFC consists of marketing and translation departments. AFC did not have an online business before the merger. The online part of the business is owned and operated by GIAC.

GIAC obtains fortune cookie sayings from Suppliers via the Internet. The Suppliers are contracted by GIAC to source the sayings and ensure a defined level of quality. The Suppliers are paid a percentage of the income from the sales to customers. Suppliers are paid via bank transfers. GIAC currently has around 30 suppliers worldwide. Suppliers can submit sayings in English and several Asian languages.

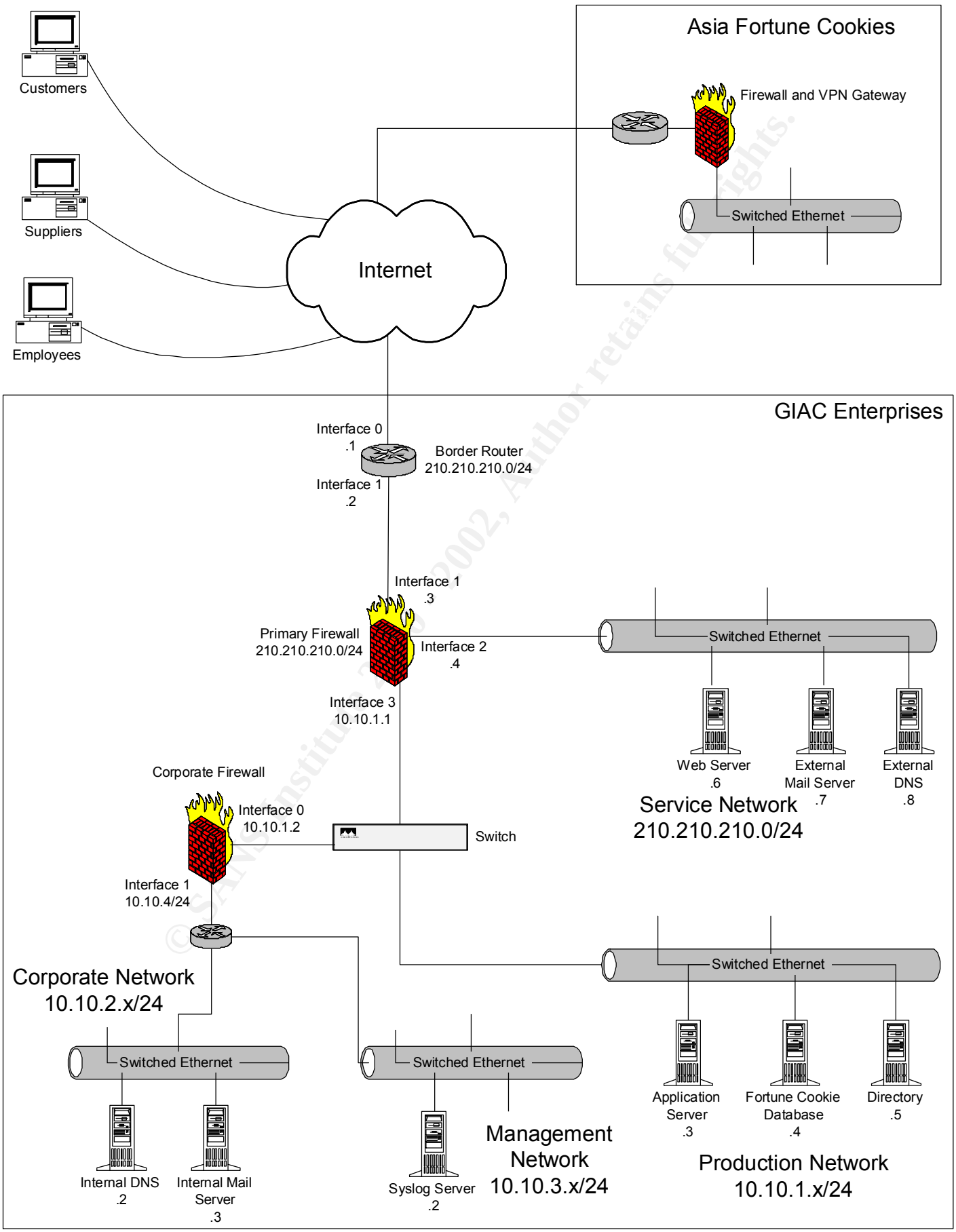
Customers buy the fortune cookie sayings from GIAC in bulk via the Internet. The customers are fortune cookie manufacturers in Australia, Asia, and North America. During registration the customers supply their contact details and credit card numbers, and are issued with authentication credentials. Registration is conducted online, though some background checking is performed to ensure that the customers are legitimate. GIAC currently has around 200 customers worldwide.

