Global Information Assurance Certification Paper

Practical Assignment
For
GIAC Firewall and Perimeter Protection
Capitol SANS, Washington DC
December 10 -15, 2000

Prepared
By
Said Nurhussein

Introduction

This practical assignment is for GIAC Level Two Firewalls, Perimeter protection, and VPNs Capitol SANS, December 10 - 15, 2000.

The practical consists of four parts:

Part-1: Defines the security architecture with diagrams and explanatory text, perimeter technologies to implement the security architecture and access for customers, partners
and suppliers.

Part-2: Based on the security architecture defined in part-1, provides security policy for Border Router, Primary Firewall and VPN.

Part-3: Audits security Architecture and policy described in parts 1 and 2.

Part-4: An exercise in enhancing and improving Parts 1 thru 3 by designing attacks against architecture from previously submitted practical.

Business Background

GIAC Enterprises is a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. As a requirement of its core business, GIAC systems must interact with customers, suppliers, partners and some remote users.

Objective

The objective of this report is to provide GIAC Enterprises an e-business architecture, security policy, auditing framework and enhancement & maintenance plan. The report will also emphasize a network security architecture that is robust yet flexible enough to allow GIAC Enterprises conduct a smooth e-business operation.

Assignment 1

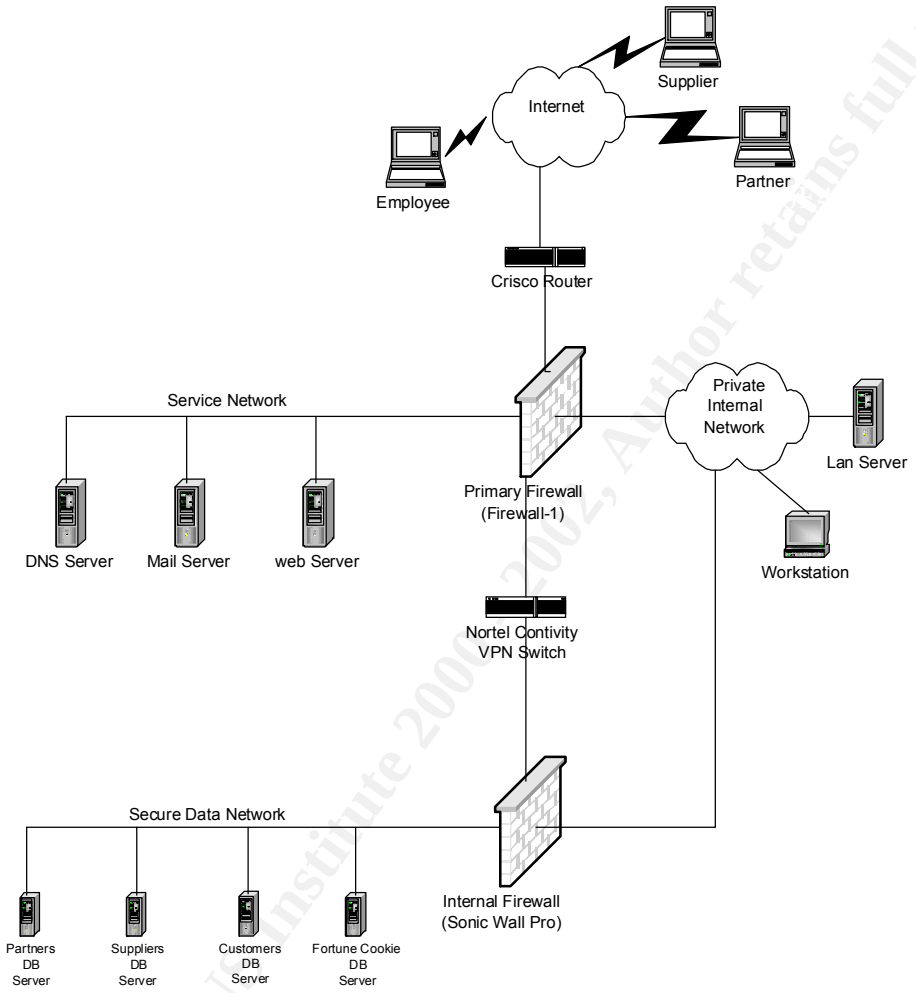
Define security architecture for GIAC Enterprises, a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. Produce a diagram or set of diagrams with explanatory text that define how to use Perimeter technologies to implement your security architecture.

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).

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.

GIAC Network Security Architecture
Diagram 1
Proposed Architecture



Overview of Security Architecture

The security architecture proposed on the previous page takes into consideration the following GIAC Enterprises business requirements, policies and principles:

- GIAC Enterprises networks must be secured as much as possible with available funds, time and staff.
- GIAC must have a secure interaction with its suppliers and partners so that it's business is not disrupted or maliciously attacked.
- Since GIAC conducts its business solely online, the protection of both its data as well as its customers' data is very critical. Therefore, all data accessed online should be encrypted.
- Secure each layer of TCP/IP stack and each component of the security architecture.
- Firewalls and routers must be hardened by restricting access to their operating system, encrypting passwords and defining appropriate filters.
- All users must have an ID and a strong password.
- All servers must implement host-based security and must be configured to only serve what they are intended to serve, e.g. a Web server should only have http(s) turned on nothing else no mail, database or any other application.
- By default, deny everything unless it's explicitly allowed.
- Log all significant network events.
- Be a good Internet neighbor: never be a conduit for hacker traffic, implement Ingress and Egress filters on routers, scan e-mail for viruses.
- As an online business, GIAC will eventually have a high profile web site and brand recognition, which may make it more vulnerable to various kinds security threats.
- Access must be defined for customers, suppliers, partners and some remote users.

