# Global Information Assurance Certification Paper

# GCFW Practical Assignment

Jim Hurst

SANS Baltimore, 2001

Version 1.5e

# GCFW Practical Assignment

Jim Hurst

SANS Baltimore, 2001

**Version 1.5e**

**August 9, 2001**

## Introduction

This paper is a practical assignment for the SANS Firewalls, Perimeter Protection, and VPNs course. Its purpose is to demonstrate an understanding of the course material. The paper is broken into four separate assigments. First, a security architecture is presented for the fictitious corporation GIAC Enterprises. Next, a security policy is presented for that architecture. The third section is an audit of the security architecture. The final task is to examine a previously posted GCFW practical, and design attacks against it.

## Assignment 1: The Security Architecture

In an age of global corporations operating 24-7, network security becomes increasingly important. GIAC Enterprises is a fictitious "dotcom," a corporation whose business is entirely based on electronic commerce. Because the assets and products of the company are almost entirely information, GIAC Enterprises (GE) requires strong security. However, the business model has a built-in tension against security: customers and suppliers also require access to the network, and their security practices are outside the control of GE. The contrasting goals of preventing unwanted access while at the same time providing access to specific parts of the corporate network to business partners will be addressed by compartmentalizing the network, and using two factor authentication to control access to the different components.

The security architecture is in many ways indivisible from the network architecture – the two are thoroughly interwoven. The goals for the security architecture, however, remain the basics: the confidentiality, availability, and integrity of the GIAC systems and data.

### Architectural Overview

The security architecture will be referred to as the GIAC Enterprises Network Infrastructure (GENI). Customers, suppliers, business partners, and employees all have unique access requirements. GENI must provide secure remote access both via phone and internet. The perimeter must be controlled and monitored via firewalls. Traffic must be routed between various parts of the organization. Internal corporate subnets must be protected from both internal and external attack. Monitoring, intrusion detection, and integrity verification are necessities. The guiding philosophy will be defense in depth: the defenses will consist of mutually supporting layers. Intrusion detection and response reinforce the defenses by giving GENI the ability to respond and adapt to changing threats.

Most organizations will have natural "breaks" in their network architecture corresponding to company divisions. GE is divided into four divisions: Sales, Purchasing, Finance, and Engineering. Although the computational requirements of the divisions are likely quite varied, for the purposes of this paper they will be considered identical and interchangeable corporate

subnets. A fifth internal network is the recent corporate acquisition, Sitting Duck Software (SDS).

**The Components**

The GENI can be decomposed into a set of interlocking components. After defining the individual components, they are examined in more detail.

The most obvious piece of the security infrastructure is the internet interface. This is an area of high risk and high maintenance: the primary firewalls for the organization. The rules applied will change regularly in response to changing business requirements. Hacker probes and attacks occur here on a routine basis.

The next component is the DMZ (a military acronym that originally stood for demilitarized zone). The DMZ is that part of the network that is visible to the outside world. The GIAC Engineering DMZ contains all externally visible servers in the giac.com domain (that is, all GIAC servers identified by the external GIAC DNS service). While all of the servers in the DMZ have internet routable IP addresses, only a handful of GIAC systems outside the DMZ do.

Another piece of the puzzle is remote access. GE must support secure remote access both via dial-up modems and the internet. A Cisco AS 5300 Remote Access Server will provide modem access. Virtual private networks managed by the external firewalls will provide internet access.

After deliberation, GIAC Enterprises has decided to run their Virtual Private Networks off the external firewalls. This means that encrypted traffic is not allowed on the internal corporate network. The GENI staff demanded to be able to scan incoming traffic for attack signatures, and this is impossible when the traffic is encrypted.

While access to the corporate network is controlled by the external firewalls, access within the network will also be controlled. An internal firewall will separate each of the four internal subnets from the rest of the internal network.

Backups are not always considered a part of the security infrastructure, but they should be. GIAC Enterprises considers disaster recovery an essential part of the infrastructure. To effectively back up numerous servers on different subnets, GENI has chosen to deploy a small backup server for each subnet.

Because GIAC must be prepared for a major disaster, the subnet at Sitting Duck has been designated as an off-site backup data center. So the SDS subnet requires considerable duplication of the GIAC infrastructure, including its own internet line and remote access server.

The final piece of the architecture is the NOC, the Network Operation Center. In the NOC

are the log servers, the integrity checker servers, the Radius servers, and the firewall management station. The NOC is the heart of the security infrastructure: it is here that the security staff monitors network operations, detects and foils attacks, and reacts to incidents. The next sections look at these pieces in greater detail.

The next page shows a network diagram of GENI. IP addresses are given for the external systems, but nearly all of the internal systems have private, non-routable addresses. These addresses are not displayed on the diagram.

### The Internet Interface

GIAC Engineering has acquired two high-speed ATM lines. These lines are connected to the corporate network by a pair of Nokia 440 firewall appliances, running Checkpoint Firewall-1 version 4.1. The Nokia 440s are also supplied with VPN cards, capable are managing many dozens of encrypted sessions at once.

Because GIAC Engineering has multiple connections to the internet, it is a requirement of the ISP that GE run the Border Gateway Protocol on its connections. The Nokias all run BGP.

The GIAC Checkpoint deployment is distributed, that is, the firewall is broken into Enforcement Points (the actual firewalls themselves, that do all the work) and a single Management Station, which downloads the rulesets to be applied to the Enforcement Points. The Management Station is a Solaris box residing in the NOC.

The strength of this arrangement is that the Nokias are attack resistant (they are alleged to be running a hardened version of OpenBSD, already the most secure flavor of UNIX). While security through obscurity is of limited value, the list of known attacks on Nokia firewalls is very short. Even if the Nokias are compromised, the attacker cannot easily change the ruleset to bypass the firewall, because that is only allowed from the Management Server.

