Global Information Assurance Certification Paper

GIAC Enterprises

Attempting to Achieve Defense in Depth

Author: **Brad Sanford**
Date: **10/14/2001**
Track: **GCFW**
Version: **1.6 Revised 8/13**

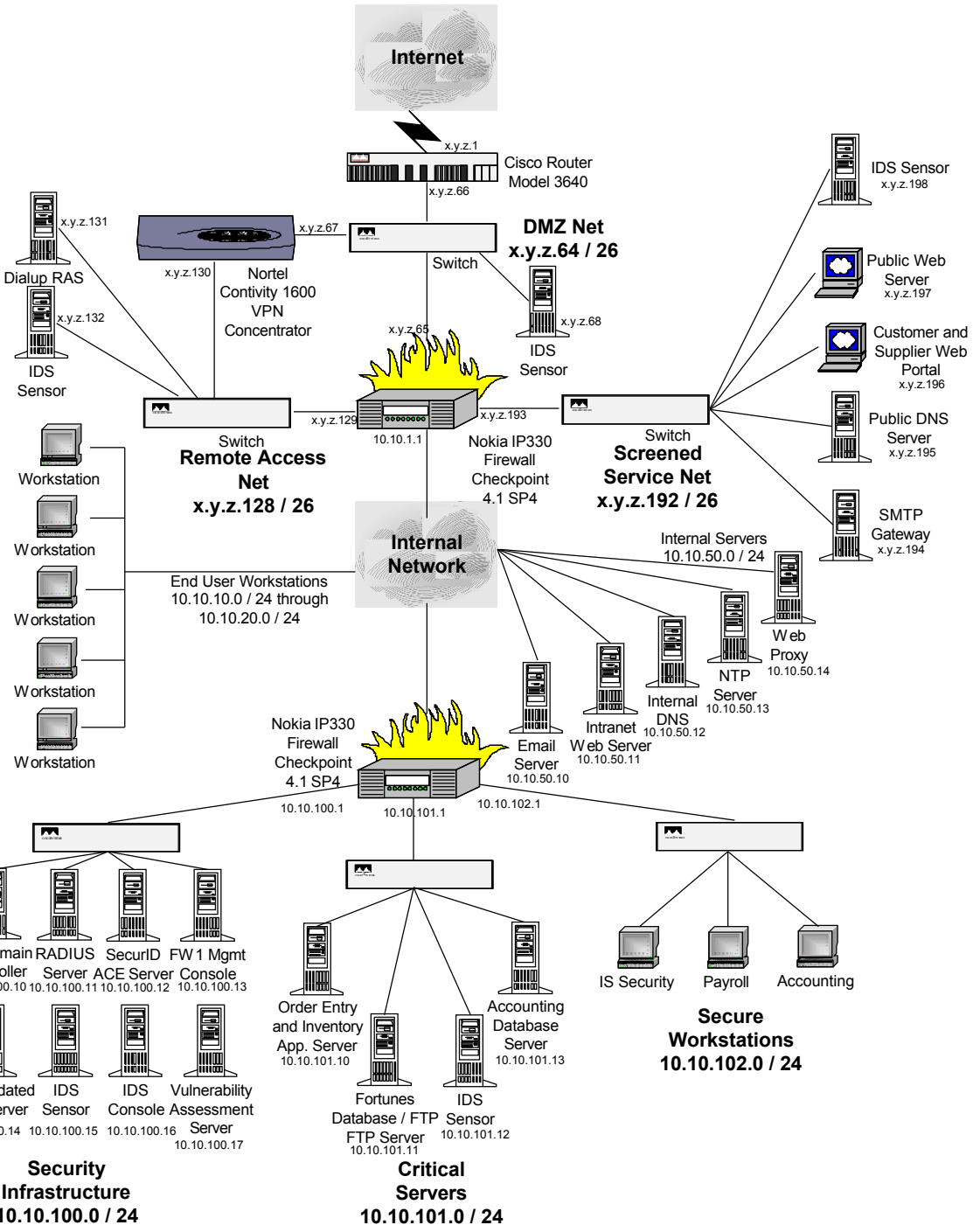
Introduction

GIAC Enterprises is a relatively large e-business generating annual revenues of approximately $500 Million through the online sale of fortune cookie sayings. GIAC Enterprises has a workforce which is composed of a approximately 350 freelance fortune cookie saying authors, several international business partners which translate the fortune cookie sayings into multiple languages and resell the fortunes to other international customers, and a permanent workforce of approximately 250 employees divided into several departments. The Sales and Marketing departments make up the bulk of the workforce since it takes a lot of face time, free lunches, and coffee mugs to close the deal in an industry as competitive as the fortune cookie saying business. Information Systems and Data Processing is the second largest department, as running a large successful e-Business such as GIAC enterprises requires a significant number of highly skilled and somewhat specialized individuals. The remaining staff are primarily involved in supporting the employee and finance related functions of the business such as Accounting, Payroll, Human Resources, Benefits, etc.

The Information Systems and Data Processing Department consists of all the usual groups of IS specialists: Application Developers, Systems and Database Administrators, 24 x 7 Operations and Support Staff, and an extremely overworked IS Security team consisting of 5 individuals. After many long and sometimes heated discussions, the IS Security team has, finally convinced upper management of the importance of Information Security as a business enabler and have been given some capital resources to improve the security architecture of GIAC enterprises. While maintaining business continuity remains the paramount concern, upper management at GIAC Enterprises does now realize that maintaining the security of all mission critical e-business applications and the underlying infrastructure which supports them, is no longer a luxury but is an absolute necessity. Of course, the fact that "Fortunes R Us" (GIAC Enterprises largest competitor) was forced into bankruptcy after their primary e-business web server was compromised by the Code Red worm and their entire fortune cookie sayings database was subsequently downloaded by a 12 year old Russian hacker and posted to newsgroups on the Internet probably helped to bring about their new "enlightened" views on IS Security.

Network Security Architecture

The IS Security team at GIAC Enterprises chose the following network security architecture in order to fulfill the needs of their user base while adding some additional layers of security to their previous architecture. While there are still some additional components that the IS Security team would like to implement as part of their defense in depth strategy at a later date they feel this is a significant improvement in their overall network security architecture. The following diagram depicts the network security architecture of GIAC Enterprises network:



All servers on the DMZ, Screened Service Net, and Remote Access Net are running Slackware Linux 8.0 with Kernel 2.4.9. These servers have been appropriately hardened for service as bastion hosts. The DNS server is running Bind 8.2.5, the Web Servers are running Apache 1.3.22, and the SMTP gateway is running Sendmail 8.12.1 and Interscan Viruswall 3.6 with updated scan engines and virus signatures.

Requirements

There are 5 distinct groups of individuals who regularly interact with information systems hosted by GIAC Enterprises. These Groups are as follows:

GENERAL PUBLIC
The general public typically interacts with GIAC Enterprises through their public website, www.giacenterprises.com and via email. They require access to the GIAC Enterprises public website and they must be able to send and receive email to and from GIAC Enterprises employees. This is a requirement that is shared by each of the remaining groups as well.

CUSTOMERS
Customers are those individuals and companies who purchase fortunes in bulk from GIAC Enterprises via the online Customer Web portal via the Internet. They require encrypted and authenticated access to the GIAC Enterprises Customer Web Portal, customer.giacenterprises.com, where they can place new orders and check the status of previous orders, review and make payments to their account, and download fulfilled orders.

SUPPLIERS
Suppliers are those individuals and companies who author fortune cookie sayings and sell them to GIAC Enterprises. These suppliers are mostly freelance authors who are geographically dispersed across the United States. They produce fortunes in bulk offline and then connect to the GIAC Enterprises network to upload their fortunes. Suppliers require encrypted and authenticated access to the GIAC Enterprises Supplier Web Portal, supplier.giacenterprises.com, where the can check the status of their accounts, receive and bid on future orders, and view general supplier related information and communications via the Internet. Since suppliers are considered employees, they also require access to the GIAC Enterprises Intranet website and internal mail server. Additionally, in order upload their fortunes, Suppliers require authenticated and encrypted access to the Fortunes Database and FTP Server.

BUSINESS PARTNERS
Business partners of GIAC Enterprises are primarily overseas organizations that provide language translation services to GIAC Enterprises for all of their fortunes, as well as resell the fortunes to overseas businesses. GIAC Enterprises has a very close and interdependent relationship with its international business partners. As a result, Business Partners have significantly more requirements than either customers or suppliers alone. In addition to all of the requirements of the previously mentioned groups, Business Partners also require encrypted and authenticated access to the Order Entry and Inventory Applications which run on the Order Entry and Inventory Application Server, and the Accounting Database Server. Access to

these applications is accomplished through a client server application written in house by GIAC Enterprises which utilizes TCP ports 15001 through 15003.