The security architecture consists of the following **perimeter defense** technologies:

Border Router - Cisco 3600 IOS 11.0

The border router will be used as a gateway to the Internet. Its primary function is to route packets to their appropriate destinations. It will also be used to implement base security policy via Egress, Ingress, and other filters to complement the primary firewall.

Primary Firewall (Firewall-1)

The primary firewall is a hardened Windows NT server with Firewall-1 version 4.1 (SP3) software. This firewall will enforce most of GIAC Enterprises' network security policy.

VPN Device (Nortel Contivity)

The Nortel Contivity VPN switch (model 1520) will be configured to allow suppliers, partners and employees to access GIAC databases via a secure VPN tunnel using IPsec protocols.

Secondary Firewall (Sonic-Wall Pro version 5.1.1)

In addition to the primary firewall, the critical data network will be separated from the rest of GIAC internal network via a secondary firewall that complements and further implements the multi-layer approach to network security.

Access Definitions

Customers: direct access via a single SSL enabled web site will be provided for customers to use for purchasing fortune cookie sayings.

Suppliers: are allowed to connect (via VPN Switch) to suppliers' database server on the secure network in order to supply GIAC fortune cookie sayings.

Partners: are granted access to the partners' database server on the secure network -- to download fortune cookie saying and resell them.

Employees: Authorized employees may access the secure network via the VPN switch.

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, filters, 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".

PART 2 --- Security Policy

2.1 Security Policy

The security architecture defined in Part 1 will enforce the following general GIAC Enterprises IT Security Policy:

- Internet traffic shall only interact with the service network.
- GIAC networks shall not be used as a conduit for any other third party traffic.
- All customer personal information and transaction data shall be encrypted.
- Every GIAC Enterprises network user shall have an ID and a strong password. GIAC internal networks shall be available only to authenticated and authorized users and hosts
- Contractors and consultants shall access GIAC Enterprise IT resources after acquiring permission form the Security Officer
- All GIAC IT users must be informed and trained about security issues and sign any legal clauses that may be in effect.
- GIAC employees may not use internal IT resources to access controversial or inappropriate (illegal) web sites
- Services such as NetBios, Napster, IRC, rlogin, RCP will not be coming into or going outside of GIAC network
- Virus scanning shall be performed on all inbound and outbound e-mail.

2.2 Border Router ACLs

The border router will implement SANS' recommended top ten rules as its Base Policy.

The following ACLs and implement the IT security architecture defined in part 2.1:

1. Implement an 'Ingress Filter' (block spoofed addresses) – packets coming form outside GIAC Enterprises, internal hosts, reserved addresses and null host.

Description
This ACL will help protect GIAC networks from DDoS attacks by dropping any inbound packets that have spoofed, private, loop back, null and reserved IP addresses As the source IP address. This filter should be applied on all routers.

Syntax

```
Interface Serial 0
        Ip address nnn.121.1.1  255.255.255.D
        Ip  access-group 10 in

access-list 10 deny nnn.121.0.0  0.0.255.255
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 deny 127.0.0.0 0.255.255.255
access-list 10 deny 172.16.0.0 0.15.255.255
access-list 10 deny 192.168.0.0 0.0.255.255
access-list 10 deny 224.0.0.0 31.255.255.255
access-list 10 deny host 0.0.0.0
access-list 10 permit any
```

2. Implement an 'Egress Filter' to block any spoofed addresses from leaving GIAC Enterprises network.

Description
The purpose for this ACL is to protect GIAC networks from being used as a source for DDoS attacks. If any packet leaving GIAC's has a source address that does not belong to GIAC's Internal network, it was most likely spoofed.

Syntax
Interface Ethernet 0
Ip address nnn.121.1.1 255.255.255.0
Ip access-group 10 in

access-list 10 permit nnn.121.1.0 .255.255.255
access-list 10 deny any any log input

3. Block login services such as telnet and ftp from coming into GIAC Enterprises' networks

Description
Login services such as telnet and ftp are security risks because they send login/session transaction over the network in clear text. Therefore, it's recommended that they be disabled. The use of SSH is recommended in lieu of these login services.

Syntax
access-list 114 deny tcp any any range ftp telnet exec log

Gotcha!
GIAC Enterprises is expected to interact with various organizations to conduct its business. Because SSH and other secure remote technologies are not widely used yet (compared to telnet & ftp), the above filter may create problems if an employee, consultant or partner has a need to telnet/ftp to a particular host to work on some project. If that's the case, the above filter can be modified to the following:

Access-list 114 permit tcp <remote-client> <selected-host> telnet log
access-list 114 deny tcp any any range ftp telnet exec log

4. Block sunrpc and NFS services

Description
Remote Procedure Calls (RPC) is a client/server process that is used by applications that need to send small request from a client to a server. RPC uses a port mapper that dynamically assigns service ports upon startup,so this can be tricky to control. Because of this issue, it is recommended that inbound and outbound RPC be blocked at the router.
NFS is a protocol that enables access to files on a remote system. Because NFS has weak authentication (allows clients to access remote files based on their IP address only), it is recommended that inbound and outbound traffic (port 2049 – tcp & udp) be blocked.