The security architecture design is driven by the business requirements. The security related business requirements are assumed to be:

1. Customers must register over the Internet, supplying their contact details and credit card numbers, and be issued with authentication credentials.
2. Customers must authenticate to the web site before being authorised to purchase sayings.
3. Suppliers will be registered offline and be issued with authentication credentials.
4. Suppliers must authenticate to the web site before being authorised to submit sayings.
5. Partners, in this case AFC, must be given access to fortune cookie sayings for translation between various languages.
6. GIAC employees must have secure remote access into the GIAC corporate network.

1.2 Security Architecture

The security architecture is given below.



No redundancy is shown in the network diagram for simplicity. However the primary firewall, service and production networks are duplicated for load sharing purposes.

1.2.1 Authentication

Customers and suppliers are authenticated at the web server with username/password credentials. Strong password management is defined and enforced to minimise the risk of credentials being compromised. The password management policy is given in Appendix A.

Partners, the AFC employees, access the production network using a gateway to gateway VPN over the Internet. A Checkpoint VPN-1 appliance is used at the AFC network and at the GIAC network. No network level authentication is required by the AFC employees only by the gateways. The AFC employees authenticate to the application server on the GIAC production network using username/password credentials. Once authenticated the AFC employees are allowed to access the sayings for translation. The VPN-1 appliances authenticate each other using a shared secret.

The username/password credentials for customers, suppliers, and partners are stored in the directory.

Employees use Checkpoint VPN-1 SecureClient software with 512 bit private keys and Entrust client certificates to authenticate to the primary firewall for remote access.

1.2.2 System Components

Border Router

Make: Cisco
Version: 3640 with IOS version 12.0

The border router performs initial packet filtering. It filters out the traffic that is generally known to be used for attacks or is unnecessary. The security role of the border router is not to prevent these attacks but to reduce the amount of noise hitting the primary firewall.

Primary Firewall

Make: Nokia Appliance
Model: IP330
Software Version: FireWall-1 4.1 build 41821 for IPSO 3.3 (SP3).

Nokia appliance was selected so administrators would not need to be experts in hardening the operating system.

The primary firewall directly protects the service and production networks from attacks from the Internet, and terminates VPN connections (IPSEC) from partners (AFC employees) and GIAC employees.

Corporate Firewall

Make: Nokia Appliance
Model: IP330
Software Version: Firewall-1 4.1 build 41821 for IPSO 3.3 (SP3)

Nokia appliance was selected so administrators would not need to be experts in hardening the operating system.

The corporate firewall protects the corporate network from attacks via compromised hosts on the service or production networks.

The firewall is configured to allow:

- Any traffic from the primary firewall that is from a terminated GIAC employee VPN connection.
- Management traffic from the corporate network to the service and production networks.
- HTTP and HTTPS traffic initiated from the corporate network to the Internet.

AFC Firewall

Make: Nokia Appliance
Model: IP330
Software Version: Firewall-1 4.1 build 41716 for IPSO 3.3

The AFC firewall protects the AFC network and sets up an IPSec session with the GIAC Primary firewall to allow AFC employees connectivity to the GIAC production network.

ServiceNetwork

The service network consists of the external DNS, a mail relay server, and the company's Internet facing web server. The customers and suppliers access the fortune cookie application via the web server.

Customers and suppliers set up server side authenticated SSL sessions with the web server and then provide their username/password credentials for authentication.

The web server, DNS server, and mail server all run on Microsoft 2000 Server (SP1) operating system, that has been hardened according to industry best practices.

The web server is running IIS 5.0 with Active Server Pages for user login sessions and talking DCOM back to the Application Server.

Production Network

The production network consists of the application server, fortune cookie database server, and directory. The application server contains the business logic for the fortune cookie application. In particular the application server contains the authorisation rules that determine what functions customers and suppliers can perform. The database stores the fortune cookie sayings, and the directory stores user profiles for the customers and suppliers. The user profile includes a username, password, a credit card number for customers, and bank account details for suppliers.

The application server, database, and directory run on Microsoft 2000 Server (SP1) operating system, that has been hardened according to industry best practices. The database is Microsoft SQL Server. The directory is Microsoft Active Directory. The application server is a Microsoft Transaction Server.