EMPLOYEES
Most employees of GIAC Enterprises are allowed to check email and access the company intranet web site while away from the office. Employees may access the company network either by Dialup RAS or by VPN. A very small subset of employees with IS oncall responsibilities require authenticated and encrypted but otherwise unrestricted access to the servers in order to provide 24 X 7 administrative support to the enterprise. These employees are required to use token based authentication before gaining access to the network.

When locally connected to the GIAC Enterprises Network employees have many more requirements: they must be able to browse the web, share files with one another, authenticate to the Domain, access each of the application servers, etc.

Network Security Architecture Explained

In the current architecture the network is "divided" into 8 distinct networks:

- The Internet (AKA the perimeter net) is connected to the outside interface of our perimeter router. This is where GIAC Enterprises' customers, suppliers, and business partners are located. This is also where the bad guys live. This network is considered actively HOSTILE. Requests originating from this network are not be trusted unless independently authenticated. Sensitive information that must traverse this network must be encrypted.
- The DMZ Network resides outside our Perimeter Firewall and VPN Concentrator. This network is protected from the Internet only by the perimeter router. This network is where the internal interface of the perimeter router and the external interfaces of our Firewall and VPN Concentrator are connected. GIAC Enterprises hosts no network services in the DMZ.
- The Remote Access Network is connected to the inside interface of the VPN concentrator and an "internal" interface of the perimeter firewall. This network is essentially a screened subnet that has been dedicated to remote access. The dialup RAS server is also connected to this network. This network is considered a "semi trusted" network. In order to gain access to this network a user must authenticate to either the dialup RAS server or the VPN Concentrator. Users who authenticate with userids and passwords will be given IP addresses from one DHCP address pool while users who have authenticated with stronger token-based authentication will be given an IP address from a different DHCP address pool. Users at business partner locations who gain access to the Remote access net through VPN tunnels that terminate on the VPN concentrator will have IP addresses from their own IP address range. Some level of trust may be granted to requests originating from this network based on IP address range and the confidence GIAC Enterprises places in the integrity of the authentication

mechanisms used and the security posture of GIAC Enterprises business partners.

- The Screened Service Network is connected to one of the "internal" interfaces of the perimeter firewall. This is the network where all the servers that provide network services to the Internet reside. The public web server and Customer and Supplier Web servers reside here. As does the Public DNS server and the public email gateway. Servers residing in this network will undoubtedly be attacked from the Internet via any ports which are allowed through the firewall. All servers residing in this network should be treated as bastion hosts, by having their operating systems hardened to every degree possible and those network services which must remain exposed to the Internet must have their patches kept current at all times. As little trust as is possible should be granted to the systems residing on this network, as they are the most likely systems to be targeted for attack. When trust must be extended to systems on the DMZ the principle of least privilege should be diligently adhered to when instituting the "trust" in the firewall security policy and in the "trusting" system.
- The Internal network resides inside the firewall and is connected to the internal interface of the perimeter firewall. This network is where most of the internal users' workstations are located. Servers that provide services to the entire company such as email, internal DNS, and Intranet web servers are located here as well. This network is never to be connected to any external network through any means that does not pass through the perimeter firewall. Specifically, rogue dialup lines, leased lines, or "alternative" Internet connections are expressly prohibited by GIAC Enterprises Security Policy. This network can be trusted as much as GIAC Enterprises internal employees can be trusted to follow the stated security policy.
- The Security Infrastructure Network is a secured internal network that resides behind one interface of the Internal firewall. Servers that compromise the security infrastructure of GIAC enterprises reside on this highly restricted segment. Only the IS security team has general access to the systems located on this segment. This segment contains many of the most sensitive security devices and servers on the GIAC Enterprises network and is considered a trusted segment. Unauthorized network traffic to and from this segment is highly scrutinized on a daily basis.
- The Critical Servers Network is a secured internal network that resides behind one interface of the Internal firewall. The 3 mission critical company servers and the Fortunes database reside on this segment. While many general users require access to one or more of these servers, access is strictly limited to those services that are required by the client software and no others. Unauthorized attempts to access the servers on this network are highly scrutinized on a daily basis.
- The Secure Workstations Segment is a secured internal network that resides behind a third interface on the internal firewall. This network segment is reserved for individuals with special security needs. IP addresses are statically

assigned on this network in order to make the process of creating and maintaining appropriate access control lists and firewall rules less burdensome. The IS Security department, as well as several individuals from the accounting and payroll departments have workstations residing on this segment. Workstations on this segment are also protected from the rest of the internal network by the Internal firewall, however the security policy protecting these workstations is considerably less stringent than those protecting the Security Infrastructure and Critical servers networks.

GIAC Enterprises has also added a slight boost to the security of its networks through the exclusive use of switches as the means through which edge connectivity to the network is provided to the end users and servers. This somewhat limits the ability of any system on the network to sniff the network traffic of others on the network without first modifying the configuration of one of the switches.

PERIMETER ROUTER

The Perimeter router represents the first layer of Defense in GIAC Enterprises network security architecture. However, it is worth noting that the primary purpose of this router is to provide connectivity to the Internet, with security being its secondary function. In addition to helping GIAC Enterprises protect its own network, the perimeter router is useful in helping GIAC Enterprises be a good Internet citizen. The perimeter router helps GIAC Enterprises protect its network in the following ways:

- It blocks inbound traffic originating from private address spaces
- It blocks inbound traffic with spoofed source addresses that belong to GIAC Enterprises IP address range
- It blocks the dissemination of information about the structure of the internal networks by blocking "ICMP unreachable" error messages
- It blocks IP directed broadcasts which can cause denial of service conditions across your internal networks such as Smurf attacks
- It blocks packets that are attempting to utilize source routing which usually indicates an attempt to bypass some key network access control point, such as a firewall, by subverting the ordinary routing of packets within the network.
- In addition it provides a point at the edge of the GIAC Enterprises network where malicious traffic can be blocked before it reaches any GIAC Enterprises networks.

Additionally the perimeter router helps GIAC Enterprises be a good Internet citizen in the following ways:

- It blocks outbound traffic originating from private address spaces from leaving the network.
- It blocks outbound traffic with spoofed source addresses not belonging to GIAC enterprises from leaving the network.

Both of these measures help to ensure that the GIAC Enterprises Network will not be used to anonymously launch attacks against other Internet accessible networks or services.

PERIMETER FIREWALL

The perimeter firewall represents the primary network control point within the network. Its placement segregates the GIAC Enterprise network into four main segments: The DMZ network, the screened service network, the remote access network and the internal network. Except for the special case of the traffic going between the remote access network and the DMZ network, all traffic that needs to go from one GIAC Enterprises network to another must pass through the perimeter firewall. The security policy enforced by the firewall is the primary network access control protecting GIAC Enterprises from network based attacks. Additionally since GIAC Enterprises uses private address space for their internal network, the firewall additionally provides Network Address Translation services to the internal users and servers when the must communicate with other Internet based entities. The firewall does not protect GIAC enterprises from network traffic which does not pass through the firewall such as unauthorized dialup connections to the Internet located behind the firewall on the internal network. Neither does it protect the network from exploits which are promulgated through services which are authorized to pass through the firewall. For example the firewall will not protect the public web server from attacks that accomplished through standard http requests since http requests are allowed to pass through the firewall to the public web server unmolested.

VPN CONCENTRATOR

The VPN concentrator is the only device other than the perimeter firewall that controls the flow of network traffic between the four GIAC Enterprises networks. It provides a means for network traffic the get from the DMZ (and therefore the Internet) to the remote access network and visa versa. The VPN concentrator enforces a security policy that requires authentication and strong encryption before allowing such communication to take place however. This device serves as an encryption gateway for remote users who which to access the GIAC enterprises network via the Internet in a Host to Gateway configuration. The VPN Concentrator also serves as an Encryption Gateway for GIAC Enterprises' international business partners in a Gateway to Gateway configuration. The VPN concentrator facilitates the secure communication between these parties. Since the VPN concentrator is located on the remote access network and has a legal IP address there is no need to perform Network Address Translation on the Concentrator which can sometimes be problematic with certain protocols. Nevertheless, the VPN concentrator is still placed outside the perimeter firewall so that an additional layer of security policy enforcement can be performed as the traffic passes through the perimeter firewall to the internal network. In this way the firewall can still serve as a legitimate control point even for tunneled VPN traffic from GIAC Enterprises business partners.

DIALUP RAS SERVER

The dialup RAS server exists to primarily provide access to the GIAC Enterprises network for employees who do not have a personal Internet Service Provider and therefore do not have the ability to access the VPN concentrator from the Internet. The RAS server requires authentication before allowing the dialup user to the remote access network. These dialup users are given an IP address from a specific DHCP address pool so that they can be easily identified. The RAS server is located on the remote access network for similar reasons as the VPN concentrator. Since all traffic from the RAS server must pass through the firewall in order to reach other GIAC Enterprises networks, the perimeter firewall can continue to be used as an enforcement point where security policy can be applied to the traffic before it enters the other GIAC enterprises networks.