Syntax
access-list 114 deny tcp any any eq sunrpc log
access-list 114 deny udp any any eq sunrpc log
access-list 114 deny tcp any any range nfs lockd log
access-list 114 deny tcp any any 2049 log
access-list 114 deny udp any any 2049 log
access-list 114 deny tcp any any 4045 log
access-list 114 deny udp any any 4045 log

5. NetBios in Windows NT must be blocked from crossing the border router because it can allow global file sharing over the Internet.

Description
NetBios is a high risk Windows protocol that uses several ports to enable services to communicate with each other. NetBios establishes internal networks resources 'shares' with default access permission 'everyone, full control' and broadcasts available resources in plain text . For these reasons, it's recommended that NetBios ports be blocked.

Syntax
access-list 114 deny tcp any any 135 log
access-list 114 deny udp any any 135 log
access-list 114 deny udp any any 135 138 log
access-list 114 deny tcp any any 139 log
access-list 114 deny tcp any any 445 log
access-list 114 deny udp any any 445 log

6. X-windows servers pose a major security hole if not configured properly.

Description
X-Windows is a client/server based GUI system for UNIX hosts.
Any system listed in the trusted host list of an X-Windows server can connect
to the client list. An intruder can capture client screen content, read keyboard strokes
as username/password are typed or control applications on a client system.

Syntax
access-list 114 deny tcp any any range 6000 6255 log

7. Naming services (DNS) ports to all GIAC machines which are not DNS servers must be blocked and allow zone transfers only from external secondaries.

Description
DNS systems are seldom the first main system targeted hackers. Therefore,
It's prudent to block UDP port 53 and TCP port 53 to traffic to all hosts
That are not DNS servers or trusted secondary DNS servers.

Syntax
access-list 114 allow tcp <authorized-secondary> <dns-server> 53 log
access-list 114 allow udp any <dns-server> 53 log
access-list 114 deny tcp any any 53 log
access-list 114 deny udp any any 53 log

8. **Mail to all machines which are not external mail relays, POP (109/tcpd) and 110/tcp IMAP (143/tcp) must be blocked**

Description
SMTP uses TCP port 25 to handle e-mail transmission between mail servers.
It sends clear text traffic over the network with header info being accessible
to anyone who sniffs the network. It is recommended that only the mail server
open this port.

Syntax

access-list 114 allow tcp any <mail-server> 25 log
access-list 114 allow tcp any any 109 log
access-list 114 allow tcp any any 110 log
access-list 114 allow tcp any any 143 log

9. Allow web traffic from the Internet should only get directed to external web servers.

Description
HTTP using TCP port 80 (8000,8888,8080) can expose internal web servers to several type of malicious attacks. To avoid the atttacks, allow http or https traffic from the Internet to be directed only to the external web server.

Syntax
access-list 114 allow tcp any <web-server> 80 log
access-list 114 allow tcp any <web-server> 443 log
access-list 114 deny tcp any any 80 log
access-list 114 deny tcp any any 8000 log
access-list 114 deny tcp any any 8080 log
access-list 114 deny tcp any any 8888 log

10. Block small services

Description

TCP and UDP services such as Echo, Discard, Chargen and Daytime are rarely used and may be the target of potential exploit by create hacker. It is generally recommended that these services are disabled and their ports blocked.

Syntax

access list 114 deny tcp any any range 0 20 log
access-list 114 deny udp any any range 0 20 log
access-list 114 deny tcp any any 37 log
access-list 114 deny udp any any 37 log

11. Block miscellaneous services such as tftp, nntp, ntp, finger and snmp

Description
The miscellaneous services listed below should be blocked because they grant access to resources without authentication, and also give a potential hacker a valuable reconnaissance information about your network.

Syntax

access-list 114 udp any any 69 log
access-list 114 udp any any range 161 162 log
access-list 114 tcp any any 79 log
access-list 114 tcp any any 119 log
access-list 114 tcp any any 123 log
access-list 114 tcp any any range 161 162 log
access-list 114 tcp any any 179 log
access-list 114 tcp any any 515 log
access-list 114 tcp any any 1080 log

12. Armor the router

a) Limit which hosts or networks can connect to the router

```
access-list 17 permit nnn.121.1.0 0.0.0.255
line vty 0 4
acces-class 17
login
```

e.g. nnn.121.1.0 = internal network

b) Disable snmp

Unless there's critical need, it's recommended to disable SNMP.

```
no snmp
```

c) Disable source routing

Loose source routing will be disabled so that hackers won't be able to program their packets to go to certain route thereby using GIAC networks as a pass thru.

```
no ip source-route
```

d) Encrypt password

Because Cisco router's passwords are typically stored in the configuration file in plain text, it's wise to encrypt passwords by the command below:

service password encryption.

e. Disable miscellaneous services

Some services such as echo, chargen discard, daytime may be disabled to prevent some undiscovered vulnerabilites from being used against the router.

no service tcp-small-servers
no service udp-small-servers
no service finger
no ip http

f. Limit ICMP

Prevent layer 3 to 2 layer broadcast mapping and smurf attacks
no ip direct-broadcast
no ip unreachables

g. Define a Warning Banner on all incoming remotely accessible links:
Banner /
Warning: Authorized Access Only.
/

h. Log significant events and console messages

Use the UNIX syslog to log the border router's events to a central syslogd server.
e.g.
logging nnn.121.1.99
logging trap debug
logging console emergencies

2.3 Primary Firewall Rules

In addition to the base policy (SANS top ten rules) outlined in section 2.2, GIAC Enterprises Primary Firewall (Firewall-1) will implement the following policies.