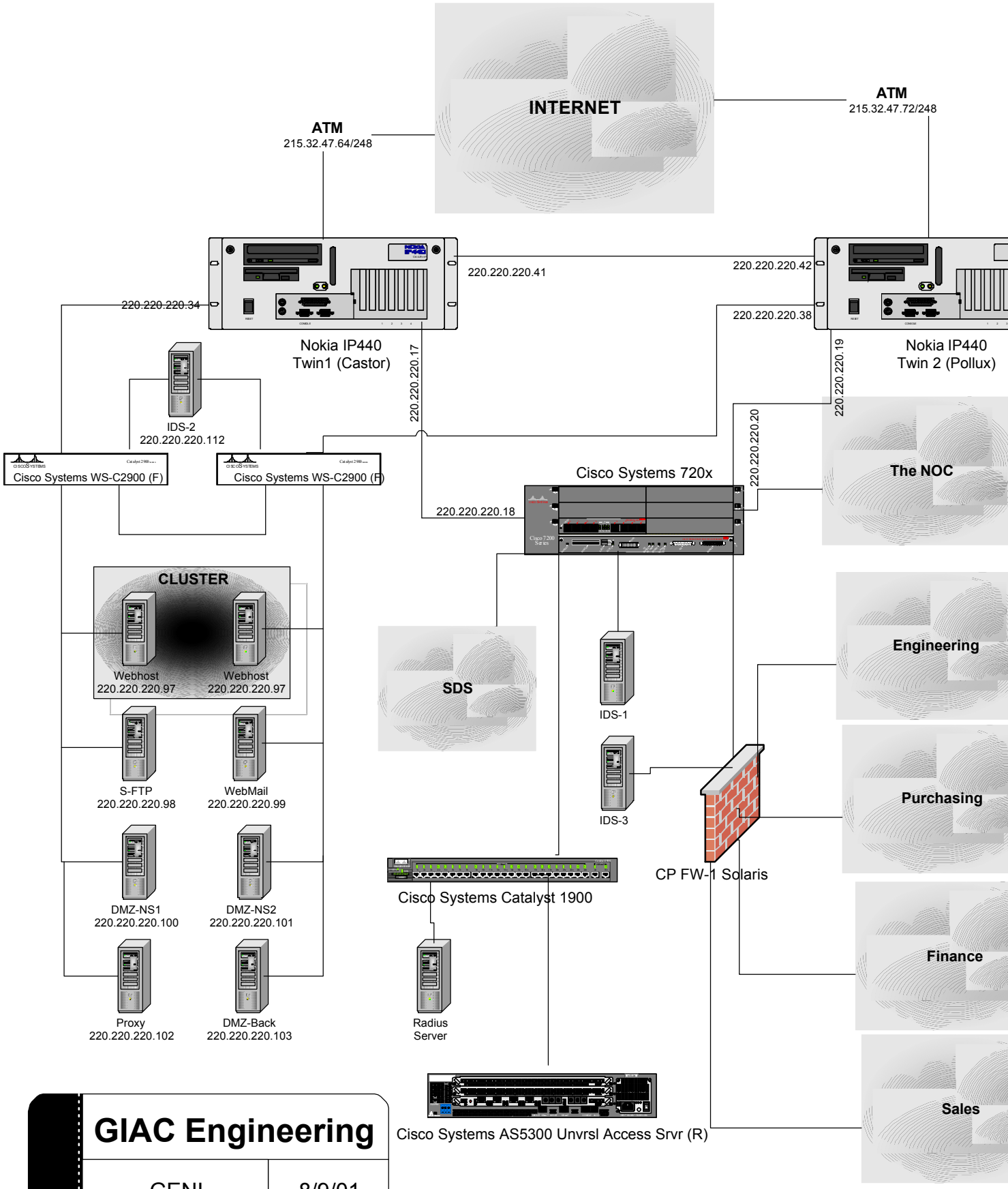
### The DMZ

Next to the internet interface, the DMZ is the area most at risk to external attack. The machines have internet routable IP addresses, and (with the exception of dmz-back) have internet name resolution via the GIAC DNS servers. The GIAC DMZ consists of several distinct and independent servers: the main GIAC web host www.giac.com (aka webhost.giac.com, aka giac.com, it is actually a cluster of Solaris boxes), the S-FTP server sftp.giac.com, the proxy application server proxy.giac.com, the mail server mailhost.giac.com (which is actually just a relay to the real mail server, MailBox) and the webmail server webmail.giac.com.

All of these systems are considered to be at high risk of compromise, so they have been designed specifically for this role. In particular, all Solaris machines have been treated

with YASSP (Yet Another Solaris Security Package) to turn off all unneeded services. The single windows box has been hardened according to the SANS guidelines for Windows NT [1] .

Command line access to these systems is via SSH (the secure shell, essentially an encrypted version of telnet) [2]. File transfer to and from these systems is via S-FTP, which is an encrypted version of FTP. Authentication is accomplished via Cryptocard one-time password generators [3] and the Radius protocol.




# GIAC Engineering

| GENI | 8/9/01 |
|---|---|

All of these systems are considered to be at high risk of compromise, so they have been designed specifically for this role. In particular, all Solaris machines have been treated with YASSP (Yet Another Solaris Security Package) to turn off all unneeded services. The single windows box has been hardened according to the SANS guidelines for Windows NT [1] .

Command line access to these systems is via SSH (the secure shell, essentially an encrypted version of telnet) [2]. File transfer to and from these systems is via S-FTP, which is an encrypted version of FTP [2]. Authentication is accomplished via Cryptocard one-time password generators [3] and the Radius protocol.

There are several things going on in the DMZ. Proxy is an application firewall, providing external services (and NAT, network address translation) to internal corporate users, and is a key part of the security infrastructure. The webhost and S-FTP servers provide services to the internet at large, including browsing, e-commerce, uploads, and downloads. The boxes mailhost and webmail, provide for incoming and remote-access mail, respectively, as securely as possible, by serving as relays between the internet and the internal network. The intent here is to compartmentalize these high-risk hosts, so that compromise via one service or another does not impact the other services being offered. Finally, the backup server, dmz-back, does daily backups on the DMZ machines. It is not accessible to the internet, but is placed in the DMZ subnet to limit traffic between the DMZ and the internal network. One large server could probably accomplish most of these tasks, but several smaller servers provide for defense in depth.

The webhost runs the Apache webserver, along with the Tomcat servlet manager. It is a locked down system specifically designed to be resistant. Management occurs via SSH. It runs no other services beyond HTTP, HTTPS, and S-FTP, although people regularly complain that it should run FTP. Educating customers about the risks of cleartext file transfer is one of the onerous duties that has been delegated to the security staff.

The proxy application server, proxy.giac.com, runs the iPlanet proxy server. Normal users route their internet through the proxy server. It performs NAT, and prevents internet usage from providing user details to the outside world.

The S-FTP server is a major clearinghouse for data into and out of the organization. Customers pick up packaged fortunes here. Suppliers drop off raw fortunes. Again, SSH is used for management, S-FTP is used for transfer, and Radius for authentication. The S-FTP server is one of the most critical pieces of infrastructure, because it is responsible for the delivery of finished product to customers, and the receipt of raw materials from suppliers. This server is actually a cluster of Sun Enterprise systems.