INTRUSION DETECTION SENSORS AND CONSOLE

The intrusion detection sensors exist to monitor the network for signs of illicit activity an to generate alerts upon the discovery of such anomalous activity. The IDS sensors are deployed at various key points within the network where suspicious activity is likely to be seen. Each IDS sensor has been deployed in promiscuous mode, monitoring a port on the switch to which it is connected that mirrors all traffic traversing the uplink port of the switch. IDS sensors are deployed on all 3 external legs of the perimeter firewall as well as on the security infrastructure and critical servers networks. All intrusion detection sensors are configured to report any "detects" back to a centralized IDS console that provides a unified view of IDS alert activity across all sensors. The IDS console resides on the protected security infrastructure network. The IDS console is monitored in realtime by IS Security staff.

SPLIT DNS

Split DNS has been deployed in order to prevent the possible disclosure of information to would be attackers. The public DNS is located in the screened service network and contains only information about the publicly accessible servers. The internal DNS resides on the internal network so that is readily accessible to all internal users and contains information about all GIAC Enterprises servers and workstations.

SMTP GATEWAY

A Virus scanning SMTP gateway has been deployed on the screened service net to facilitate the delivery of email to and from the Internet. All inbound email from the Internet is directed to this server via the MX records in the public DNS. The email is scanned for viruses and then passed on to the internal email system. Infected attachments are stripped from the email messages and an alert is sent back to the sender as well as to the IS Security team's alert mailbox. Email sent from the internal email system to Internet email addresses are forwarded from the internal mail system to the virus scanning gateway which acts as an SMTP relay for the internal email system. The messages are then scanned for viruses before leaving the company network.

WEB PROXY

A virus scanning web proxy is deployed on the internal network to facilitate more secure browsing of the web as well as to conserve bandwidth through the caching of frequently viewed web pages on the local server. All users have configured their browsers to utilize this web proxy in order to browse the web. The web proxy scans all files for viruses and hostile active content and allows GIAC Enterprises employees to continue to access web based email services such as hotmail and AOLmail which would otherwise have to be restricted due to the virus threat. No internal users are allowed to browse the web directly through the firewall.

NTP SERVER

The NTP server is located on the internal network so that it is readily available to any server or workstation that is configured to utilize it. Its primary purpose is to facilitate time synchronization of workstations, servers, and network devices across the enterprise. Synchronized clocks on all systems across the enterprise is the first step toward being able to easily correlate events across multiple disparate systems with the enterprise.

INTERNAL FIREWALL

The internal firewall has its external interface connected to the internal network and has three additional interfaces which support secured internal network segments, the Security infrastructure network, the critical servers network, and the secure workstations network. The primary purpose of the internal firewall is to create secure internal network segments for internal systems that need to have a heightened security posture for some reason. It is able to achieve its purpose by physically segregating the internal networks from one another and enforcing a security policy on all traffic that wished to traverse the internal firewall in order to get to or from one of these protected networks.

On the Security Infrastructure network we find systems such as the RADIUS, SecurID ACE, and NT Domain authentication servers, as well as our firewall and IDS management consoles, and other servers which serve sensitive security related functions, such as the consolidated remote logging server and the vulnerability assessment server that contains the results of our automated network based vulnerability assessments from Nmap, Nessus, Whisker and the like.

On the Critical Servers network we find the mission critical business servers that house the applications and data that gives GIAC Enterprises its competitive advantage over the competition.

On the Secure workstations network we find workstations with statically assigned IP addresses that have a need for heightened security, either because of the information stored on the workstation or because of the sensitive nature of the applications that must be accessed by the user of those workstations.

Perimeter Router Security Policy

Since the perimeter router represents the first line of defense for our network we must first harden the router itself to protect it from attack. To accomplish this task we will want to do several things:

```
! Get rid of all unneeded services
!   Turn off the silly tcp and udp services like echo, chargen, and discard
no service tcp-small-servers
no service udp-small-servers
!   Turn off finger
no service finger
!   Turn off snmp
no service snmp
! Turn off http server
no ip http server
! Turn off bootp server
no ip bootp server

! Enable stronger password storage
!   keep clear-text passwords from being displayed in configuration file
service password-encryption
!   use stronger hashing for the enable password in the configuration file
enable secret

! Only allow the secure workstations network to connect to the router
access-list 10 permit 10.10.102.0 0.0.0.255
access-list 10 deny any log
   line vty 0 4
     access-class 10
     login

! Display a login warning banner
banner login /
*** WARNING ***
This system is the property of GIAC Enterprises.
All unauthorized access is strictly prohibited.
If you are not explicitly authorized to access this system, disconnect now.
Failure to do so may result in criminal prosecution, civil penalties, or both.
By continuing beyond this point you attest under penalty of perjury that you are an
authorized user of this system, and that you consent to monitoring of your activities.
If you do not agree with this statement, disconnect now.
/
```

```
! Enable logging to consolidated logging server
logging 10.10.100.14
```

Now that reasonable steps have been taken to harden the router itself, we can begin to filter traffic with the router.

```
! In order to avoid disseminating information about the internal structure of the
! network, block all ICMP "unreachable" error messages.
no ip unreachables

!  Block all IP directed broadcasts to prevent denial of service conditions on our
network
! as well as prevent GIAC Enterprises from becoming a Smurf amplifier.
no ip direct-broadcast

! Block all source routed packets
no ip source-route
```

Note: The policy outlined above should be implemented on all GIAC Enterprises routers. The following access controls are installed only on the perimeter router, however.

```
! Block all inbound traffic originating from private address spaces and the Miscrsoft
! no DHCP lease address space.  Also block all inbound traffic with source IP addresses
! belonging to the GIAC Enterprises address space

ip access-list 11 deny 192.168.0.0 0.0.255.255
ip access-list 11 deny 172.16.0.0 0.15.255.255
ip access-list 11 deny 10.0.0.0 0.255.255.255
ip access-list 11 deny 169.254.0.0 0.0.255.255

ip access-list 11 deny x.y.z.0 0.0.0.255
ip access-list 11 permit any

interface s0/0
   ip address x.y.z.1
   ip access-group 11 in

! Block all outbound traffic that does not have source IP addresses in the GIAC
! Enterprises address space.
ip access-list 12 permit x.y.z.0 0.255.255.255

interface e0/0
   ip address x.y.z.66
   ip access-group 12 in
```

Perimeter Firewall Policy

The first stage to defining the Checkpoint firewall policy is to define the network objects (i.e. networks, servers, workstations) that will need to be referenced in specific firewall rules.

Here are the network objects that need to be defined for GIAC enterprises perimeter firewall.

First define the firewalls themselves:

FW-Perim	x.y.z.65, x.y.z.129, x.y.z.193, 10.10.1.1
FW-Internal	10.10.1.2, 10.10.100.1, 10.10.101.1, 10.10.102.1

Next define the networks:

Net-Perim	x.y.z.0 / 26
Net-DMZ	x.y.z.64 / 26
Net-Remote	x.y.z.128 / 26
Net-Service	x.y.z.192 / 26
Net-Internal	10.10.0.0 / 16
Net-Internal-Backbone	10.10.1.0 / 24
Net-Enduser	10.10.10.0 / 24 through 10.10.20.0 / 24
Net-InternalServer	10.10.50.0 / 24
Net-SecurityInfra	10.10.100.0 / 24
Net-CriticalServers	10.10.101.0 / 24
Net-SecureWkstn	10.10.102.0 / 24

Next define the networks for all business partners we have VPN connections to

Net-Business-Partners	a.a.a.0 / 24, b.b.b.0 / 24, c.c.c.0 / 24, etc.