The format of Firewall-1 rule base is as follows:

Source
Destination
Service (port)
Action (accept, deny, reject, drop, authenticate, etc)
Track (long, short, alert, etc.)

Policy: Lock down the Firewall

Description

In order for the primary firewall to secure GIAC networks, we must first secure the firewall itself. Most Firewalls consist of software that's installed On an UNIX, Linux or Windows based host. In this design the Firewall-1 will be Installed on a Windows machine; therefore, we'll make sure that the Windows/NT machine is hardened (latest patches, unnecessary services turned off, etc); and then we will deny traffic from any where to the firewall.

Filter

Source	Destination	Service	Action	Track
Any	Firewall	Any	Drop	Long

Gotcha!

This rule may be very restrictive because it will make the firewall inaccessible to everyone, including the Firewall Administrator. It also doesn't allow for the firewall to Drop noisy protocols such as NBT/IDENT without consuming processing power and log space.

So the filter needs to be modified to:

Source	Destination	Service	Action	Track
FW-Admin-host	Firewall	Firewall-1	Accept	Long
Any	Firewall	NBT/IDENT	Reject	
Any	Firewall	Any	Drop	Long

Note: Ordering is critical here; the FW-Admin and reject noisy protocols must be placed before the lockdown.

Policy: Allow traffic from the Mail Server to Internal Network

Description
The primary firewall must allow SMTP traffic to pass thru from the service network to the internal network so GIAC employees can send and receive e-mail from the Internet.

Filter

Source	Destination	Service	Action	Track
Mail-server	Internal-network	SMTP	Accept	Long

Policy: Allow traffic from the DNS Server to Internal Network

Description
In order for GIAC Enterprises employees to query the DNS server for hostname And IP lookup queries on the DNS server, the firewall must allow UDP port 53 to pass thru from service network to Internal network.

Filter

Source	Destination	Service	Action	Track
DNS-server	Internal-network	Domain/UDP	Accept	Long

Policy: Allow traffic from Internal Network to Web Servers

Description
Internal users also need to access GIAC Enterprises web servers. The primary firewall will allow HTTP traffic to pass thru from the Internal network to web servers. on the service network.

Filter

Source	Destination	Service	Action	Track
Internal-network	Web-servers	HTTP	Accept	Long

Policy: Allow traffic from Internal Network to Mail Server

Description
Internal users also need to access GIAC Enterprises Mail servers to retrieve e-mail Messages. The primary firewall will allow SMTP and POP3 traffic to pass thru from the internal network to mail server on the service network.

Filter

Source	Destination	Service	Action	Track
Internal-network	Mail-server	SMTP/POP3	Accept	Long

Policy: Don't Allow any other (non http or mail) traffic from Internal Network to the Service Network.

Description
Internal users should not be allowed to connect to servers that are on the service Network . All they need is access to the web server and access to the mail server (granted on the previous filters). Any other traffic from Internal to Service networks must be denied.

Filter

Source	Destination	Service	Action	Track
Internal-network	Service-network	Any	Drop	Long

Policy: Internal users should be allowed full outbound access.

Description
Internal users should be allowed to full outbound access – i.e. they can connect To any host or visit any web site outside the GIAC Enterprises network (Internet).

Filter

Source	Destination	Service	Action	Track
Internal-network	Any	Any	Accept	Long

Gotcha!
The above filter is very permissive, in that some employees may visit inappropriate, controversial or bandwidth hog web sites. It may also put GIAC Enterprises in legal problems or degrade its networks' performance.

A possilble solution to the problem might be to identify the most notorious (bad) sites and Create object groups for them and them block outbound traffic to those sites.
e.g.
create an object group called 'Napster' with a list of the web site IP addresses; and another object group called 'Inappropriate' with a list of the most known 'bad' web sites' domain/IP and then modify the previous filter to:

Filter

Source	Destination	Service	Action	Track
Internal-network	Napster	Any	Drop	Long
Internal-network	Inappropriate	Any	Drop	Long
Internal-network	Any	Any	Accept	Long

Policy: Grant outside users access to GIAC web servers and Mail server

Description
This policy is very critical to GIAC Enterprises business. The primary firewall must be correctly configured to allow GIAC customers to browse fortune cookie sayings on the web and also communicate via e-mail.

Filter

Source	Destination	Service	Action	Track
Any	Web-server	HTTP/HTTPS	Accept	Long
Any	Mail-server	SMTP	Accept	Long

Policy: Grant outside users access to GIAC web server, Mail server and DNS Server.

Description

This policy is also very critical to GIAC Enterprises business. The primary firewall must be correctly configured to allow GIAC customers to lookup the web site, purchase fortune cookie sayings on online and communicate via e-mail.