Corporate Network

The corporate network is used by employees for general workgroup communications, such as email, schedules, intranet web site, etc. Access to the corporate network is protected by the corporate firewall.

AFC Network

The AFC employees use a Microsoft VB application that connects to the GIAC application server using DCOM over VPN connection.

Appendix A Password Management

1. Password authentication exchanges over the Internet must be protected with 128 bit server side authenticated SSL sessions.
2. Passwords must have at least 8 characters and no more than 20 characters.
3. Passwords may comprise of any printable characters. They must include at least one letter and one number. Passwords are case sensitive.
4. Passwords expire every 3 months and must be changed. A password history is kept to prevent users from choosing passwords that they previously used.
5. After 3 incorrect login attempts the users accounts are locked for 1 hour.
6. If a user forgets their password then they must contact the telephone helpdesk.
7. Passwords are stored in the directory in a hashed form.

Assignment 2 – Security Policy

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 ACLs, 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 implement 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 protocol 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".

Solution

2.1 Border Router

Make: Cisco
Version: 3640 with IOS version 12.1

The border router is configured to explicitly deny traffic that is unnecessary or generally used for malicious purposes. All other traffic is permitted. This philosophy was chosen so that the filter rules would remain static and hence easy to manage.

Anti-spoofing filtering is applied for both ingress(into GIAC) and egress(out of GIAC) traffic.

The border router has two interfaces: interface0(to primary firewall); interface1(to Internet).

2.1.1 Global Configurations

- Deny source routed packets.

```
no ip source-route
```

- Deny any management from interface 0
- Permit management only from corporate network (10.10.2.x/24) via interface 1

```
access-list 10 permit ip 10.10.2.0 0.0.0.255
     line vty 0 4
     access-class 10
     login
```

- Disable finger service
  `no service finger`
- Enable secret. Use the enable secret command to set the administrator password for the router. This command hashes the password using MD5 which is stronger than the Vigenere cipher used with the enable password command.
- A warning banner with the appropriate legal information in configured using the banner login command.
- Logging information is sent to the syslog server on the corporate network.
- To prevent Smurf denial of service attack, the no ip directed-broadcast command is used. This is set by default on IOS 12.0 and later.

2.1.2 Interface0

Configuration is:

```
Interface Serial 0
     ip address 210.210.210.1 255.255.255.0
     ip access-group 101 in
```

NB the following access list must be implemented in the order given:

- Anti spoofing: Deny any packets originating from outside GIAC with a source IP address that is private or from the internal GIAC network.

```
access-list 101 deny ip 0.0.0.0 0.255.255.255
access-list 101 deny ip 10.0.0.0 0.255.255.255
access-list 101 deny ip 127.0.0.0 0.255.255.255
access-list 101 deny ip 172.16.0.0 0.15.255.255
access-list 101 deny ip 192.168.0.0 0.0.255.255
access-list 101 deny ip 224.0.0.0 31.255.255.255
access-list 101 deny ip 224.0.0.0 31.255.255.255
access-list 101 deny ip 210.210.210.0 0.0.0.255
```

- Deny login services: telnet(23/tcp), SSH(22/tcp), FTP(21/tcp), NetBIOS(139/tcp), rlogin(512/tcp to 514/tcp)

```
access-list 101 deny tcp any any range ftp telnet log
access-list 101 deny tcp any any eq 139 log
access-list 101 deny tcp any any range 512 514 log
```

- Deny RPC and NFS: Portmap/rpcbind(111/tcp and 111/udp), NFS(2049/tcp and 2049/udp), lockd(4045/tcp and 4045/udp)

```
access-list 101 deny tcp any any eq 111 log
access-list 101 deny udp any any eq 111 log
access-list 101 deny tcp any any eq 2049 log
access-list 101 deny udp any any eq 2049 log
access-list 101 deny tcp any any eq 4045 log
access-list 101 deny udp any any eq 4045 log
```

- Deny NetBIOS in Windows NT/2000: 135(tcp and udp), 137(udp), 138(udp), 139(udp), 445(tcp and udp)

```
access-list 101 deny tcp any any eq 135 log
access-list 101 deny udp any any eq 135 log
access-list 101 deny udp any any eq 137 log
access-list 101 deny udp any any eq 138 log
access-list 101 deny udp any any eq 139 log
access-list 101 deny tcp any any eq 445 log
access-list 101 deny udp any any eq 445 log
```