Next define the network gear, servers, and workstations:

Perim-router	x.y.z.1, x.y.z.66
DMZ-VPN-Concentrator	x.y.z.67, x.y.z.130
DMZ-IDS	x.y.z.68
Remote-RAS	x.y.z.131
Remote-IDS	x.y.z.132
Service-SMTP	x.y.z.194
Service-DNS	x.y.x.195
Service-Web-Portal	x.y.z.196

Service-Public-Web	x.y.z.197
Service-IDS	x.y.z.198
InternalServer-Email	10.10.50.10
InternalServer-Intranet	10.10.50.11
InternalServer-DNS	10.10.50.12
InternalServer-NTP	10.10.50.13
InternalServer-Web-Proxy	10.10.50.14
SecurityInfra-PDC	10.10.100.10
SecurityInfra-RADIUS	10.10.100.11
SecurityInfra-ACE	10.10.100.12
SecurityInfra-FW-Console	10.10.100.13
SecurityInfra-Log-Server	10.10.100.14
SecurityInfra-IDS	10.10.100.15
SecurityInfra-IDS-Console	10.10.100.16
SecurityInfra-Assessment	10.10.100.17
CriticalServer-Order-Inv	10.10.101.10
CriticalServer-Fortunes-DB	10.10.101.11
CriticalServer-IDS	10.10.101.12
CriticalServer-Acct-DB	10.10.101.13
SecureWkstn-Security	10.10.102.0 / 27
SecureWkstn-Payroll	10.10.102.32 / 27
SecureWhstn-Acct	10.10.102.64 / 27

Lastly define the DHCP Address pools that the Dialup RAS server and VPN concentrator will assign to remote users

Remote-Token-Users	x.y.z.144 / 28
Remote-Password-Users	x.y.z.160 / 28
Remote-Suppliers	x.y.z.176 / 28

With the network objects defined we can now begin to build the perimeter firewall policy. Checkpoint firewall policies are constructed via a graphical user interface known as the policy editor. We will use the policy editor to build a checkpoint policy capable of enforcing the following requirements in the perimeter firewall:

General Public

- Need to be able to browse the public web site
- Need to be able to resolve public DNS names
- Need to be able to send and receive email to and from GIAC Enterprises

Customers

- Same requirements as General Public plus
- Need to be able to browse the Customer Web Portal over an authenticated HTTPS connection. All interaction with the web portal is over HTTPS.

Suppliers

- Same requirements as General Public plus
- Need to be able to browse the Supplier Web Portal over an authenticated HTTPS connection. All interaction with the web portal is over HTTPS.
- Must be able to use the VPN to browse the Intranet web site.
- Must be able to use the VPN to access the internal email system via IMAP4
- Must be able to use the VPN to upload data files to the Fortunes database and FTP server via FTP

Business Partners

- Same Requirements as General Public, Customers, and Suppliers plus
- Must be able to use the VPN tunnel to access the Order Entry and Inventory applications over proprietary protocol utilizing TCP ports 15001 through 15003

Employees (Remote Requirements)

- Same requirements as General Public plus
- Must be able to use the VPN or Dialup RAS to browse the Intranet web site.
- Must be able to use the VPN or Dialup RAS to access the internal email system via IMAP4
- Certain employees must be able to use the VPN with token authentication to have unrestricted access to the internal network.

Employees (Internal Requirements)

- Must be able to browse the GIAC Enterprises Public Website and the Customer and Supplier Web Portals
- Must be able to browse the internet (via the Web Proxy only)
- Must be able to send and receive email (via internal email or SMTP gateway only)
- On the internal network employees must be able to do much more, such as share files with one another, authenticate to the domain, etc. but those activities remain inside the perimeter firewall, and therefore require no additional rules in the perimeter firewall.

Server, Device, and Workstation Specific Requirements

- All Devices on the GIAG Enterprises network are allowed to send their syslogs to the consolidated logging server
- All IDS Sensors are allowed to send their syslogs to the IDS console
- IS Security is allowed to telnet and ssh anywhere on the GIAC enterprises network.

- The Dialup RAS and VPN Concentrator must be able to perform RADIUS authentication against the RADIUS server
- The public and internal DNS servers need to be able to resolve DNS names from the Internet
- All devices on the GIAC enterprises network are allowed to synchronize time off the internal NTP server. The NTP server uses an external GPS time source.
- The Vulnerability Assessment server must be allowed unrestricted access to the GIAC Enterprises network

Default Policy
Everything that is not explicitly allowed should be blocked and logged. We'll also want to drop all of the Netbios/IP broadcast traffic without logging it to help reduce the amount of noise in the log file.

The following Checkpoint FW-1 policy cane be installed on the perimeter router to enforce the previously stated policy requirements. For clarity, the rule number, install on, time, and comment fields have been removed from this representation of the checkpoint policy. Each rule would be installed on FW-Perim and have no time restrictions in place.

Rule	Source	Destination	Service	Action	Track	Comments
1	Net-Internal	Any	NBT	Drop		Drop all Netbios over TCP/IP broadcast noise
2	SecureWkstn-Security	Net-Perim Net-DMZ Net-Remote Net Service	Telnet Ssh Firewall-1	Accept	Long	Allow Security Team to telnet, ssh, and remotely administer firewalls anywhere
3	SecurityInfra-Assessment	Net-Perim Net-DMZ Net-Remote Net Service	Any	Accept	Long	Allow the Vulnerability Assessment box unrestricted network access
4	Any	FW-Perim	Any	Drop	Long	Do not allow anyone to connect to the firewall itself
5	Any	Service-Public-Web	Http	Accept	Long	Allow everyone to browse the public web site
6	Any	Service-Web-Portal	Https	Accept	Long	Allow anyone who can successfully authenticate to access the customer and supplier web portal
7	Any	Service-DNS	Dns-udp	Accept	Long	Allow anyone to resolve public DNS names

8	Any	Service-SMTP	Smtp	Accept	Long	Allow anyone to send email to the email virus scanning gateway
9	Service-SMTP	Any	Smtp	Accept	Long	Allow the virus scanning email gateway to send email to anyone
10	InternalServer-Web-Proxy	Not Net-Perim Not Net-DMZ Not Net-Remote Not Net-Service	Http https	Accept	Long	Allow the internal web proxy to access web content on the internet
11	Service-DNS	Not Net-Internal Not Net-Perim Not Net-DMZ Not-Net-Remote	Dns-tcp Dns-udp	Accept		Allow the public DNS to resolve DNS names from the Internet
12	InternalServer-DNS	Any	Dns-tcp Dns-udp	Accept		Allow the Internal DNS server to resolve DNS names from anywhere
13	Net-Perim Net-DMZ Net-Remote Net Service	SecurityInfra-Log-Server	Syslog	Accept		Allow any system to syslog to the consolidated log server
14	Net-Perim Net-DMZ Net-Remote Net Service	InternalServer-NTP	Ntp	Accept	long	Allow any system to synchronize time with the NTP server
15	DMZ-IDS Remote-IDS Service-IDS	Security-Infra-IDS-Console	Syslog	Accept		Allow the IDS boxes to syslog back to the IDS console
16	Remote-Suppliers Net-Business-Partners Remote-Password-Users	InternalServer-Intranet	Https	Accept	Long	Allow GIAC suppliers, business partners and employees to access the Intranet web site
17	Remote-Suppliers Net-Business-Partners Remote-Password-Users	InternalServer-Email	IMAP4	Accept	Long	Allow GIAC suppliers, business partners and employees to access the internal email system
18	Remote-Suppliers Net-Business-Partners	CriticalServer-Fortunes-DB	FTP	Accept	Long	Allow GIAC suppliers and business partners to upload FTP to the Fortunes Database Server
19	Net-Business-Partners	CriiticalServer-Order-Inv CriticalServer-Acct-DB	TCP15001 TCP15002 TCP15003	Accept	Long	Allow GIAC business partners to access the Order entry and Accounting database via a custom application.

20	Remote-Token-Users	Net-Internal	Any	Accept	Long	Allow a select group of employees unrestricted access to the network after they authenticate to the VPN via token
21	DMZ-VPN-Concentrator Remote-RAS	SecurityInfra-RADIUS	RADIUS	Accept	Long	Allow the VPN and dialup RAS server to authenticate users via RADIUS (proxy)
22	Any	Any	Any	Drop	Long	Drop everything that is not expressly permitted.

Contivity VPN Policy

VPN "Policies" on Nortel Contivity Switches are closely related to object called Groups. A group can be thought of as collection of policy settings that can be applied to a VPN session. Host to gateway and gateway to gateway VPN's both utilize groups in a similar fashion. For the purpose of this activity I was only able to obtain web management access to the Contivity box so I will have to improvise somewhat with regards to formatting. Unlike the Checkpoint firewall GUI which consolidates the firewall rules into a single, comprehensive, and easy to manage policy, the web interface of the Contivity switch requires you to access many web pages in order to get a comprehensive view of the policy that is implemented on the box.

GIAC Enterprises will need 3 different groups: one for host to gateway VPN users who authenticate via RADIUS with a userid and password , one for host to gateway VPN users who authenticate via RADIUS with a SecurID token, and one for gateway to gateway VPN users (Business Partners). All three groups have similar requirements of authentication and strong encryption, however. The 3 groups have the following characteristics:

The group for the Host to Gateway VPN users who use passwords:

Group Name:	HOST-GW-PASSWORD
Access Hours:	Anytime
Password Management:	Disabled*
Idle Timeout:	00:15:00
Filters:	None
IPX:	Disabled
Address Pool Name:	HOST-PW
Split Tunneling:	Disabled
Split Tunnel Networks:	None
Client Selection:	
Allow both Contivity and non-Contivity Clients:	Enabled
Allow Undefined networks for non-Contivity clients:	Disabled

Database Authentication (LDAP):	Disabled
RADIUS Authentication:	
Userid and Password:	Enabled
Encryption:	
ESP – Triple DES with MD5 Integrity:	Enabled**
IKE Encryption and Diffie-Hellman Group:	Triple DES with Group2
Perfect Forward Secrecy:	Enabled
Forced Logoff:	00:00:00
Banner:	Warning – Authorized Users Only…
Rekey Timeout:	02:00:00
Allow Password Storage on Client:	Disabled
Client Policy:	None
IPSec Transport Mode Connections:	Enabled

* Passwords are managed through the RADIUS implementation
** ESP utilizing Triple DES with MD5 authentication was chosen because we needed encryption in addition to authentication of the message.