Filter

Source	Destination	Service	Action	Track
Any	DNS-Server	Domain/UDP	Accept	Long
Any	Web-server	HTTP/HTTPS	Accept	Long
Any	Mail-server	SMTP	Accept	Long

Policy: Don't originate traffic from service network.

Description
This policy is needed so that GIAC Enterprises Web, Mail or DNS servers are not used by a hacker as stepping stone to attack the internal, secure or any other network on the Internet.

Filter

Source	Destination	Service	Action	Track
Service-Network	Any	Any	Drop	Alert

Policy: Allow VPN traffic to and from the VPN switch.

Description
This policy will grant GIAC Enterprises suppliers, partners and employees access to selected database servers from remote locations.

Filter

Source	Destination	Service	Action	Track
Any	VPN-Switch	IKE, AH, ESP, IPsec	Accept	Long
VPN-Switch	Any	IPsec, IKE, AH, ESP	Accept	Long

Policy: Deny everything else.

Description
This policy will deny any traffic that is not explicitly allowed (in preceding filters) and logs any attempts.

Filter

Source	Destination	Service	Action	Track
Any	Any	Any	Drop	Long

2.4 Secondary Firewall

The secondary firewall will be used to separate the critical data (secure) network from the rest of GIAC Enterprises network.

The Sonic Wall Pro Firewall will have the following rule in the form of:

Action (allow, deny)
Service
Source
Destination
Time
Day

1. Allow SSH connections from the internal to the secure network.

Filter:

Action	Service	Source	Destination
Allow	SSH	LAN	Secure-network

2. Allow VPN traffic from and to secure network.

Filter:

Action	Service	Source	Destination
Allow	IKE	VPN-switch	Secure-network
Allow	AH	VPN-switch	Secure-network
Allow	ESP	VPN-switch	Secure-network
Allow	IKE	Secure-network	VPN-switch
Allow	AH	Secure-network	VPN-switch
Allow	ESP	Secure-network	VPN-switch

3. Allow SSL & database specific traffic between Web servers and secure network.

Filter:

Action	Service	Source	Destination
Allow	HTTP/HTTPS	Web server	Secure-network
Allow	SQL query	Web server	Secure-network
Allow	HTTP/HTTPS	Secure-network	Web server
Allow	SQL query	Secure-network	Web server

4. Deny everything else.

Filter:

Action	Service	Source	Destination
Deny	Default	* (Any)	Secure-network

2.5 VPN Device

A VPN is a network that is constructed by using the Internet to connect two nodes. It uses encryption and/or authentication mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted along the way. IPsec is the most widely used protocol on VPN devices and it is a collection of protocols: IKE, AH and ESP.

During the Internet Key Exchange (IKE) process, two VPN nodes may agree on Authentication Header (AH) protocol or Encapsulating Security Protocol (ESP). AH protects data transmission by data origin authentication, connectionless integrity and protection against replay attacks; the data payload, however, is not encrypted. ESP protects data transmission by: payload encryption, data origin authentication, data protection against replay attacks, connectionless integrity and limited traffic flow confidentiality.

In the proposed GIAC Enterprises security architecture, the Nortel Contivity VPN Switch has two network interfaces: the un-trusted interface is connected to the primary firewall and the trusted interface is connected to the secure network.

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 Border Router and 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 Border Router and Primary Firewall are 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.

3.1 Plan the Assessment

The first item of the plan should be to schedule an 'Assessment Meeting' with GIAC Enterprises IT manager, network administrators, system administrators and any other third parties (ISP, Partners' IT staff) that may be affected by the assessment.

Prior to conducting the security audit, complete the following tasks:

- Make sure you obtain a signed contract that grants permission to perform the audit and describes the extent of the audit and identifies resources for the scope of the work.The contract is a very critical element of the audit process, because it's your legal protection against any problems that may arise during the audit.
- In order to understand GIAC IT resources and their business value, review the security policy in detail.
- Obtain any available manuals and network diagrams.
- Provide an estimate on the time and cost of the assessment; and the type of report you'll deliver.
- Present a project plan highlighting tasks to be performed. Try to to perform the audit during quiet and busy times so you can get a realistic picture of GIAC network traffic patterns.
- Compile a contact person list of all network/system administrators involved (in case the any system goes down during the assessment).

3.2 Pre-Assessment Research

The purpose of the audit is to find out whether the Border Router and the Primary Firewall are enforcing the security policy outlined in Assignment 2.

The assessment will be implemented in three phases:

a. Information gathering
b. Searching for targets
c. Identifying vulnerabilities

a. Information Gathering

First, we will gather as much information as possible about GIAC Enterprises from publicly available sources such as Securities and Exchange Commission (SEC), company web site, business directories, whois databases. The types of information we gather could be identifying key GIAC executives and employees along with their their address , phone numbers and e-mail addresses. The information we gather here could be used for social engineering purposes.

b. Searching Targets

In this phase, we will use a variety of tools to gather information about GIAC Enterprises IT architecture components. Some of the useful information that can be gathered here are the types machines, operating systems, routers, firewalls, software, and IP addresses/hostnames being used on GIAC networks.