The Webmail machine is the only Windows machine in the DMZ. It is a Microsoft Outlook Access server, which functions as an outgoing relay for mail. Internet users who authenticate via CryptoCards and Radius can access their internal email via this server. A

strong case was made within the GENI design team against having any Windows servers. However, the corporate email system was already determined to be Microsoft Outlook. Because external access to email is a design imperative, the GENI team had little choice but to find some way to deliver Outlook mail to internet users. The Outlook Access server offered the least objectionable way to do this.

The machine mailhost is a Solaris server. It accepts incoming mail from the internet, but rather than storing it, it forwards it to the corporate mail server inside the firewall. This two-piece server approach reflects the fact that the DMZ machines are at the highest risk for compromise from outside. Therefore, the DMZ mail host is not trusted to store mail files, since some of them may be sensitive. It acts only as a virus scanner and mail router. Mailhost also receives automated updates of virus signatures via https regularly.

Finally, two Domain Name Service servers live in the DMZ. These are the authoritative servers for the GIAC Enterprises namespace. They are small single purpose Solaris boxes running bind Version 9.

### Remote Access

The term remote access is often used vaguely. In this context, remote access means dialup users with modems, and home ISDN users. Internet access to email is discussed in the DMZ section, while access to GIAC servers not in the DMZ is accomplished by VPNs, discussed below.

A Cisco AS5300 Remote Access Server (RAS) provides support for dialup users. This device contains 96 56K modems, connected to a single Primary Rate Interface (PRI). Salesmen and remote employees routinely use this modem bank. CryptoCards and Radius provide authentication. It is anticipated that the single AS5300 will be utilized at full capacity early in 2002, and another RAS/PRI pair will be deployed.

Remote users must be defined and authenticated at the Radius server to secure access. This topic is addressed in the Network Operations Center section below.

### Virtual Private Networks

Home users and certain business partners require access to other parts of the internal corporate network. This is accomplished by encrypting traffic between the GIAC corporate network and remote networks or clients.

A virtual private network works by establishing an encrypted session between two endpoints, which may be either individual systems or networks. Because the traffic between the endpoints is encrypted, sensitive information can then be sent across insecure channels. In GENI, the local endpoint for the encrypted session will be the Nokia firewalls at the internet interface. Checkpoint's VPN software VPN-1 is used, along with the SecuRemote client.

The VPN bandwidth achievable by the Nokias is enhanced by the addition of dedicated processor cards for VPN encryption/decryption. This gives each firewall an effective bandwidth of 10 Mbps of encrypted traffic, which is anticipated to be adequate for the next 24 months.

There are advantages and disadvantages to this approach. On the plus side, in this configuration, the firewall can regulate all traffic, so it does not have to "pass" on encrypted traffic. It is cheaper not to have to purchase another dedicated device, and there should be no NAT problems. On the minus side, this put high demands on the firewall/vpn boxes, and it makes it harder to change vendors when the systems are tightly coupled.

In the end, it was decided that the risk of encrypted traffic inside the corporate net was too high, because it makes it too easy to defeat the intrusion detection systems. With the decryption occurring at the perimeter, the IDS can scan the incoming traffic for attack signatures.

In deploying a VPN, administrators must define the encryption domain, which is the set of systems behind the endpoint for which traffic must be encrypted and decrypted. Each of the internal corporate subnets, plus SDS, has a defined encryption domain. These encryption domain systems are segmented from the rest of the internal subnet, because they are somewhat suspect, and their traffic with the internal network is more closely controlled.

When a SecuRemote client attempts to establish an encrypted session with a system in the encryption domain, the client and the firewall/vpn do the necessary handshaking to establish an encrypted session. The authentication part of this protocol depends on one-time passwords, again using CryptoCards and Radius.

### Internal Firewalls

The internal network is perceived to be a much safer place than the wild and wooly internet, or the frequently attacked DMZ. But this perception may be unfounded, because many if not most attacks come from inside. While most employees are trustworthy, employees have a huge advantage over hackers in compromising systems, and that is access. Most employees have daily access to computing resources, and physical access as well. They have opportunities to shoulder surf, read and pilfer passwords on sticky notes, rummage through desks and trashcans, and eavesdrop.

The GENI recognizes this. It is impossible to achieve perfect security on the internal network. Instead, GENI compartmentalizes the internal network, and attempts to monitor and prevent attacks both within and between departments. This is done by a set of internal firewalls, between the main corporate routers and each division. The ruleset varies from firewall to firewall, but essentially discourages unapproved access from one

division to computational resources within another.

These firewalls are also Checkpoint Firewall-1. However, in an effort to reduce the chances of firewall compromise, these internal firewalls run on Solaris machines. The theory here is that most firewall vulnerabilities are problems with the underlying operating system. By using different OS's for the two layers of firewall, OS specific vulnerabilities provide less potential for compromise. This provides some degree of security, while only requiring expertise on a single firewall.

### Intrusion Detection

Without intrusion detection, attackers have the luxury of footprinting, scanning, and attacking a network at their leisure. GENI uses a set of network based intrusion detection systems hanging off switch ports placed in promiscuous mode. These intrusion detection systems use SNORT, and send their logs to a log server in the NOC. While SNORT is not the fanciest IDS available, it is cheap, easy to extend, and signatures become available for it very quickly.

Integrity checking is a host-based form of intrusion detection. Integrity checkers monitor the state of a server, and look for changes from a known good system. GENI uses the Tripwire integrity checker to monitor key systems and record any relevant changes to log servers located in the NOC.

### The Network Operations Center

The final piece of the architecture is the Network Operations Center. The NOC is the home base of the MIS team, a part of the engineering division. This is the place where the security infrastructure is monitored and controlled. The pieces in the NOC include the Firewall-1 Management Server, the CiscoSecure/CryptoAdmin Radius server, the Tripwire Management Station, the network timeserver, and log servers for numerous unix boxes, firewalls, routers, and intrusion detection systems. The NOC is the sanctum sanctorum of security – very little traffic besides logging is allowed in. Physical access is required to access certain pieces of infrastructure. One handy piece of infrastructure in the NOC is a set of terminal servers that provide console access to the UNIX servers in the NOC. The terminal server provides direct access to key servers from a small set of IP addresses for MIS personnel.

This concludes the discussion of the security architecture. The GENI architecture uses compartmentalization, defense in depth, and monitoring to make GIAC an attack resistant environment.