The group for the Host to Gateway VPN users who use tokens:

Group Name:	HOST-GW-TOKEN
Access Hours:	Anytime
Password Management:	Disabled*
Idle Timeout:	00:15:00
Filters:	None
IPX:	Disabled
Address Pool Name:	HOST-TOKEN
Split Tunneling:	Disabled
Split Tunnel Networks:	None
Client Selection:	
Allow both Contivity and non-Contivity Clients:	Enabled
Allow Undefined networks for non-Contivity clients:	Disabled
Database Authentication (LDAP):	Disabled
RADIUS Authentication:	
Security Dynamics SecurID:	Enabled
Encryption:	
ESP – Triple DES with MD5 Integrity:	Enabled
IKE Encryption and Diffie-Hellman Group:	Triple DES with Group2
Perfect Forward Secrecy:	Enabled
Forced Logoff:	00:00:00
Banner:	Warning – Authorized Users Only…
Rekey Timeout:	02:00:00
Allow Password Storage on Client:	Disabled

Client Policy:	None
IPSec Transport Mode Connections:	Enabled

* Using tokens so no passwords to be managed

The group for the Gateway to Gateway VPN tunnels:

Group Name:	GW-GW
Nailed Up:	Disabled
Access Hours:	Anytime
Password Management:	Disabled*
Idle Timeout:	00:15:00
Encryption:	
ESP – Triple DES with MD5 Integrity:	Enabled
IKE Encryption and Diffie-Hellman Group:	Triple DES with Group2
Perfect Forward Secrecy:	Enabled
Rekey Timeout:	02:00:00

Note: there are several parameters that have been omitted for the save of brevity.

Host to gateway users are associated with the appropriate group and authenticated via RADIUS.

Gateway to gateways VPN endpoints are associated with the appropriate group through a branch office object. The branch office object has the following characteristics:

Connection Name:	Business-Partner-A
Group Name:	GW-GW
State:	Enabled
Local Endpoint Address:	x.y.z.67
Remote Endpoint Address:	a.a.a.a (IP Address)
Tunnel Type:	IPSec
IPSec Authentication:	
Hex Pre Shared Key:	Enabled
Hex Pre Shared Key:	**********
Confirm:	**********

There would be one Branch office object for each Business Partner.

How to implement Cisco Access Controls

Lets assume that you have a working Cisco 3640 router as a border router with a single serial interface on the exterior interface and an Ethernet interface as the interior interface. Your router has not been hardened and does not have any ACL's installed.

Here's a simple tutorial explaining how to harden the router and implement the access controls described earlier.

Recall our configuration commands and access lists (without all the comments):

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no service snmp
no ip http server
no ip bootp server
service password-encryption
enable secret
access-list 10 permit 10.10.102.0 0.0.0.255
access-list 10 deny any log
   line vty 0 4
     access-class 10
     login
banner login /
*** WARNING ***
This system is the property of GIAC Enterprises.
All unauthorized access is strictly prohibited.
If you are not explicitly authorized to access this system, disconnect now.
Failure to do so may result in criminal prosecution, civil penalties or both.
By continuing beyond this point you attest under penalty of perjury that you are an
authorized user of this system, and that you consent to monitoring of your activities.
If you do not agree with this statement, disconnect now.
/
logging 10.10.100.14
no ip unreachables
no ip direct-broadcast
no ip source-route
ip access-list 11 deny 192.168.0.0 0.0.255.255
ip access-list 11 deny 172.16.0.0 0.15.255.255
ip access-list 11 deny 10.0.0.0 0.255.255.255
ip access-list 11 deny 169.254.0.0 0.0.255.255
ip access-list 11 deny x.y.z.0 0.0.0.255
ip access-list 11 permit any
interface s0/0
   ip address x.y.z.1
   ip access-group 11 in
ip access-list 12 permit x.y.z.0 0.255.255.255
interface e0/0
   ip address x.y.z.66
   ip access-group 12 in
```

To implement configuration commands and access lists perform the following tasks:
Login to the router via telnet

```
telnet x.y.z.1

User Access Verification
Password:
```

You will be at the router> prompt, enter the enable command

```
Router> enable
```

You will be prompted for the enable password, enter it and you will be taken to the enable prompt.

```
Password:
Router#
```

Go into global configuration mode by entering the "conf t" command. Be very careful, while in configuration mode. It's possible to cause yourself some serious problems if you're not paying attention. Be especially careful when applying access lists to interfaces to make sure that you don't lock yourself out of the router. You also want to check your syntax to make sure you don't make typos if you can help it because editing numbered access lists can be a pain. If you make a mistake or you don't feel comfortable with the changes you've made to the configuration file and just want to get out of configuration mode without making any changes just hit control-c.

```
Router#conf t
Router(config)#
```

Now begin hardening the router

```
Router(config)#no service tcp-small-servers
Router(config)#no service udp-small-servers
Router(config)#no service finger
Router(config)#no service snmp
Router(config)#no ip http server
Router(config)#no ip bootp server
Router(config)#service password-encryption
Router(config)#enable secret
```

Now restrict login access to the router. Be sure that you define the access list before Attempting to enable it, otherwise you may not be able to login to the router across the network.

```
Router(config)#access-list 10 permit 10.10.102.0 0.0.0.255
```

```
Router(config)#access-list 10 deny any log
Router(config)#    line vty 0 4
Router(config)#      access-class 10
Router(config)#      login
```

Set the login Banner by entering "banner login" followed by the ending character you want to use such as "/". Then enter the lines of your warning banner followed by another the ending character you specified earlier.

```
Router(config)#banner login /
Enter text message, end with '/'
*** WARNING ***
This system is the property of GIAC Enterprises.
All unauthorized access is strictly prohibited.
If you are not explicitly authorized to access this system,
disconnect now.  Failure to do so may result in criminal
prosecution, civil penalties, or both.  By continuing beyond this
point you attest under penalty of perjury that you are an
authorized user of this system, and that you consent to
monitoring of your activities.  If you do not agree with this
statement, disconnect now.
/
Router(config)#
```

Enable logging to the syslog server, and block ICMP unreachable messages, IP directed broadcasts, and source routed packets.

```
Router(config)#logging 10.10.100.14
Router(config)#no ip unreachables
Router(config)#no ip direct-broadcast
Router(config)#no ip source-route
```

Create the ingress and egress filtering ACL's. The format of the standard ACL's we are using is as follows:

ip access-list <access list number> <action> [<source> <wildcard>] | [any]

Where:

<access list number> is a number between 1 and 99,
<action> is either permit or deny, and
<source><wildcard> specifies a source address to match against and a wildcard to specify how many bits of the source address to check in order to determine a match. In other words, in order for an address to match a source/wildcard pair every bit in the source address must match every bit in the address you are checking against, EXCEPT for those bits that are set to 1 in the wildcard. As an

example, wildcard of 0.0.0.0 requires every single bit to match up, while a wildcard of 0.0.0.255 would require only the first 24 bits of the addresses to match up. The keyword "any" can be used to match any address in lieu of specifying a source/wildcard pair.

```
Router(config)#ip access-list 11 deny 192.168.0.0 0.0.255.255
Router(config)#ip access-list 11 deny 172.16.0.0 0.15.255.255
Router(config)#ip access-list 11 deny 10.0.0.0 0.255.255.255
Router(config)#ip access-list 11 deny 169.254.0.0 0.0.255.255
Router(config)#ip access-list 11 deny x.y.z.0 0.0.0.255
Router(config)#ip access-list 11 permit any

Router(config)#ip access-list 12 permit x.y.z.0 0.255.255.255
```

If you mess up one of these commands you can remove it by issuing the "no" command in front of the incorrect line. For example if you incorrectly typed

```
Router(config)#access-list 11 deny 169.255.0.0 0.0.255.255
```

as the 4th line of access list 11 you could remove it by typing

```
Router(config)#no access-list 11 deny 165.255.0.0 0.0.255.255
```

You would then be free to re-add the line. Unfortunately, it will be added after the last line of access list 11, so if you didn't catch your error right away you would have to delete every line of access list 11 after the 4th line and re-add each one of the in order to maintain the correct ordering.

After you have your access lists correct, apply the ingress filter to the serial interface, and the egress filter to the Ethernet interface. It may be wise to issue a "wr t" command to display the configuration file so that you can verify that your access controls are correct before proceeding, just to be safe.