- Deny X windows: 6000/tcp through 6255/tcp

```
access-list 101 deny tcp any any range 6000 6255 log
```

- Deny naming services: DNS zone transfers(53/tcp), LDAP 389(tcp and udp). **Note** that the border router will allow DNS(53/udp) through; the firewall will enforce that only the external DNS server will receive these requests. This is done so that the border router does not need to be changed if the IP address of the external DNS server changes.

```
access-list 101 deny tcp any any eq 53 log
access-list 101 deny tcp any any eq 389 log
access-list 101 deny udp any any eq 389 log
```

- Deny mail: POP(109/tcp and 110/tcp), IMAP (143/tcp). Note that the border router will allow SMTP (25/tcp) through; the firewall will enforce that only the external mail server will receive these requests.

```
access-list 101 deny tcp any any eq 109 log
access-list 101 deny tcp any any eq 110 log
access-list 101 deny tcp any any eq 143 log
```

- Deny "Small services": Ports below 20/tcp and 20/udp, time(37/udp and 37/tcp)

```
access-list 101 deny tcp any any lt 20 log
access-list 101 deny udp any any lt 20 log
access-list 101 deny tcp any any lt 37 log
access-list 101 deny udp any any lt 37 log
```

- Deny miscellaneous: TFTP(69/udp), finger(79/tcp), NNTP(119/tcp), NTP(123/tcp), LPD(515/tcp), syslog(514/udp), SNMP(161/tcp and 161/udp, 162/tcp and 162/udp), BGP(179/tcp), SOCKS(1080/tcp)

```
access-list 101 deny udp any any eq 69 log
access-list 101 deny tcp any any eq 79 log
access-list 101 deny tcp any any eq 199 log
access-list 101 deny tcp any any eq 123 log
access-list 101 deny tcp any any eq 515 log
access-list 101 deny udp any any eq 514 log
access-list 101 deny tcp any any eq 161 log
access-list 101 deny udp any any eq 161 log
access-list 101 deny tcp any any eq 162 log
access-list 101 deny udp any any eq 162 log
access-list 101 deny tcp any any eq 179 log
access-list 101 deny tcp any any eq 1080 log
```

- ICMP: Deny incoming echo request(type 8), re-directs (type 5),

```
access-list 101 deny icmp any any echo log
access-list 101 deny icmp any any 5 log
```

- Permit all other packets.

```
access-list 101 permit any any
```

2.1.3 Interface1

Configuration is:

```
Interface Serial 1
     ip address 210.210.210.2 255.255.255.0
     ip access-group 102 in
```

Management is allowed from this interface.

- ICMP: Block outgoing echo replies(type 0), time exceeded(type 11), and destination unreachable messages except for "packet too big" messages (type 3, code 4).

```
access-list 102 permit icmp any any 3 4 log
access-list 102 deny icmp any any 3 log
access-list 102 deny icmp any any 11 log
access-list 102 deny icmp any any 0 log
```

- Egress filtering: Permit any packets originating from inside GIAC with a source IP address from the internal network.

```
access-list 102 permit ip 210.210.210.0 255.255.255.0
any log
```

References: Cisco Site: Manuals on router configuration.

2.2 Primary Firewall

Make: Nokia Appliance
Model: IP330
Software Version: Firewall-1 4.1 build 41716 for IPSO 3.3

Anti-spoofing: The interfaces are configured to detect IP spoofing. Any spoofed packets are dropped and logged.

Interface	Valid Addresses
1	Other

2	This net (210.210.210.0)
3	Specific – corporate (10.10.2.0/24), management (10.10.3.0/24), production networks (10.10.1.0/24)

The explicit rule base is configured as follows:

- Stealth rule prevents users from connecting to the firewall.
- Accept access from the Internet or the corporate network to the service network for web, mail, and DNS traffic.
- Accept DCOM from the web server on the service network to the application server on the production network.
- Accept management traffic from the management network in the corporate network into the service network.
- Accept Syslog traffic from the border router to the syslog server on the management network.
- Accept zone transfers from the internal DNS to the external DNS.
- Accept DNS queries from the external DNS to the Internet.
- Accept HTTP/HTTPS from the corporate and management networks to the Internet. This allows employees to surf the web.
- Accept SMTP from the external mail server to the Internet.
- Cleanup rule: Drop all other packets and log

The FW-1 policy editor entries are as follows:

No	Source	Destination	Service	Action	Track	Install On	Time
1	Any	Firewall_local	Any	drop	long	Primary FW	Any
2	Any	web server	http	accept		Primary FW	Any
3	Any	web server	https	accept		Primary FW	Any
4	Any	external mail server	smtp	accept		Primary FW	Any
5	Any	external DNS	domain-udp	accept		Primary FW	Any
6	web server	application server	DCOM	accept		Primary FW	Any
7	management network	service network	any	accept		Primary FW	Any
8	border router	syslog server	Syslog(UDP)	accept		Primary FW	Any
9	internal DNS	external DNS	domain-tcp	accept		Primary FW	Any
10	external DNS	Internet	domain-udp	accept		Primary FW	Any
11	corporate network	Any	http	accept		Primary FW	Any
12	corporate network	Any	https	accept		Primary FW	Any
13	management	Any	http	accept		Primary FW	Any

	network						
14	management network	Any	https	accept		Primary FW	Any
15	external mail server	Internet	smtp	accept		Primary FW	Any
16	Any	Any	Any	drop	long	Primary FW	Any

Reference: Checkpoint Firewall-1 Manual: VPN-1/Firewall-1 Administration Guide

2.3 VPN access for Remote GIAC Employees

The GIAC employees use Checkpoint SecureClient (4.1 build 4176 SP3) software to set up secure connections to the Primary firewall over the Internet.

The Primary firewall has Checkpoint VPN-1 installed.

IKE encryption is used. FWZ was not chosen because it is proprietary. The IKE properties for the users are:

- Authentication scheme: public key
- Encryption transform: ESP is used since confidentiality is required.
- Data integrity: SHA1
- Encryption algorithm: strong (3DES)

Remote employees are authenticated using 512 bit private keys and Entrust certificates.

Remote employees are dynamically allocated IP addresses from a pool of private addresses. This pool is known to the corporate firewall to allow this traffic into the corporate and management networks.

The primary firewall is configured to allow:

- Traffic from the terminated VPN sessions from remote GIAC employees to the corporate and management networks.

The Corporate firewall is configured to allow:

- Traffic from remote GIAC employee VPN sessions into the corporate and management networks.

Reference: Checkpoint Firewall-1 Manual: Virtual Private Networks

2.4 VPN Access for AFC Employees

The AFC firewall and the GIAC primary firewall set up an IPSec session.

IKE encryption is used. The IKE properties for the users are:

- Authentication scheme: pre-shared secret
- Encryption transform: ESP since confidentiality is required.
- Data integrity: SHA1
- Encryption algorithm: strong (3DES)

The AFC employees that require access to the GIAC application server are on a dedicated subnet. Traffic from this subnet is permitted, by the AFC firewall, to enter the IPSec connection to the GIAC primary firewall. The GIAC primary firewall is configured so that traffic from the AFC IPSec connection is allowed to access any server on the production network.

The primary firewall is configured to allow:

- Traffic from the terminated VPN sessions from AFC firewall to the production network.

Reference: Checkpoint Firewall-1 Manual: Virtual Private Networks

Assignment 3 – Audit Your Security Architecture

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.

Solution

3.1 Audit Plan

The aim of the audit to verify that:

1. The security policy on the primary firewall is implemented as specified in the assignments 1 and 2.
2. Logging and alerting are working correctly.
3. Determine what, if any, vulnerabilities exist in the network when viewed from the perimeter.

The general approach of an audit is to work through the various layers that defend the network, verifying that each layer performs its intended function. The layers include the border router, the primary firewall, the corporate firewall, the servers on the service network, and the servers on the production network. This assignment deals with the auditing of the primary firewall only.

An external security consultant will conduct the audit. The system administrators who built the system will not conduct the audit since they may make the same assumptions or have the same biases that were used to build the system. Furthermore it is unrealistic to expect that the system administrators will also be security experts.

Timing

Network scanning tools can potentially bring down systems. Hence it is important to conduct the tests when the network is not heavily used. However, the timing of the audit is complicated by the fact that the network is used consistently over 24 hrs since the customers, partners, and suppliers are distributed worldwide. So there are few windows of low activity. The network is built with full redundancy so there are two primary firewalls. Thus the approach taken is to direct all the traffic to one of the primary firewalls while the other is being scanned, and vice versa.

Cost

Required personnel: One security consultant with expertise in checkpoint firewall-1, network scanners, and network security principles.

Number of hours: 2 days.

Risks and Considerations

There are no risks that the system will be unavailable to users during the scans due to the redundant design of the network.