## Assignment 2: The Security Policy

Assignment 2 is to define a security policy for the architecture developed in Assignment 1. Policy in this context is not the corporate security policy, but the firewall rules and access control lists for the various components. Policies will be analyzed for three pieces of the network infrastructure: the border routers, the primary firewall, and the VPNs.

### Security Policy for the Border Routers

The GENI situation is somewhat unusual in that the border router and firewall functions are performed by two applications running on a single box. Typically, they would be separate, perhaps even maintained by different groups. For the purposes of this discussion, they are treated separately, with the router aspects of the appliances discussed here and the firewall aspects discussed next.

Because of the redundant gateways in GENI, the Nokia firewall appliances are required to run BGP, the Border Gateway Protocol. BGP works to automatically keep separate autonomous systems informed of the available network routes. Unfortunately, it does not require authentication before accepting updates, so that an attacker could send spoofed routing information, in particular, crafted routing updates, and make hash out of GENI's network connectivity. Denial of service and perhaps even nastier attacks could be launched this way, so insuring the integrity of the router is the first access control list issue. Next, telnet access to the Nokias will be limited to the NOC.

GENI will prevent spoofing from internal systems, as part of being a good internet citizen. No one but DMZ addresses (220.220.221.96/27) can talk thru the DMZ interfaces, and no one but the designated-access internal subnet can talk thru the interface to the main internal router. No one can use GENI internal addresses from outside. The term designated-access internal subnet refers to the small group of non-DMZ internal systems that actually have externally routable IP addresses (discussed more in the next section). Most of the internal systems never access the internet except via proxy (in the DMZ), but a handful of systems will need full access. These handful are in the designated access subnet, 220.220.220.64/27 (usually as a secondary IP address, their primary address remains in whatever local subnet they belong to).

All traffic not mentioned as being blocked above will be permitted by the routers.

These rules will be enforced with access control lists in the Cisco IOS language. An access control list can permit or deny traffic based on IP address, source, destination, port (service), and several other categories. An access control list is applied to a single interface on a routing device. Order is important within the list, because processing ends after the first match. Every access list ends with an implicit default deny, so that anything that is not explicitly permit in the list is denied. The details of the access lists will be supplied for only the first Nokia. The second will have similar lists applied to the same interfaces, but with different IP addresses.

The border routers have four interfaces: the twin router, the internet, the DMZ, and the main switch. Each of these will have its own access list.

The first access control list controls the internet interface. First, allow only BGP updates from our ISP's designated subnet of 215.32.47.64/29 so that spoofed BGP updates can't sneak in. Second, block all other telnet traffic. Third, allow everything else. The list then becomes:

```
ip access-group 150 in
access-list 150 permit tcp 215.32.47.64 0.0.0.248 220.220.220.6 0 0.0.0.0 eq 179
access-list 150 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 23
access-list 150 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

This list is applied to the internet interface (for the present purposes, serial 0), as follows:

```
interface serial 0
ip access-group 150
```

The next access list is for the DMZ interface (Ethernet0). No BGP traffic from the DMZ will be allowed outside the DMZ. Only traffic from the DMZ's address block will be allowed out.

```
ip access-group 160 in
access-list 160 deny tcp 220.220.221.96 0.0.0.224 0.0.0.0 255.255.255.255 eq 179
access-list 160 permit ip 220.220.221.96 0.0.0.224 0.0.0.0 255.255.255.255
```

The list is applied to interface Ethernet 0 (aka 220.220.220.34) like so:

```
interface Ethernet 0
ip access-group 160 in
```

The next interface to consider is the serial interface between the two Nokias. Because they're in the same autonomous system (a Cisco grouping concept), they must talk with each other. Nothing should be allowed over this interface except traffic from the twin. This list for the first router is:

```
ip access-group 170
access-list 170 permit ip 220.220.220.42 0.0.0.0 220.220.220.41 0.0.0.0
```

(the second router uses the same list with the source and destination reversed)

and it is applied with:

```
interface serial 1
ip access-group 170 in
```

The final access list on the border router is on interface Ethernet 2, which connects to the main internal route/switch module, a Cisco 7200. Only BGP traffic from SDS is allowed in through the interface (220.220.220.64/27). Any traffic is allowed out through the interface, so there is no access list. The incoming list is:

```
ip access-group 180 in
access-list 180 permit  tcp 220.220.222.64 255.255.255.224 0.0.0.0
255.255.255.255 eq 179
access-list 180 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 179
access-list 180 permit ip 220.220.221.96 0.0.0.224 0.0.0.0 255.255.255.255