```
Router(config)#interface s0/0
Router(config-if)#    ip address x.y.z.1
Router(config-if)#    ip access-group 11 in

Router(config-if)#interface e0/0
Router(config-if)#    ip address x.y.z.66
Router(config-if)#    ip access-group 12 in
```

The access list restrictions will take place immediately upon the issuance of the "ip access-group" command. The other configuration commands will take place as soon as the configuration file is written to memory. This is accomplished by issuing the control-Z command.

```
Router(config-if)#^Z
```

The policy is now applied but in order to make your you policy would survive a power down you will need to write the configuration to NVRAM with the "wr" command

```
Router(config-if)#wr
```

Possible Vulnerabilities

There were three ACL's in the perimeter firewall policy: access list 10 which restricted login access to the router, access list 11which performed ingress filtering, and access list 12 which performed egress filtering.

Access list 10 addresses a potential vulnerability with the login process. Without this ACL anyone from any source IP address could attempt to login to the router. The attacker could attempt to guess the password, or since telnet is a cleartext protocol they may have been able to somehow sniff the password from the wire at some point. This access control ensures that only those individuals residing on the wesure workstations network are allowed to even attempt to login to the router, regardless of whether they know the password or not.

Access list 11 addresses a potential Denial of Service Vulnerability or Trust Relationship vulnerability. Many Denial of Service attacks employ spoofed source IP addresses in order to make it more difficult to trace the attack back to its origin. By blocking all spoofed traffic at the perimeter router the remainder of the network is somewhat insulated from the attack, at least on the internal network. Since certain access controls are based on source IP addresses there exists the possibility that critical controls may be bypassed if the attacker is able to make the destination believe that the request is coming from a trusted network, such as the internal network for example. Attacks which rely on TCP sequence number prediction are one such example of this kind of attack.

Access List 12 addresses much the same issues as Access list 11, however the primary purpose of access list 12 is to help ensure that you do not allow malicious traffic of the kind described above, out of your network. It can be thought of as a "good Internet citizen" ACL.

Testing the ACL's

To verify that access list 10 is working correctly simply attempt to telnet to the router from a several source IP addresses that are not on the secure workstations network. If you get a login prompt, then the ACL is not working correctly. If you do not get a login prompt from those workstations, simply verify that you can telnet and get a login

prompt from the secure workstations network. If you get prompted to login from the secure workstation network the ACL has been properly implemented.

To verify that access list 11 is working correctly perform a small port scan of your perimeter firewall from a system on the Internet with nmap. Use the decoy option to specify an address from each one of the denied IP ranges as well as your own. Monitor the firewall logs to see which systems show up in the firewall logs. If only the real IP address of the nmap scanner shows up you know the ACL is working. If all of the spoofed addresses show up in the logs then there is a problem with the ACL. The format of an nmap command that would accomplish this follows:

```
Nmap -sT -p 1-50 -D 10.10.10.10,192.168.10.10,172.16.10.10,
169.254.10.10,x.y.z.10,real.scanner.ip.address x.y.z.65
```

To verify that access list 12 is working properly, perform the same kind of nmap scan of a system under your control on the Internet or outside your perimeter firewall running IP chains, or some personal firewall software such as Zone Alarm, or Norton Personal Firewall. Check the firewall logs as we did for access list 11.

Auditing the Firewall

Lance Spitzner has an excellent guide to assist you in planning and conducting a firewall audit. While I have embellished his approach in several ways, many portions of the following audit plan and methodologies were directly borrowed from Lance's firewall auditing white paper (Spitzner, 2000) located here: http://www.enteract.com/~lspitz/audit.html

The first stage of the audit is to define the goals of the audit. It's a good idea to try to state the goals as simply as possible. Here are the goals for this audit:

- Verify that the firewall OS is secure
- Determine the security policy that is supposed to enforced by the firewall
- Verify that the firewall is properly enforcing the stated security policy
- Evaluate the results of the audit and propose corrective measures

Please note that is very important to keep a log of all audit activities. Be sure that the log contains accurate date and time stamps so that all audit activities can be correlated the log files that may be generated on the various components "touched" by the audit.

Also note that it is often wise to conduct the network scanning portions of the audit during periods of low activity. Certain auditing techniques such as port scanning and vulnerability scanning can potentially add a significant load to the firewall. Limiting the scans to off hours will reduce the likelihood of problems that may impact users of the network. It also makes log file analysis somewhat easier as there are fewer non-audit related entries generated during periods of low activity. For certain audit activities is it

prudent to schedule an outage, or al least inform the user and technical community that an outage could result from your activities before conducting those components of the audit. When you are checking to see if your firewall is vulnerable to denial of service attacks is a perfect example. You may actually cause the outage with your audit, so it's best to make sure that everyone has been informed of the potential consequences well in advance. Activities that do not place an additional load on the firewall such as verifying specific OS configuration settings can be conducted during normal business hours.

A comprehensive firewall audit will involve several port scans and vulnerability scans, some log file review, a hands on examination of the OS configuration, loads of data analysis, a few follow-up tests, and quite a bit of documentation. I would plan on at least a week if you're used to performing these kinds of audit and already have all your tools in place and know how to use them. Otherwise, you may need a couple of weeks to complete the audit. Many external auditing companies charge $200/hr or more to conduct this kind of audit so it certainly seems reasonable to spend a little bit of time learning how to conduct this kind of audit in house.

Before you begin you will need to make sure that you have several tools: A port scanner with as much flexibility as possible. My personal opinion is that nmap is the best general purpose port scanner you're going to find anywhere. You'll also need a good vulnerability scanner like, Nessus, ISS, or Cybercop Scanner. In addition to these two tools, I like to have some kind of sniffer available as well.

Verify that the firewall OS is secure:

- No OS is secure if you can't physically secure the server it resides on, so make sure that the firewall is safe from unauthorized access.

- Verify that the OS has been correctly hardened. There are many excellent hardening checklists and tutorials available for various operating systems. Find one for your operating system or create your own and audit the firewall OS against this checklist. For Linux, Solaris, and NT firewalls, Lance Spitzner has some excellent "Armoring" white-papers that specifically focus on armoring those Operating Systems for firewalls (Spitzner, 2000-2001). SANS also has some excellent "Step-by-Step" guides for securing Linux, Solaris, Windows NT, and Windows 2000.
  Armoring Linux – http://www.enteract.com/~lspitz/linux.html
  Armoring Solaris – http://www.enteract.com/~lspitz/armoring.html
  Armoring NT – http://www.enteract.com/~lspitz/nt.html
  SANS "Step-by-Step" guides – http://www.sansstore.org

- Set up your port scanner and vulnerability scanner on an IP address that does not belong to the firewall administrator group or "authorized GUI clients" list on

the firewall, and scan the firewall itself, with your port scanner.

Scan for TCP

```
# nmap -sS -p1-65535 10.10.1.1
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
All 65535 scanned ports on  (10.10.1.1) are: filtered
```

Scan for UDP

```
# nmap -sU -p1-65535 10.10.1.1
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
All 65535 scanned ports on  (10.10.1.1) are: filtered
```

Does the firewall respond to ICMP Echo requests

```
# ping 10.10.1.1
PING 10.10.1.1 (10.10.1.1): 56 data bytes

--- 10.10.1.1 ping statistics ---
6 packets transmitted, 0 packets received, 100% packet loss
```

You should not find any open ports at all and the firewall should not respond to ping. If it has no open ports, and doesn't respond to ICMP then there aren't many avenues through which to compromise the firewall itself remotely. If any port at all shows up here you want to determine exactly what it is before proceeding, and make a note to get rid of it.

- You may want to scan the firewall with your vulnerability scanner, especially if there was a port open. Since my firewall did not have any listening ports the nessus scan was completely uneventful. Be careful not to run all of the Denial of Service checks at this time, unless you have a scheduled outage (just in case).

- If you have a scheduled outage for part of your audit, you can stop the firewall with the "fwstop" command and then scan the OS without the firewall protection to see how "naked" the firewall would be if the firewall were to crash. Before doing this with a real firewall make sure you completely disconnect it from the network before stopping the firewall.

  Scan for TCP

```
# nmap -sS -p1-65535 10.10.1.1
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
Interesting ports on (10.10.1.1):
```

```
(The 65534 ports scanned but not shown below are in state:
closed)
Port        State       Service
22/tcp      open        ssh
```

Scan for UDP

```
# nmap -sU -p1-65535 10.10.1.1
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
All 65535 scanned ports on  (10.10.1.1) are: filtered
```

Does the firewall respond to ICMP Echo requests

```
# ping 10.10.1.1
PING 10.10.1.1 (10.10.1.1): 56 data bytes
64 bytes from 10.10.1.1: icmp_seq=0 ttl=253 time=1.3ms
64 bytes from 10.10.1.1: icmp_seq=1 ttl=253 time=1.1ms