The firewall needs to be scanned from all three interfaces to check to completely check the implemented security policy.

Audit Steps

1. Obtain the security policy that the primary firewall is required to enforce. This step is critical for the audit to be successful. Without the security policy requirements it is impossible for a consultant to verify that the firewall is correctly implemented.
2. Obtain the network architecture.
3. Inspect the configuration of the primary firewall to check for any obvious problems. The configuration should be compared to "best practices" for firewall-1.
4. Using Nmap scan the primary firewall from all three interfaces. Nmap is being used to determine what is allowed through the firewall. Interface 1 is the most important since it is directly accessible from the Internet. Interface 2 is the second most important since it will limit the scope of attack from a compromised server on the service network. Finally interface 3 will limit scope of attack from any internal servers to the service network or other servers on the Internet.

   For Interface 1: The scan will be conducted on the IP addresses of the primary firewall, the corporate network, the management network, the servers on the service network, and the servers on the production network.
   IP addresses to be scanned:
   - Primary firewall interfaces: 210.210.210.3 ; 210.210.210.4 ; 10.10.1.1
   - Servers on the service network: 210.210.210.6 ; 210.210.210.7 ; 210.210.210.8
   - Corporate Network: 10.10.2.0/24

- Management Network: 10.10.3.0/24
- Servers on the production network: 10.10.1.3 ; 10.10.1.4 ; 10.10.1.5

For Interface 2: The scan will be conducted on the IP addresses of the primary firewall, the corporate network, the management network, and the servers on the production network.
IP addresses to be scanned:

- Primary firewall interfaces: 210.210.210.3 ; 210.210.210.4 ; 10.10.1.1
- Corporate Network: 10.10.2.0/24
- Management Network: 10.10.3.0/24
- Servers on the production network: 10.10.1.3 ; 10.10.1.4 ; 10.10.1.5

For Interface 3: The scan will be conducted on the IP addresses of the primary firewall, and the servers on the service network.
IP addresses to be scanned:

- Primary firewall interfaces: 210.210.210.3 ; 210.210.210.4 ; 10.10.1.1
- Servers on the service network: 210.210.210.6 ; 210.210.210.7 ; 210.210.210.8

5. Interpret the results of the scans to determine what, if any, vulnerabilities are present.

3.2 Audit Implementation

The firewall configuration was inspected and verified with the design documentation. Furthermore the configuration was checked for compliance with "best practices" and was found to be satisfactory.

3.2.1 Scanner Configuration

The Nmap scanner, version 2.53 for Windows NT from eEye Digital Security, was used with the following configuration.

Nmap options
-sS -- Check for TCP ports using TCP SYN scan. Quicker than doing a full TCP connect() scan.
-sU -- Check for UDP ports.
-P0 -- Don't do a ping since it will be blocked by the primary firewall.
-ologfile -- write human readable log to "logfile"

Ports scanned: 1 to 1024 and any other ports specified in the nmap services file.

3.2.2 Results

Interface 1

Primary firewall interfaces: All packets to these addresses were dropped by the primary firewall with no response.
Servers on the service network: The required ports on these servers were found to be open. Packets addressed to other ports were dropped by the primary firewall with no response.
Corporate Network: All packets to these addresses were dropped by the primary firewall with no response.
Management Network: All packets to these addresses were dropped by the primary firewall with no response.
Servers on the production network: All packets to these addresses were dropped by the primary firewall with no response.

Interface 2

Primary firewall interfaces: All packets to these addresses were dropped by the primary firewall with no response.
Corporate Network: All packets to these addresses were dropped by the primary firewall with no response.
Management Network: All packets to these addresses were dropped by the primary firewall with no response.
Servers on the production network: DCOM packets from the web server to the application server were permitted. All other packets were dropped with no response.

Interface 3

Primary firewall interfaces: All packets to these addresses were dropped by the primary firewall with no response, except for authenticated management traffic.
Servers on the service network: Packets with source addresses from the management network were allowed through on any port. Packets with other source addresses were only allowed through to ports http(80)/https(443) on the web server, port smtp(25) on the external mail server, and port dns(53) on the external DNS server.

3.3 Perimeter Analysis

No major security issues were discovered during the audit. However it is recommended that the following enhancements be made to the primary firewall.

1) Configure SYNDefender in gateway mode. This will reduce the effectiveness of any SYN flood attacks.