The following tools can be used in this phase:

Telent/netcat: To grab banner and find out things like organization name, machine types and operating system versions.

nslookup/dig/sam *spade*: To get information about the DNS server(type of host, OS version, Bind version, etc.) – if zone transfer attempt succeds, you can get all the hostname/IP of all the machine the DNS server administers.

nmap: This very important/useful tool can be used to scan a network to determine what services are running on each host.

traceroute: This utility can be used to gather information about the various hops that a packet takes from source to destination - it is useful to identify intervening routers and firewalls, and assists in creating a logical map of the network

c. Identifying Vulnerabilities

After gathering organizational (managers/employee names, phone#, e-mail, etc.) information and IT architecture components, we are ready to make educated guesses and implement attacks that are likely to succeed. Publicly available vulnerabilities list from CERT, vendor security alerts and Bugtraq will be used to identify vulnerable systems.

3.3 Implementing the Assessment

Every component of the security architecture (routers, firewalls, hosts, users, servers, services, etc) could become the weakest link and present a potential point of entry into GIAC Enterprises Network.

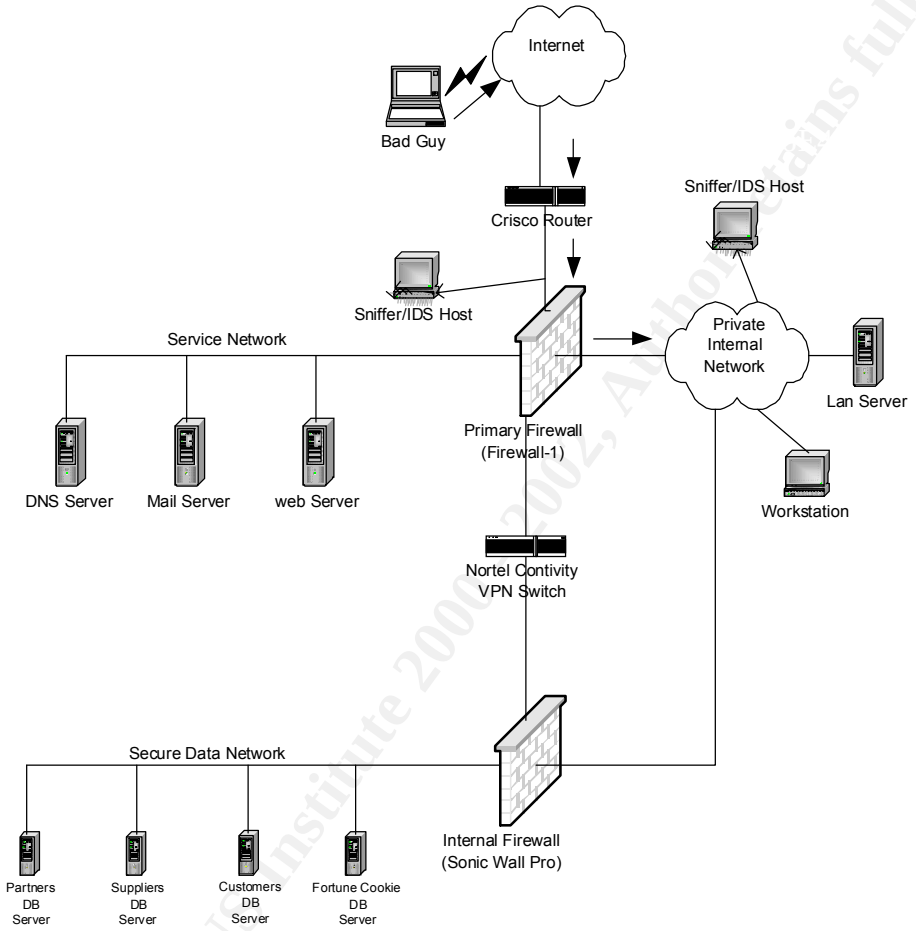
First, we'll examine if the border router actually implements the security policy listed in Assignment 2. To test this, we use a machine that targets the GIAC router from outside the GIAC networks and attempts to send packets that violate the policies listed and would place another Sniffer/IDS machine between the router and the firewall that would sniff traffic that passes thru the router that should not have. The Sniffer/IDS along with syslogd logs should help determine how effective the router was in implementing the security policy.

To check if the router is enforcing outbound specific rules, a host from inside GIAC network would target a host outside GIAC network with allowed and disallowed packets and the Sniffer/IDS would capture the results.

Second, we'll check if the primary firewall is actually enforcing the filters were defined to implement the security policy. To do this, we would place a Sniffer/IDS host on the internal network and sniff for packets that passed thru the primary firewall that should not have. To confirm if the firewall is enforcing outbound specific rules, we would attempt to connect to an outside host with packets that follow the security policy and packets that break the policy and then check the Sniffer/IDS host logs.

(See a diagram showing placement of IDS host on the next page)

GIAC Network Security Architecture
Diagram 2
Placement of Sniffer/IDS Host



3.4 Perimeter Analysis

During the course of this assessment no major security vulnerabilities were found. However, I noticed that the internal firewall before the secure data network is a packet filtering appliance firewall. This firewall may not be robust for the kinds of database applications that might run between the web server and the actual databases. If a hacker breaks into the web server, he/she could send legitimate looking packets with poisonous code from the web servers thru the secondary firewall and then compromise or damage the databases.