--- 10.10.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
```

Any expected service that shows up, like ssh in this case should be double checked to make sure that the network application listening on the port has the latest patches in place and is not vulnerable to any known attack. If anything unexpected shows up you'll want to make sure that you note it in your report so that it can be remediated.

- It might also be a good idea to check and make sure that the firewall will not route traffic when the firewall is stopped. I've actually known an organization that intentionally made the firewall continue to route traffic if the firewall failed so that the Internet would still be available in such an event. This is not the default behavior of checkpoint firewalls however, and I do not recommend this approach!

- Don't forget to start the firewall with "fwstart" before reconnecting the firewall to the network.

- As long as you're still within your outage time window, you may want to see if your firewall is vulnerable to denial of service attacks. Nessus has a very good selection of DOS attacks to try. You may also want to try jolt2 since it has been known to cause some versions of Checkpoint to have problems.

Determine the security policy that is supposed to enforced by the firewall

- Check to see if there is a written network security policy. Usually there isn't. Therefore, I recommend looking at the firewall rule base, line by line, to try to get a feel for what they want the firewall to do. If used, the comments field of each rule can be especially helpful.

- Generally speaking, it's worth questioning any rule you don't completely understand the purpose of. I also like to question "allow" rules that have an "any" in them. While I agree, they are often completely appropriate, many rules that are implemented during the fog of troubleshooting will be implemented in this manner "just to see if it fixes the problem". When the next crisis strikes, those quick fixes sometimes become permanent security policy.

Verify that the firewall is enforcing the stated security policy.

- In order to completely verify that the firewall is enforcing the stated security policy (with network scanning tools alone), you would need to scan a representative sample of servers on each network protected by the firewall from a representative sample of servers on every other network over all 65000 TCP and UDP ports. This would be VERY time consuming on even simple networks. Instead the approach taken by many firewall auditors is to scan a single system on each network protected by the firewall from a single "untrusted" system on every other network. By untrusted I mean "not specifically authorized to access the system being scanned". You can see how even this methodology can quickly consume many hours as the complexity of your firewall configuration grows: a 2 interface firewall would require 2 TCP and 2 UDP scans, a 3 interface firewall would require 6 TCP and 6 UDP scans, a 4 interface firewall would require 12 TCP and 12 UDP scans… OUCH! Math geeks out there might be interested to know that a formula for determining the number of scans required for an n-interface firewall would be n^2 – n or n * (n-1). Oops, I just gave myself away, didn't I? Nevertheless, this is the approach we will use in this audit.

- The TCP scan can be accomplished with a simple nmap command. Lets scan the public web (x.y.z.197) from an untrusted host on the internal network (10.10.10.10):

```
# nmap -sS -P0 -p1-65535 x.y.z.197
Starting nmap V. 2.54BETA5 ( www.insecure.org/nmap/ )
Interesting ports on (x.y.z.197):
(The 65534 ports scanned but not shown below are in state:
filtered)
Port        State       Service
80/tcp      open        ssh
```

  This was as we expected. Everything was filtered except for port 80. Had anything else showed up, even if it showed up in a closed state, we should still

be concerned, because for some reason that traffic was not filtered at the firewall, but was allowed through the firewall. The real key here is to look for anomalies and doggedly follow-up on any that you find. This process was repeated for other networks with similar results. However, this is no guarantee that there are no vulnerabilities in the rule base! This is just one more confirmation, along with our visual review of the rule base that there are no systemic problems with the rule base, that can be easily detected.

- Determining what UDP ports are not being filtered is not such an easy task. Lance Spitzner explains why in "Auditing Your Firewall Security": (Spitzner, 2000)

  "This method of scanning through the firewall works well for TCP, but does not work for UDP. UDP scanning works by sending a UDP packet. If the UDP port is not open and is not listening, an ICMP Port Unreachable error message is generated and sent back to the remote system. This lets us know the port is NOT open. If the UDP is open, then the UDP packet is accepted and no return packet is sent. However, we do not want to determine if a port is open, but we want to determine if a port is filtered, did our UDP packet get through the firewall. Scanning through the firewall will not work. If the UDP packet is filtered (and thus dropped by the firewall) we will not get a response. If the UDP is NOT filtered and makes it through the firewall, the packet will most likely be accepted by the remote system and once again, no response is sent. So how do we over come this?

  You use two systems, one for scanning through the firewall, a second system is placed on the other side of the firewall and sniffs all incoming UDP traffic. This way if any UDP packets are not filtered by the firewall and make it through to the other side, the network sniffer will detect and capture these packets. You can then determine which UDP packets are not filtered at the firewall."
- Under certain circumstances it may be useful to try different source ports when you scan, especially if you're auditing a filtering router based "firewall"l w/ ACL's. Ports 20 and 53 might be particularly fruitful under such circumstances. For a fully stateful firewall like Checkpoint you're not going to gain much from your extra effort.

- For every unfiltered port to every server, you should identify the network service listening on that and verify that it has all security patches applied and that there are no known vulnerabilities. This is EXTREEMLY important for any service that is going to be accessible from the Internet.

- As a matter of due diligence I would also run nessus against every server and network device on the perimeter network, DMZ network, screened service network, and remote access networks, and make a note to remediate any vulnerabilities identified in those systems.

- Check your firewall logs against your timed audit log and verify that the firewall logged all your audit activities. Investigate and document any logging anomalies discovered.

Evaluate the results of the audit and propose corrective measures

- While the overall audit results appear good, it seems that there exists a potential vulnerability with the firewall server itself should the firewall software ever crash. Apparently, the ability for anyone to attempt to login to the server via ssh under such circumstances had not been properly restricted. I recommend implementing host based access controls on ssh and limiting access to workstations on the SecureWkstn-Security network. I may also recommend placing an extended access list in the filtering router that will block all inbound traffic to the firewall on the serial interface with a destination port of TCP 22. This would require us to convert the current ingress filter from a standard access list to an extended access list, as standard access lists cannot support this type of filtering.

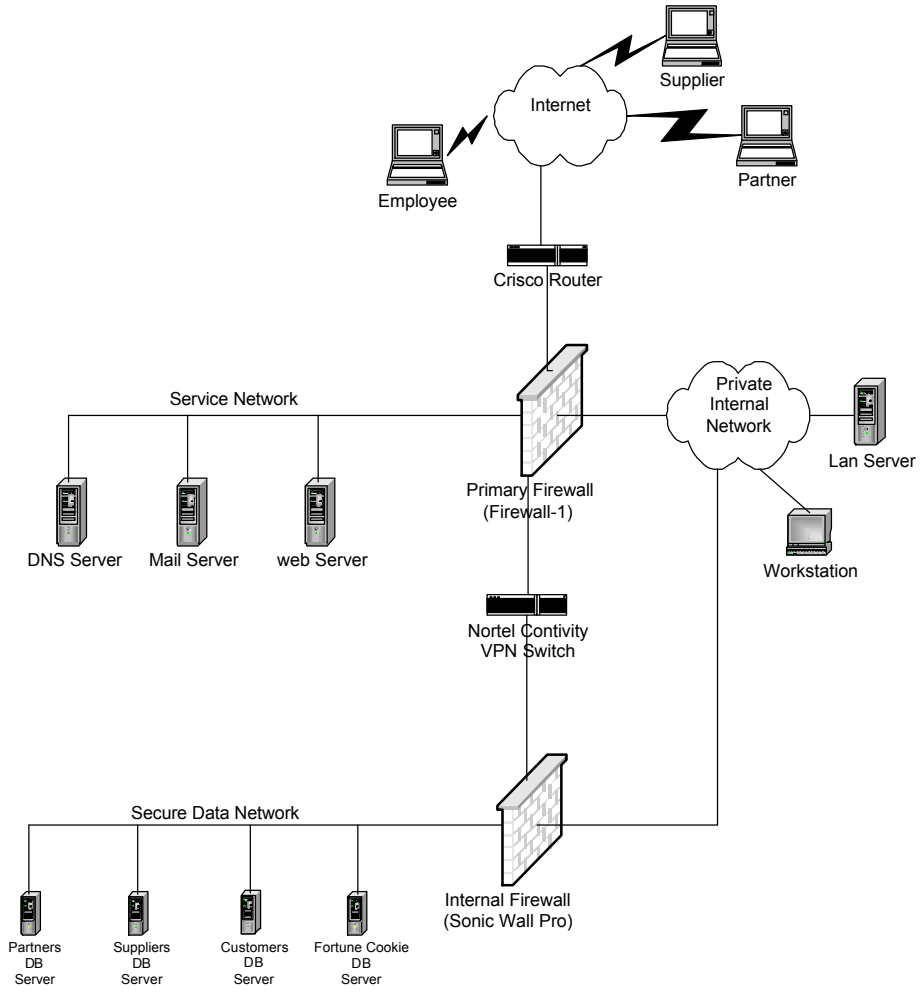
  The new access list would have the following format