interface Ethernet 1
ip access-group 180 in
```

This concludes the discussion of security policy for the border router.

**Security Policy for the Primary Firewall**

The primary firewall is perhaps the most critical piece of infrastructure at GIAC Enterprises. The company's product is information, and the firewall is the primary guardian of this information. By default, nothing is permitted, so only the services that are specifically allowed in the section can pass the firewall.

Before getting to specific rules, some generalities must be discussed. GENI is not a conglomeration of workstations and servers, but a structured system. Most of the computer systems exist within functionally defined subnets, so the groupings reflect both a system's function and its address(es). While the groups discussed here all have well-defined subnets, they will be referred in this section by name rather than IP subnet, because that is how the firewall rules have been set up. Firewall-1 requires network objects to be defined before being used in the ruleset.

One obvious group is the DMZ (theDMZ in the ruleset), the collection of systems tainted by their exposure to the dangerous outside world. The NOC (theNOC) is a much more secure grouping. Remote access users receive IP addresses from the AS5300 in the address range referred to as theRASnet. The two firewall machines are known in the ruleset as theTwins.

The firewall ruleset must also cover the corporate assets as well as the network infrastructure (it's important to remember that GIAC Enterprises exists to make money, not to support a security infrastructure!). The firewall has four defined objects for each of the corporate divisions: the entire group, the set of all servers, the subset of division servers accessible via the VPN, and the set of all user machines in the division. For examples, the groups in the Sales division are AllOfSales, SalesServers, Sales_ED (the Sales division Encryption Domain), and SalesUsers. Finance, Engineering, and Purchasing all have similar groupings. Sitting Duck Systems has only the defined group SDS and the

group SDS_ED. With the exception of the encryption domains, these internal groupings are used primarily in the internal firewalls.

Not all network objects exist in the same subnet. For example, Radius servers exist both in the NOC and in the offsite backup facility at SDS, but they are also grouped as radiusServers.

The corporate network provides numerous services. Radius servers provide authentication. DNS servers exist both inside the corporate network and in the DMZ (the DMZ servers can only resolve names inside the DMZ, whereas the internal corporate nameservers know the names of all resolvable servers). The mailhosts, both internal and DMZ provide SMTP and POP services. The services and the servers where they are available must also be defined to the firewall.

Another set of firewall objects are the users and user groups. The group of users who are privileged to access email via the internet are in the group RemoteMailUsers. The group of users who can access the Sales VPN are in the group Sales_VPN_Users, with the other divisions having equivalent groups. Users who will belong to one of these groups must be defined in the firewall according to a set of templates.

The Checkpoint Firewall-1 product works by applying a ruleset to an enforcement point. The enforcement point is the gateway system linking two networks, in this case, the twin Nokias. The ruleset is the list of processing instructions for traffic. The implied last rule in any Firewall-1 ruleset is a default denial, that is, anything that is not explicitly allowed is forbidden. Firewall-1 operates on users, groups, and services. Services may be user defined, and may be aggregations of single services as well. A Firewall-1 rule consists of a source, a destination, a service, and an action (there are additional parameters such as logging, gateway to apply the rule to, and time of day, but for the present purposes, the basics are sufficient). The two Nokias are symmetric, so the same rulesets will apply to them. The source in a rule is the computer or network where the traffic originates, while the destination is the system or network where the traffic is headed. The service represents the port number. Firewall-1 can be “tricked” by sending non-standard types of traffic across well-known ports. Generally, that is not a major risk, since an SSH server won’t make much sense of HTTP requests but it can be used to provide for covert channels. The action is what to do with the traffic: accept, reject (that is, reply that the firewall is blocking this traffic), drop (just drop it with no reply), client encrypt (apply VPN encryption/decryption), user authentication, and a few more obscure options.

The ruleset for the SDS firewall is very similar, but is not described here.

Table 1, below, summarizes the Primary Firewall Ruleset. Individual rules are explained below.

| Rule No. | Source | Destination | Service | Action |
|---|---|---|---|---|
| 1 | Any | theBlackHole | Any | Drop |
| 2 | thePests | Any | Any | Drop |
| 3 | Any | Any | NBNoise | Drop |
| 4 | Any | theNOC | Any | Drop |
| 5 | theNoc | Any | Any | Accept |
| 6 | Webhost | WebDataServers | SqlNet | Accept |
| 7 | RemoteUsers | Webmail | HTTPS | UserAuth |
| 8 | MailBox | Webmail | MailService | Accept |
| 9 | Any | MailHost | MailServices | Accept |
| 10 | MailBox | Any | MailServices | Accept |
| 11 | Any | Webhost | WebServices | Accept |
| 12 | Any | NameServers | DNS | Accept |
| 13 | NameServers | Any | DNS | Accept |
| 14 | GIAC_Inside | Proxy | ProxyServices | Accept |
| 15 | Proxy | Any | ProxyServices | Accept |
| 16 | RadiusServers | theTwins | Radius | Accept |
| 17 | theTwins | RadiusServers | Radius | Accept |
| 18 | SDS | GIAC_Internal | Any | Drop |
| 19 | SDS | Any | Any | Accept |
| 20 | theDMZ | timeServer | NTP/NNTP | Accept |
| 21 | theDMZ | dmzPrinter | Any | Accept |
| 22 | SalesDelivery | SalesPartners | SalesService | Accept |
| 23 | SalesPartners | SalesReceiving | SalesInput | Accept |
| 24 | FTPUsers | Any | FTPServices | Accept |
| 25 | DesignatedAccess | Any | Any | Accept |
| 26 | mailhost | TrendActiveUpdates | Any | Accept |
| 27 | Sales_VPN_Users | Sales_ED | Any | ClientEncrypt |
| 28 | Eng_VPN_Users | Eng_ED | Any | ClientEncrypt |
| 29 | Pur_VPN_Users | Pur_ED | Any | ClientEncrypt |
| 30 | Fin_VPN_Users | Fin_ED | Any | ClientEncrypt |
| 31 | SDS_VPN_Users | SDS_ED | Any | ClientEncrypt |
| 32 | Any | Any | Any | Drop |
| | | | | |

**Table 1: Ruleset for primary firewall**

The ruleset is complex enough to warrant some explanation. An annotated tour follows.

| | **Source** | **Destination** | **Service** | **Action** |
|---|---|---|---|---|
| Rule 1: | Any | theBlackHole | Any | Drop |

theBlackHole is a group of banned sites. Banner-spammers, private VPNS, porn sites – anything that has been judged unacceptable is added to this group. The rule above says that no one inside can talk to sites in the group theBlackHole with any service. The traffic is dropped.

| | | | | |
|---|---|---|---|---|
| Rule 2: | thePests | Any | Any | Drop |

thePests is the group of external sites that have been banned from internal contact. This is the list of hackers who've attacked, known hacker bases, plus a few objectionable networks like competitors. thePests aren't allowed in for any service.

| | | | | |
|---|---|---|---|---|
| Rule 3: | Any | Any | NBNoise | Drop |

NBNoise is the aggregate of NBDatagram, NBName, and NBSession. This is Windows netbios traffic. Windows systems are very chatty, and will fill your firewall logs, so this is a good one not to log. This rule prevents Windows boxes from talking through the firewall.

| | | | | |
|---|---|---|---|---|
| Rule 4: | Any | theNOC | Any | Drop |