Assignment 4 – Design Under Fire

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:

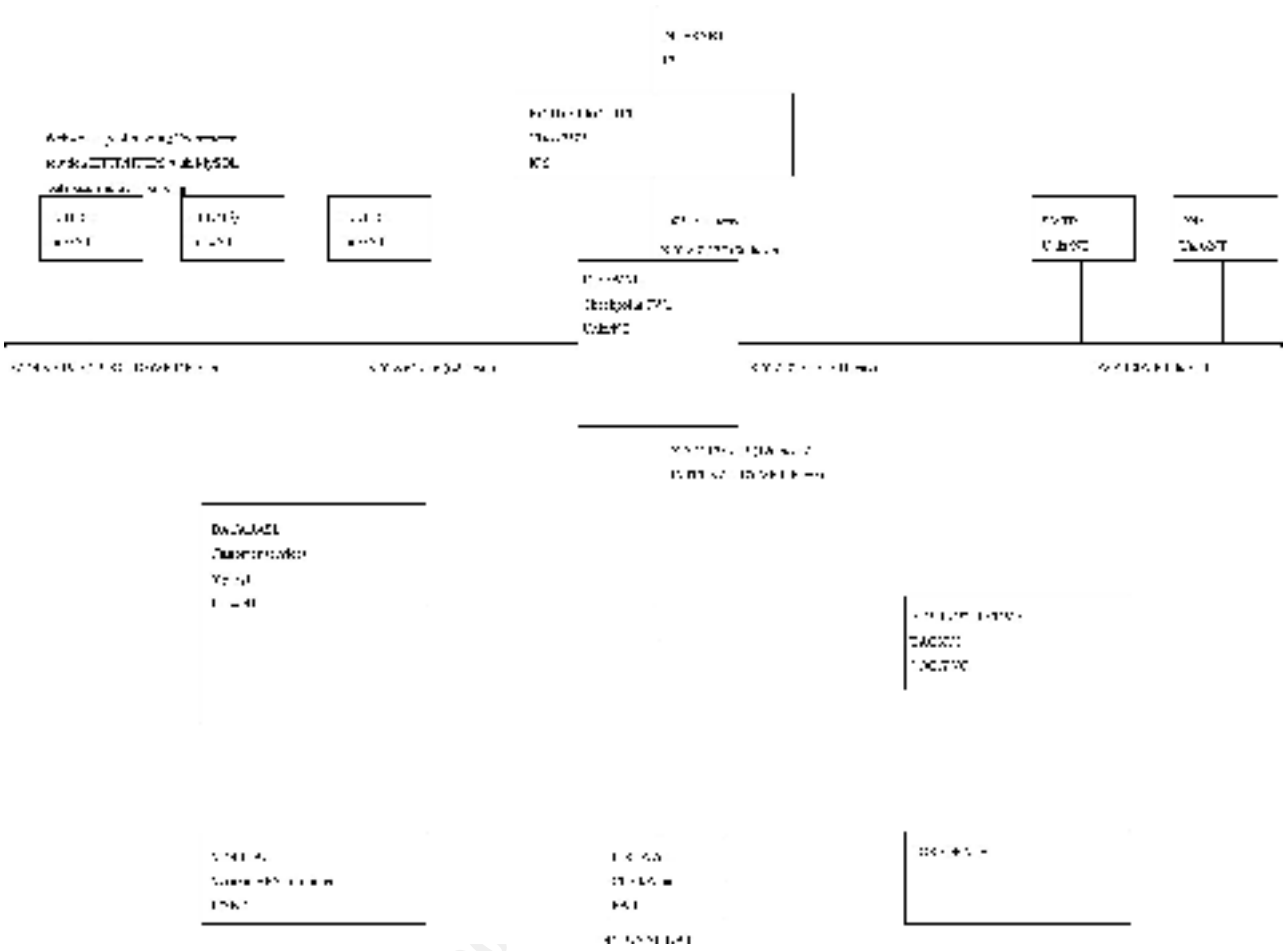
1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 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.
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 that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

Solution

The design that is under attack is by Vincent Berk
http://www.sans.org/y2k/practical/Vince_Berk_GCFW.zip

The network architecture is shown below.



4.1 Firewall Attack

Since the version of Checkpoint Firewall-1 is not specified in the design I will assume the following:

- Version 4.0 is being used.
- S/Key is used to authenticate connections from a management module.

The attack involves tricking the firewall into believing that the connection is from a legitimate management module, using a brute force method of finding the S/Key authentication secret, and then issuing a command to load a policy which allows all access.