```
ip access-list 111 deny tcp any x.y.z.65 0.0.0.0 eq 22
ip access-list 111 deny ip 192.168.0.0 0.0.255.255 any
ip access-list 111 deny ip 172.16.0.0 0.15.255.255 any
ip access-list 111 deny ip 10.0.0.0 0.255.255.255 any
ip access-list 111 deny ip 169.254.0.0 0.0.255.255 any
ip access-list 111 deny ip x.y.z.0 0.0.0.255 any
ip access-list 111 permit ip any any
interface s0/0
    ip address x.y.z.1
    ip access-group 111 in
```

Design Under Fire

I have chosen to examine the practical of Said Nurhussein (Nurhussein, 2000)

Here is a diagram of his network and a brief description of the components:



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.

Attack The Firewall

After checking SecurityFocus and the Checkpoint websites there only appear to be a few known security vulnerabilities discovered which affect Firewall-1 V4.1 SP3, the version of Firewall-1 chosen by Said Nurhussein. In looking at those vulnerabilities, however, most of them aren't really very interesting: (Check Point, 2001),(Security Focus, 2001)

- The GUI Buffer Overflow can only be perpetrated by an "Authorized GUI client".
- The GUI Client Log Viewer Symbolic Link Vulnerability requires that you be a valid administrator who using the log viewer.
- The Format Strings Vulnerability is a typical buffer overflow style attack with the caveat that it can only be perpetrated by a "valid firewall administrator connecting from an authorized management client".
- The RDP Header Firewall Bypassing Vulnerability only allows you to sneak traffic through the firewall on port 259 which isn't and really a direct attack on the firewall per se.

Fortunately (or unfortunately) there is a Firewall-1 denial of service vulnerability that could be problematic in this particular example. We do have to make a few assumptions though:

Assumption 1 – The checkpoint firewall is a limited license firewall (say 250 users).
Assumption 2 – Tunnel mode VPN's are being used between the Business Partners and GIAC Enterprises.

This vulnerability occurs because of the way Checkpoint licensing is enforced in their later versions of Firewall-1. One interface on the firewall is designated as the external interface. All other interfaces are considered to be internal interfaces. The source IP address on every packet of data inbound to any of the internal interfaces is examined by Firewall-1. Firewall-1 records each unique source address it sees arrive on any of these interfaces. As soon as the number of unique source IP addresses exceeds the number of licensed users, Firewall-1 starts generating log messages for new IP address it notices, and it does so every time it notices it. This is capable of generating a very large number of messages and driving the load on the firewall so high that it becomes unusable.

To attack the GIAC Enterprises network the way it is designed, I would first attempt to compromise a system at one of GIAC's Business Partners. Then I could use any tool,

such as synk4.c, that could generate lots of network traffic with different spoofed IP addresses and direct them to the internal interface of the GIAC Enterprises primary firewall. My spoofed traffic would "ride the VPN" to the Contivity Switch sitting behind the Checkpoint firewall and get routed to the internal interface of the firewall. In just a short amount of time, we should be able to drive the CPU to 100%.

DOS Attack against the Firewall

With so many high speed "zombies" at my disposal, I would attempt a denial of service against the firewall-1 state table. By default the state table on a Firewall-1 can only contain 25,000 entries. When you cross that threshold, no new connections can be made through the firewall until the number of connections falls back down below 25,000, resulting in a denial of service. To drive the number of connections to 25,000 you could configure 1/3 of the zombies to repeatedly attempt to connect to the web server on port 80, allow the 3 way handshake to complete and then just keep the connection open until it times out. You would configure another 1/3 of the zombies to attempt the same thing over port 443 to the web server, and configure the remaining 1/3 to attempt the same thing over port 25 to the SMTP server. Since you are creating a new connection attempt each time with a different source port, the firewall will have to build and maintain keep a separate entry in the state table until the session times out and gets reset or 1 hour (whichever is less) which is the default firewall-1 TCP timeout value.

Since there are 50 zombies and only room for 25,000 entries allowed in the state table, each zombie only has to create and keep 25,000 / 50 or 500 sessions.

Lets be generous and assume that it takes 200 bytes of upstream data to establish a single connection, that's 1600 bits of data per connection.

Since each zombie needs to create 500 of these connections at 1600 bits per connection for a total of 800,000 bits of data. Lets call that 800Kb.

Since most cable modems give you 256Kb/sec of upstream bandwidth it should take just a few seconds or possibly minutes (depending on latency issues) to fill up the state table and start causing all kinds of problems.

There are several things you could try as a countermeasure:

- You could increase the number of connections allowed in your state table. Phone boy explains how to accomplish this at http://www.phoneboy.com/faq/0289.html
- You could decrease the firewall-1 TCP timeout value to 15 minutes
- You could block the source IP's at the perimeter router.
- You could try to get the ISP to block the activity or disable the user's cable modem connection since the source IP's are not spoofed.

Note that SYN Defender will not help since these are established connections.

Attack Through The Firewall

Again, probably the easiest way to compromise the internal network is through the IPSec VPN tunnel that comes from the business partners. Assuming that you are able to compromise a system at one of the business partners, you would be able to ride the VPN tunnel right through the primary firewall to the Contivity switch, where your initial VPN tunnel would terminate. But since the Contivity switch appears to have an unrestricted IPSec VPN tunnel which terminates inside the Sonicwall secondary firewall, you would have an encrypted and unrestricted hacking tunnel right through both firewalls, that would give you complete access to the (in)Secure-Network. The encrypted tunnel would make sure that their IDS system would never detect the intrusion attempt. With unrestricted network access of this kind right onto the secure network it's just a matter of time until you find an exploit for one of the servers that reside there. From the secondary firewall rulebase we can tell that at least 1 of these database servers is probably running a web server. Although the paper is not clear on the specific version of SQL and WWW servers are in use, It's really just a matter of scanning the systems to determine what kind of systems they are and what kinds of services they are running and then simply locating the exploit scripts or vulnerability alerts for the service in question. Maybe we get lucky and there's a Microsoft web server back there… GAME OVER.

References

SANS Institute. (2000). Windows NT security step-by-step. Bethesda, MD: SANS Institute.

SANS Institute. (2001). Windows 2000 security step-by-step. Bethesda, MD: SANS Institute.

SANS Institute. (2000). Securing Linux step-by-step. Bethesda, MD: SANS Institute.

SANS Institute. (2000). Solaris Security step-by-step. Bethesda, MD: SANS Institute.

Scambray, J., McClure, S., & Kurtz, G. (2001). Hacking exposed: Network security secrets & solutions (2nd ed.). Berkeley, CA: Osborne/McGraw Hill.

Check Point Software Technologies Ltd. (2001). Alerts Archive [Web Page] URL http://www.checkpoint.com/techsupport/alerts/

Deraison R. (2000). Nessus Documentation [Web Page] URL http://www.nessus.org/documentation.html

Fyodor. (2001). Nmap network security scanner man page [Web page] URL http://www.insecure.org/nmap/nmap_manpage.html

Hall, T. (2001). Licensing Firewall-1 DoS Attack. [NTBUGTRAQ Newsgroup posting] URL http://www.securityfocus.com/archive/1/3A66843F.3AF46534@rootgroup.com

Moe A. J. (2001). SANS GIAC Firewall and Perimeter Protection Practical Assignment [On-Line Word Document] URL http://www.sans.org/y2k/practical/Alan_Moe_GCFW.doc

Nurhussein, S. (2000). Practical Assignment For GIAC Firewall and Perimeter Protection [On-line Word Document] URL http://www.sans.org/y2k/practical/said_nurhussein_gcfw.doc

Payne A. (2000). SANS GIAC Firewall and Perimeter Protection Practical Assignment [On-Line Word Document] URL http://www.sans.org/y2k/practical/Adam_Payne.doc

SecurityFocus. (2001). Vulnerabilities - Check Point Firewall-1 [Web Page] URL http://www.securityfocus.com/cgi-bin/vulns.pl?vendor=Check+Point+Software&title=Select+One&version=Any&section=vendor&which=vendor

Spitzner L. (2000). Auditing Your Firewall Setup [Web Page] URL

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

Spitzner L. (2000). Understanding the FW-1 State Table [Web Page] URL http://www.enteract.com/~lspitz/fwtable.html

Spitzner L. (2000). Armoring Linux [Web Page] URL http://www.enteract.com/~lspitz/linux.html

Spitzner L. (2000). Armoring NT [Web Page] URL http://www.enteract.com/~lspitz/nt.html

Spitzner L. (2000). Auditing Your Firewall Setup [Web Page] URL http://www.enteract.com/~lspitz/audit.html

Spitzner L. (2001). Armoring Solaris [Web Page] URL http://www.enteract.com/~lspitz/armoring.html

Welch-Abernathy D. (2001). Increasing Number of Connections Allowed [Web Page] URL http://www.phoneboy.com/faq/0289.html