To fix this potential weakness, I recommend that the secondary firewall be upgraded to a firewall that can perform stateful inspection or an application proxy server be placed somewhere before the secure data network.

Other recommendations that would help GIAC Enterprises maintain a secure Network are:

1) Make sure the latest vendor patches have been installed on GIAC Enterprises hardware and software systems (routers, firewalls, hosts, applications, etc.)

2) Require that all network and system administrators subscribe to vendor patch alert and Internet security discussion/alert mailing lists (CERT, SANS, Bugtraq).

3) The IT staff must monitor systems very diligently – review logs daily, install tools that generate log reports and alert administrators.

4) Backup all systems regularly and have a contingency recovery plan.

5) Train IT staff in the latest security technologies.

6) Conduct seminars for end-users about security policy and procedures; Request end-users to sign a form indicating acknowledgment of the provided training and security policy.

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:

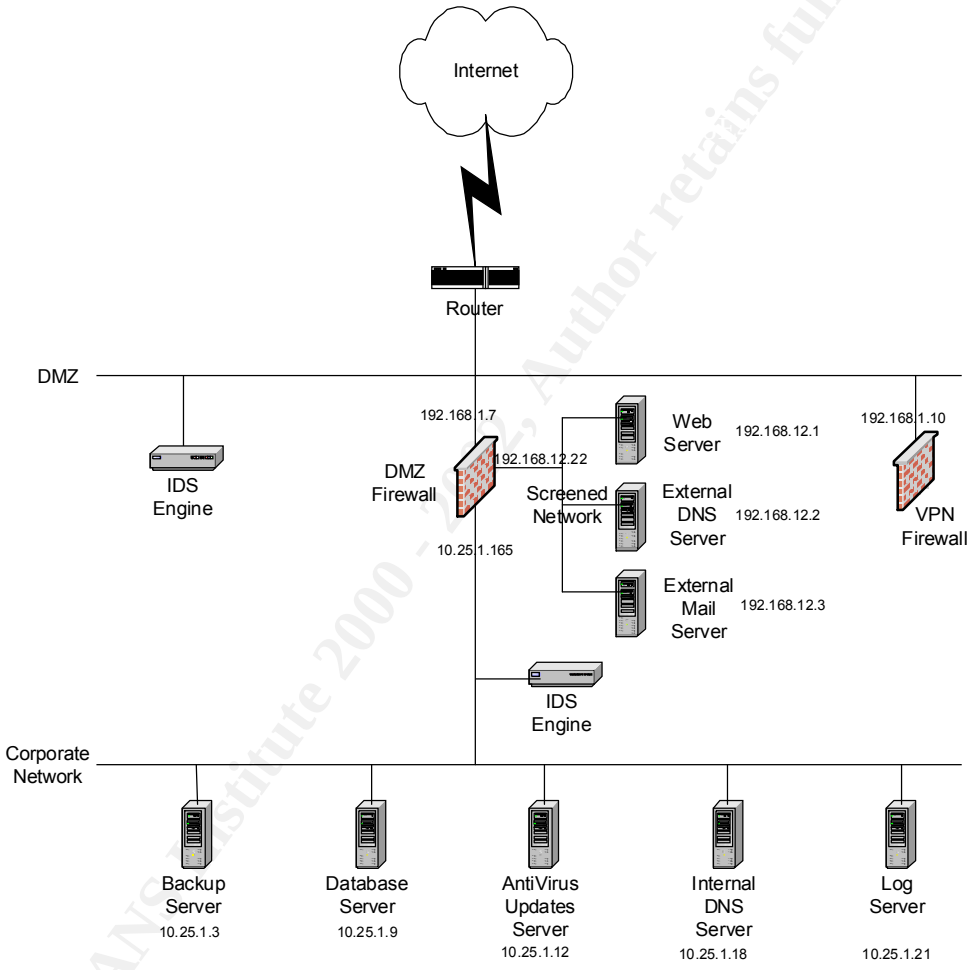
1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.

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.

For assignment 4, I chose **Janice Southerland's** network security architecture design from SANS NS2000 Monterey practicals, which can be found on:
http://www.sans.org/y2k/practical/janice_southerland_GCFW.doc

Here is the security architecture diagram



GIAC Enterprises
Nework Diagram

4.1 Attack against the Firewall

Janice in her security components overview describes the use of Firewall-1 version 4.1 as the primary firewall. After researching this software for any vulnerabilities, I found out that version 4.1 has a known bug (Bugtraq id: 2238)

Vulnerability
The license manager of Firewall-1 version 4.1 software package could allow a Denial of Service. The problem occurs when the internal interface receives a large number of packets that are source routed and containing fictitious (even valid) addresses. In a system containing a license with a limited number of protected addresses, the license manager calculates the address space protected by counting the number of address crossing the internal interface. When the large numbers of packets cross the internal interface, each IP address is added to the number calculated under license coverage. When the number of covered IP addresses is exceeded, an error message is generated on the console for each IP address outside of the covered range. With each error message generated , the load on the firewall system CPU increases. This makes it possible for a malicious user to make a firewall system inaccessible from the console by sending a large number of IP addresses to the internal interface.