The Network Operations Center is not reachable from the outside

| | | | | |
|---|---|---|---|---|
| Rule 5: | theNocUsers | Any | Any | Accept |

The workstations of authorized users in the NOC can go anywhere and do anything. The NOC servers are not in the group theNocUsers.

| | | | | |
|---|---|---|---|---|
| Rule 6: | Webhost | WebDataServers | SqlNet | Accept |

Webhost can talk to the group of database servers WebDataServers through the protocols SQLNet1 and SQLNet2.

| | | | | |
|---|---|---|---|---|
| Rule 7: | RemoteUsers | Webmail | HTTPS | UserAuth |

Selected users can access Webmail via HTTPS to read their email, after Radius authentication using their CryptoCards.

| | | | | |
|---|---|---|---|---|
| Rule 8: | MailBox | Webmail | MailServices | Accept |

MailBox can talk to Webmail with any of the mail services.

| | | | | |
|---|---|---|---|---|
| Rule 9: | Any | MailHost | MailServices | Accept |

Anyone can talk to MailBox with any of the mail services.

| | | | | |
|---|---|---|---|---|
| Rule 10: | MailBox | Any | MailServices | Accept |

MailBox can talk to anyone with any of the mail services.

| | | | | |
|---|---|---|---|---|
| Rule 11: | Any | Webhost | WebServices | Accept |

Anyone can talk to the web server with HTTP, HTTPS, and S-FTP.

| | | | | |
|---|---|---|---|---|
| Rule 12: | Any | NameServers | DNS | Accept |

Anyone can talk to the name servers for DNS name resolution.

| | | | | |
|---|---|---|---|---|
| Rule 13: | NameServers | Any | DNS | Accept |

The name servers can talk DNS to anyone.

| | | | | |
|---|---|---|---|---|
| Rule 14: | GIAC_Inside | Proxy | ProxyServices | Accept |

All internal clients may use the Proxy server for FTP, HTTP, HTTPS, Telnet, GRE, LDAP, and the various RealAudios.

| | | | | |
|---|---|---|---|---|
| Rule 15: | Proxy | Any | ProxyServices | Accept |

And the proxy firewall can forward those requests from inside to anywhere.

| | | | | |
|---|---|---|---|---|
| Rule 16: | RadiusServers | theTwins | Radius | Accept |

The Firewall enforcement points can talk to the radius servers with the radius protocols.

| | | | | |
|---|---|---|---|---|
| Rule 17: | theTwins | RadiusServers | Radius | Accept |

And the Radius Servers can talk back.

| | | | | |
|---|---|---|---|---|
| Rule 18: | SDS | GIAC_Internal | Any | Drop |

Sitting Duck Sytems cannot talk to the various departments (but GIAC internal does not include the DMZ, so SDS can talk to the DMZ via the next rule).

| | | | | |
|---|---|---|---|---|
| Rule 19: | SDS | Any | Any | Accept |

But SDS can talk to the Internet via these gateways.

| | | | | |
|---|---|---|---|---|
| Rule 20: | theDMZ | timeServer | NTP/NNTP | Accept |

The DMZ systems get their times from the network time server timeserver.

| | | | | |
|---|---|---|---|---|
| Rule 21: | theDMZ | dmzPrinter | Any | Accept |

The DMZ systems can print to the printer dmzPrinter

| | | | | |
|---|---|---|---|---|
| Rule 22: | SalesDelivery | SalesPartners | SalesService | Accept |

The designated SalesDelivery servers can talk to the group SalesPartners with FTP, Telnet, SSH, S-FTP, HTTP, HTTPS, and PPTP.

| | | | | |
|---|---|---|---|---|
| Rule 23: | SalesPartners | SalesReceiving | SalesInput | Accept |

The Sales Partners can talk to the SalesReceiving group (which must have routable IP addresses) with the SalesInput services, which include FTP, S-FTP, Telnet, SSH, HTTP, HTTPS, and PPTP.

| | | | | |
|---|---|---|---|---|
| Rule 24: | FTPUsers | Any | FTPServices | Accept |

A small group of users are allowed direct FTP, HTTP, and HTTPS connections.

| | | | | |
|---|---|---|---|---|
| Rule 25: | DesignatedAccess | Any | Any | Accept |

DesignatedAccess is the group of superusers within the divisions, plus assorted brass like the CEO. They are allowed unrestricted access.

| | | | | |
|---|---|---|---|---|
| Rule 26: | mailhost | TrendActiveUpdates | Any | Accept |

The mailhost machine handles the automatic virus updates.

| | | | | |
|---|---|---|---|---|
| Rule 27: | Sales_VPN_Users | Sales_ED | Any | ClientEncrypt |

Sales VPN users who successfully authenticate with the Cryptocard/Radius servers can access the Sales Encryption Domain with any services.

| | | | | |
|---|---|---|---|---|
| Rule 28: | Eng_VPN_Users | Eng_ED | Any | ClientEncrypt |

Similarly for Engineering

| | | | | |
|---|---|---|---|---|
| Rule 29: | Pur_VPN_Users | Pur_ED | Any | ClientEncrypt |

Similarly for Purchasing

| | | | | |
|---|---|---|---|---|
| Rule 30: | Fin_VPN_Users | Fin_ED | Any | ClientEncrypt |

Similarly for Finance

| | | | | |
|---|---|---|---|---|
| Rule 31: | SDS_VPN_Users | SDS_ED | Any | ClientEncrypt |

Similarly for SDS.

| | | | | |
|---|---|---|---|---|
| Rule 32: | Any | Any | Any | Drop |

Rule 32 is the default deny. Anything not allowed by this point is dropped here.

**Testing the Firewall Rules**

Testing this ruleset is a non-trivial undertaking, but it can be done. The key is to understand the source/destination/service triplet that the rules evaluate. With a little creativity, it is possible to create any of these triplets. To test a rule, an administrator must create the appropriate traffic to trigger the rule, and turn logging on for the rule. For example, to test Rule 1 (Source=Any, Dest=theBlackHole, Service=Any, Action=Drop), turn logging on within the rule. Then point any browser at a BlackHole site. The browser should not get through, and the dropped traffic should show up as an entry in the firewall log.

Other rules are somewhat trickier, but still achievable. Consider Rule 2 (S=thePests, D=Any, Svc=Any, Action=Drop). The actual pests lists is outside GIAC control. But an administrator can access a dial-up account, find out its ISP-provided IP address, add that address to the pests list, and then try to access the GIAC webhost. The dialup account should be denied access, and the resulting drop should show up in the firewall log.

In this ruleset, all the rules can be tested either from the inside or from a dialup account, because we do not have special purpose rules for individual outside sites. That is, to test a given rule for outside sites, an outside site under GIAC control (like a dialup) can be added to a group of outside sites, and used for testing. In the case of a rule that targets an individual IP address, rather than a group, it might be necessary to use hacker tools to spoof the IP address of a particular outside site when that outside site is not under GIAC control. NMAP or similar tools are available that can perform this function to varying degrees.

**Security Policy for the Virtual Private Network**

The VPN has been alluded to numerous times in the above discussion. GENI is supporting five separate Encryption Domains (that is, groups of servers accessible via VPN). The endpoints of the VPN are the VPN client on the far end, and the Nokia firewalls. This means that incoming encrypted traffic is decrypted at the firewall, and outgoing VPN traffic from inside GIAC arrives at the firewall where it is encrypted before being sent to its final destination. While this has certain disadvantages, it means that traffic traveling through the internal network is not encrypted, and is thus subject to sniffing by the internal Intrusion Detection Systems. (Because GENI is a switched network, sniffing requires control of the switches, which, because they are Radius protected, is non-trivial). Because traffic on a VPN is invisible to the intrusion detection systems, VPNs represent a large security vulnerability.

The Checkpoint VPN is based upon individual users. A user as defined in Firewall-1 has two sets of properties important to VPN access: authentication and encryption. Our VPN users will authenticate via Cryptocard and Radius. The encryption properties include the choice of FWZ versus IKE as encryption methods, and the use of firewall passwords or certificates as well as issues like whether or not to log successful authentications. GENI uses IKE, with certificates.