The steps in the attack are:

1) Determine the IP address of the management module. The inter-module authentication protocol doesn't verify the source IP address by looking at the IP packets. Instead it believes the IP address that is handed to it. Hence there is no need for the attacker to spoof the IP address of the management module. The protocol is

asynchronous so it is possible to wait until the firewall sends a list of allowable IP addresses before sending back an IP address that the firewall wants to see.
2) Run a brute force attack to determine what the S/Key secret is. The program can be obtained from the reference below.
3) Login to the firewall as the management module and load a policy which allows all traffic.

The result of this attack is to remove any filtering performed by the firewall and leave the rest of the network exposed to the attacker.

Reference: The BlackHat 2000 Conference. http://www.phoneboy.com/docs/bh2000/

4.2 Denial of Service Attack

The aim of this attack is to deny legitimate users access to the web servers in the above architecture.

The attack used is the Tribe Flood Network attack. The 50 compromised cable modem/DSL systems are loaded with the TFN daemon software. The attacker uses another host as the TFN master to launch the attack.

The attack is initiated by the TFN master sending an ICMP echo reply to the daemons with the IP addresses of the web servers to flood and an instruction to use a SYN flood. Each daemon then launches the SYN flood attack on the web servers.

A SYN flood attack consists of the attacking machine sending a SYN to the target machine with an unreachable source address; The target machine allocates some resources for the half open TCP connection, replies with a SYN/ACK to the unreachable source address, and waits for a reply until is receives one or times out. The target machine never receives a reply so the half open connection is maintained by the target until it times out. The target machine can only support a limited number of half open connections at any one time; Once the limit is reached any subsequent SYN requests are discarded. Hence if the attacker sends enough SYN requests then the target machine will not be able to service legitimate requests and service is denied.

Countermeasures to mitigate this attack include:

- Configure the border router or firewall to not accept packets from illegal source IP addresses.
- Internet service providers should implement egress filtering to discard packets outbound from their networks that do not have source IP addresses from their network.
- Firewall-1 has the SYNDefender module that can handle a larger number of SYN requests than a host.
- The number of allowable half-open TCP connections can be increased on the hosts. Though this is only useful if the attack is on a small scale.

References:

SANS Course Notes

4.3 Internal System Attack

The attack is being launched by a group of hackers enlisted by an unscrupulous competitor to the E-commerce company. The aim of the attack is to undermine the confidence that customers have in the security of the E-commerce company and hence divert business to the competitors.

The attack involves the hackers exploiting a software bug in the web server and loading their own web page on the front page of the server. This page will warn the potential customers that they are accessing a site that has been hacked and any personal data they submit to the site including credit card numbers will be published onto the Internet.

This attack demonstrates that implementing a firewall does not secure the system from end to end and at all levels. It is still possible to exploit any application level bugs in the systems that are accessible through the firewall, such as in the web servers and application servers.

For the purposes of this attack I am assuming the following:

- Allaire Cold Fusion version 4.0 is being used
- The sample application, Expression Evaluator, hasn't been removed from the build.
- It hasn't been patched for this attack.

The assumed environment allows an attacker to read files, upload files to the server, and execute files. Hence it is possible for an attacker to replace the main web page.

The attack involves the following steps:

1. Determine that Cold Fusion is being used. This could be from a combination of things including cfm file extensions in the URLs (using view source on the browser will show many of these), or by inspecting the cookies that are returned and noting the presence of "CF" in their names.
2. Send the following URL to the server http://<server name>>/cfdocs/expeval/openfile.cfm where *server name* is the hostname of the server. You will be asked to select a file from the local machine to upload to the server, for example choose dummy.txt.
3. The server uses ExprCalc to evaluate the file and then delete it. It responds with http://<<servername>>/cfdocs/expeval/exprcalc.cfm?RequestTimeout=2000&OpenFilePath=C:\Inetpub\wwwroot\cfdocs\expeval\.\dummy.txt

4. By replacing dummy.txt with exprcalc.cfm, and submitting the URL, it is possible to have exprcalc delete itself. Then further files can be uploaded without them being deleted.
5. Then upload a new main page for the server, index.html, with the desired content.

References:

http://www.sans.org/infosecFAQ/threats/coldfusion.htm
http://www.wwdsi.com/demo/advisories/cfusion.txt
http://www.allaire.com/handlers/index.cfm?ID=8727&Method=full