Attack
To exploit this vulnerability, fragment based attack tools such as jolt2 can be used to construct incomplete or illegal fragments and attack the firewall.
The malicious packets need not be addressed to the firewall; all the hacker needs to do is route the packets to a host behind the firewall and crash the firewall while it is performing as a pass thru.

Because FW-1 does not inspect nor log fragmented packets until the packet has first been reassembled, these malicious fragment packets cannot be detected by the firewall's rule base.

Solution
Check Point has verified that a malicious internal user can cause high CPU utilization on the firewall using the described attack. This will not cause any valid connections to be blocked or invalid connections to be allowed, but it will cause high CPU utilization and may impact performance. An immediate workaround is available for this issue; at the command prompt, type the following command:

```
fw ctl debug -buf
```

This will prevent the high CPU utilization by blocking console error message logging. This issue will be addressed in an upcoming service pack.

4.2 Denial of Service Attack

The 50 compromised cable modem hosts will have a combined bandwidth equivalent to about 28 T1 lines. A hacker using these compromised systems can easily generate bandwidth starvation type of DoS attacks against any large network. He/she can also run client program on the compromised systems to generates packets using spoofed addresses and then use GIAC Enterprises network as Broadcast Amplification site or send TCP, SYN, UDP, ICMP flood packets to cause a DoS attack.

To mitigate this potential DoS attack, the following countermeasures can be implemented:

- Define and Egress filter on the router to stop spoofed IP packets from leaving your network. This filter reduces the possibility of your internal network from being used as a source of DoS attack against a third party network.

- Configure your routers and firewalls to forward IP packets that only have source IP address from your assigned IP address range.

- Make sure that your network cannot be used as Broadcast Amplification to flood other networks with DoS attacks.

- Ensure that your NAT device only translates addresses authorized for your internal address space.

See Assignment 2 for more detailed ACLs and firewall rules that can be applied to mitigate DoS attacks.

4.3 Attack plan to compromise internal network

My attack plan would be to first use the well-known network probing tools such as nmap and try to collect as much information as possible about the network architecture.

Janice Southerland's network architecture includes a dedicated backup server. I would attempt to attack this server because it probably is not hardened and in order to run backups it may have established some form of trust relationship with other servers. Assuming that the backup software package being is used one from vendors such as Veritas, Sun, Legato and Computer Associates, it is easy to find a backup software vulnerability that can be used to attack the backup server.

A quick search on Bugtraq reveals the following vulnerablities related to the most widely used backup software packages:

2001-01-19: Windows 2000 EFS Temporary File Retrieval Vulnerability
2001-01-15: Veritas Backup Denial of Service Vulnerability
2000-11-03: RedHat Linux restore Insecure Environment Variables Vulnerability
2000-11-01: Microsoft Network Monitor Multiple Buffer Overflow Vulnerabilities
2000-08-28: Microsoft Windows 2000 Local Security Policy Corruption Vulnerability
2000-08-02: NAI Net Tools PKI Server Directory Traversal Vulnerability
2000-07-31: Computer Associates ARCserveIT ClientAgent Temporary File Vulnerability
2000-06-22: Wu-Ftpd Remote Format String Stack Overwrite Vulnerability
2000-06-14: Solaris ufsrestore Buffer Overflow Vulnerability
2000-06-05: Microsoft Windows NT 4.0 PDC/BDC Synchonization Reused Keystream Vulnerability
2000-06-05: BRU BRUEXECLOG Environment Variable Vulnerability
2000-05-16: Netopia DSL Router Vulnerability
2000-05-03: Cisco Router Online Help Vulnerability
2000-02-28: Multiple Vendor "dump" Buffer Overflow Vulnerability
2000-01-04: Allaire ColdFusion 4.0x CFCACHE Vulnerability
1999-11-01: Multiple Vendor Amanda 'runtar' permissions Vulnerabilities
1999-11-01: Multiple Vendor Amanda 'amandad' Symlink Vulnerability
1999-09-26: Arkiea Backup rnavc & nlserverd HOME Environment Variable Buffer Overflow Vulnerability
1999-09-26: Arkiea Backup nlserverd Remote Denial of Service Vulnerability
1999-07-25: Microsoft Windows 2000 EFS Vulnerability
1999-05-06: Oracle 8 File Access Vulnerabilities
1999-04-29: Oracle 8 oratclsh Suid Vulnerability
1998-10-21: Solaris Tape Device Permissions Vulnerability
1998-04-29: Solaris ufsrestore Vulnerability
1996-12-04: AIX login(1) Vulnerability
1992-04-10: IRIX lp Vulnerability

So if I break into the backup server, I have a higher of chance of attacking the database server and compromising/damaging critical business information.

References

Web sites

http://www.sans.org

http://www.cert.org

http://www.securityfocus.com/

http://www.enteract.com/~lspitz/papers.html

Books

1. TCP/IP Illustrated, Volume I: The protocols. Addison Wesley, Reading, Mass.,1994

2. Hacking Exposed, Stuart McClure, Joel Scambray, George Kurtz,
Osborn/McGraw Hill, 1999

Tools

Network Mapper: http://www.insecure.org/nmap

Internet Scanner: http://www.iss.net

Nessus http://www.nessus.org

PhoneSweep: http://www.sandstorm.net

Arin database: http://www.arin.net/whois

---------- end-of-practical ----------