The far end of the VPN consists of a client (in our case, a Windows box) running the Checkpoint SecuRemote client. The SR client then sits between the OS and the network interface, monitoring and altering outgoing traffic bound for a site in the encryption domain.

The SecuRemote client is configured by defining the GENI firewalls as a site (which requires nothing more than providing the IP address of the Nokias). When this occurs, the IKE handshaking occurs between the client and the firewall, and a certificate is delivered to the client that will be used for future encryption sessions. When traffic to a

known encryption domain passes, the SR client encrypts it before sending it out.

The Nokia firewall is responsible for encrypting and decrypting the VPN traffic. When it receives encrypted traffic from the outside, it reads the header to determine the client. It then knows how to decrypt the traffic, based on the previous handshake. It decrypts the traffic, and forwards it to the appropriate internal systems. When the firewall receives traffic from an inside encryption domain to a client, it encrypts the traffic based on the previous handshake with the client. If the old handshake has expired, it initiates a new round of handshakes to send a new certificate to the client.

### Testing the VPN

The VPN test occurs in two stages. First, does it *appear* to work? This is accomplished by setting up a client, defining the GENI firewalls as sites, and trying to access one of the defined encryption domains. Assuming that everything appears to be working, then it is time for the second test. This requires running a sniffer on the Nokia firewall (or, if that isn't possible, on a server attached to a switch outside the firewall and receiving firewall traffic through a port set to promiscuous mode). The sniffer is used to isolate traffic between the client and an encryption domain. If the traffic looks encrypted, it probably is. But true fans of encryption might wish to pursue the issue further, and dig the appropriate certificates out of the two endpoints to verify the encryption.

## Assignment 3: Audit the Security Architecture

Assignment 3 is to provide technical support for a comprehensive information systems audit for GIAC Enterprises, in particular to audit the Primary Firewall. There are three parts to the assignment: 1) plan the assessment, 2) implement the assessment, and 3) conduct a perimeter analysis. This assignment will be approached from the perspective of an outside consultant, that is, the team conducting the audit (henceforth referred to as Asbestos Bulwark Consulting, or ABC) are assumed not to be GIAC employees.

### Planning the Assessment

While the first two assignments have been primarily technical in nature, this task has a stronger business component. An outside organization is to provide professional services of a sensitive nature to GIAC Enterprises, so care should be taken to assure that the two parties are in agreement on the contract terms, cost, statement of work, schedule, deliverables, and risks. These terms should be formalized and signed off on by responsible persons on both sides. A signed contract is a must – network scanning and penetration is illegal in many states, and ABC must protect itself. But the contract also represents a shared consensus about the scope of the audit.

When the contractual issues are resolved, it is time to tackle the details of planning the

assessment. Key personnel on both sides must be identified, and they must meet to hammer out the details of the firewall audit. This could be done online, but a face to face meeting is strongly encouraged. The audit is a complex and technical procedure involving potential downtime and consequent loss of revenue, so there should be a clear understanding on both side of what to expect. This is best accomplished by meeting in the physical world, presumably at the GIAC site.

The technical manager from GIAC Engineering responsible for network infrastructure should be present, along with his firewall analyst or security administrator. Other parties from GIAC that may be present are upper level management, network administration, customer advocates (or customer representatives), purchasing advocates (or supplier representatives), and representatives from SDS.

The consultant must bring in a list of issues requiring resolution. GIAC should also bring its issues. In particular, ABC needs to inform GIAC of their requirements for office space and equipment (if any), their schedule (both beginning and end, and time of day), the types of tools that will be used, the potential for disruption from testing, the ABC completion criteria, and what GIAC can expect when the audit is complete. ABC and GIAC should also develop at this point a recovery strategy if GIAC services are disrupted: what should ABC do if unexpected results occur? What is the plan if a server gets destroyed? All systems to be tested should be backed up, and disaster recovery plans in place. ABC must be provided with a set of technical and management contacts available during any hours of active testing. GIAC and ABC must work together to develop a threat model, and a testing plan that addresses the anticipated threats.

Two general approaches to evaluating the GIAC firewall are possible. If ABC knows the details of the policy in advance, this will color the emphasis and direction of ABC's analysis (which is by no means necessarily a bad thing). This approach is the "white-box" approach – the internal details are known before testing begins. GIAC may not wish to share the details of their policy, in which case ABC can make very few assumptions about what they are up against (black-box testing). In this case, GIAC has decided to share the details of their security policy with ABC, in order to have a more focused audit.

With the security policy in hand, ABC must plan the technical implementation. Interviews with key GIAC personnel are recommended at this point. ABC proposed a three pronged audit: scanning/penetration from outside the firewall, scanning/penetration from inside the DMZ, and scanning/penetration from inside one of the corporate subnets (purchasing got stuck with this one). The first case requires no equipment or access. For the second phase, an ABC server (fully equipped with lots of hacking tools) will be dropped into the DMZ. For the third phase, ABC requires a user account on a PC within the purchasing subnet.

The assessment will be implemented by the book, the book in this case being *Hacking Exposed*, by Scambray et al[4]. The first steps, which occur primarily offsite, will be footprinting, scanning, and enumeration.

### Footprinting

Footprinting is the gathering of information about an organization by any means available to create security profile of their networks. Footprinting provides attackers with a systematic way to collect and organize information, and so to draw a picture of their target. *Hacking Exposed* breaks footprinting into the categories internet, intranet, remote access, and extranet.

Tasks in the internet category include identifying network blocks, DNS servers, systems reachable via the internet, services running on each identified system, system architectures and operating systems, IDSes, and access control mechanisms. On each system, identification of users, groups, banners, and routing is targeted.

In the Intranet subtask, ABC will identify networking protocols in use, internal domain names, and subnets. As in the internet subtask, they will also attempt to identify architectures and OSes, listening ports, and users and groups on individual systems.

In the remote access subtask, ABC proposed running wardialers over the corporate PBX. GIAC was initially resistant to the idea, but after internal discussion decided to allow this during non-business hours. ABC will also probe the RAS, trying to identify the system type and authentication mechanisms.

In the extranet stage, ABC will study the corporate VPN, attempting to identify the encryption domains and the technologies used.

The tools used in this stage include network queries from ARIN [5], a search of the whois database for registrar, organizational, and domain info, DNS interrogation, and good old tracerouting to determine network topology.

### Scanning

Scanning is the process of systematically sweeping through a network and identifying live systems. When the list of live systems is complete, then port scans will be applied to each identified system. The end result of this stage will be a list of systems and their associated services, along with auxiliary information about architecture, operating system and version, and versions of different services.

A good scan provides a lot of information about a network, and given the lengthy lists of security vulnerabilities (on BugTraq [6] for example), it offers a lot of avenues of attack.

ABC will implement scanning by running sweeps from non-Windows systems using Cheops [7]. Cheops integrates ping sweeps, traceroutes, port scans, and OS detection. For the Windows machine, ABC will use nmap and netcat. Any switches and routers will be primary targets during this phase, because owning a switch can be quite a handy thing

to an attacker.

### Enumeration

The next step is enumeration, which is the extraction of user account and shared resource information from the systems.

For Windows systems, ABC will look for null sessions, NETBios shares, and domain controllers. Some of the enumeration tools for windows are built into Windows 2000 (like net view and nbstat). For the rest, ABC will use the enum tool from Bindview[8].

For UNIX systems, ABC will use the UNIX utilities finger and rpcinfo, along with shareware netcat and the commercial product CyberCop Scanner from PGP Security [9]. The web site will assessed by crawling it with Sam Spade from Blighty Design[10].

The PhoneSweep product will do the remote access scanning and enumeration from Sandstorm Enterprises[11]. The wardialer will be used to identify all system with modems set to autoanswer.

### The Revised Threat Assessment

With the completion of the footprinting, scanning, and enumeration phases, ABC is now in a position to revise the vulnerability assessment. If GIAC enterprises is at all typical, a variety of attacks will suggest themselves, from brute force password attacks to null sessions to a long list of buffer overflow attacks. The job of ABC at this point is to analyze and correlate the information from the three probes, and develop a list of attacks with a likelihood of success. This list will be presented to GIAC as one of the primary deliverables from the audit.

### Level of Effort

Because ABC is a specialist in this field, the level of effort for footprinting, scanning, and enumeration is reduced. The labor estimates are given below. Three levels of technical skill are used: a junior technician at $100/hour, a senior technician at $200/hour, and a senior analyst at $250/hour. These prices are somewhat arbitrary, but roughly in line with market rates.

| | | | | |
|---|---|---|---|---|
| Footprinting | Junior technician | 3 days @ $100/hr | offsite | $2400 |
| | Senior technician | ½ day @ $200/hr | offsite | $800 |
| Enumeration | Junior technician | ½ day @ $100/hr | offsite | $400 |
| | Senior technician | ½ day @ $200/hr | offsite | $800 |
| | Junior technician | 1 ½ day @ $100/hr | onsite | $1200 |
| | Senior technician | 1 ½ day @ $200/hr | onsite | $2400 |

| | | | | |
|---|---|---|---|---|
| Scanning | Junior technician | ½ day @ $100/hr | offsite | $400 |
| | Senior technician | ½ day @ $200/hr | offsite | $800 |
| | Junior technician | 1 day @ $100/hr | onsite | $800 |
| | Senior technician | 1 day @ $200/hr | onsite | $1600 |
| Wardialing | Junior technician | ½ day @ $100/hr | offsite | $400 |
| Senior Anal. | Senior technician | 3 days @ $250/hr | offsite | $6000 |
| Total: | | | | $18,000 |

The estimated cost is then $18,000 for the revised threat analysis package, plus six person days expenses.

**Implementing the Assessment**

This section will show the methodology used to validate that the primary firewall is actually implementing the security policy as defined in the ruleset above. It is assumed here that the wish of GIAC Enterprises was not to be hacked by ABC (a full penetration test), but rather simply the delivery of the list of eminently hackable targets by ABC from the previous section.

The assessment that GIAC Enterprises desires is rather the validation of the ruleset given above. Due to the (source, source, service) nature of the Checkpoint Firewall-1 ruleset, validation of these rules can be accomplished by repetition of a simple set of steps. First, determine where the source is, and devise a means of either sending the appropriate signals from that source, or spoofing the appropriate signals from that source. Second, determine the destination, and service. Then send signals from the source to the firewall with that destination and service. Verify 1) that the correct action is logged in the firewall log and 2) that the correct action takes place.

Take, for example, Rule 1:

| | | | | |
|---|---|---|---|---|
| Rule 1: | Any | theBlackHole | Any | Drop |

This one is easy, no spoofing is required. The browser on our internal windows box can be pointed at one of the sites in theBlackHole group. The firewall log is then filtered for all entries with a destination of the IP address of the target. A log entry should show with a source of our Windows machine, at the correct time, with an action of drop. Further, the web page of the BlackHole site should not come up on the browser. If these two things are accomplished, the rule is considered validated.

An only slightly tougher case is rule 2:

| | | | | |
|---|---|---|---|---|
| Rule 2: | thePests | Any | Any | Drop |

In this case, both spoofing and an external network address (either from the ABC home

network, or from a dialup account) are required. The use of nmap with a decoy can be used to accomplish this. In decoy mode, nmap sends spoofed IP addresses, so we simply spoof an IP address of one of the pests, and proceed with a port scan. Supposing that 10.10.10.10 is on the pest list, the following command can be used to accomplish rule 2:

```
nmap –D 10.10.10.10 220.220.221.65
```

This will scan host 220.220.220.65 both from our legitimate network address, and with a spoofed address of 10.10.10.10. The firewall should deny both, but the spoofed traffic should trigger a drop from rule 2 for the spoofed traffic appearing to be from thePests. Filtering either on a source address of thePests, or on a rule applied of 2 should show entries for the entire port scan. Nmap should report the failure to scan the host, and the firewall log should have a record of the scan.

Alternatively, an external network address under ABC control can be added to the group thePests, and the verification can proceed from there.

Rule 3 again presents an easy verification job from the inside:

```
Rule 3:          Any          Any                NBNoise        Drop
```

Normally, the logging for this rule would be turned off, to block the ever so chatty windows machines from filling the firewall log with netbios traffic. For validation, log the results of Rule 3, and define a new WINS server on the Windows machine outside the firewall. Do an nbstat of the new WINS server from a Windows command shell like so:

```
nbstat –A 10.10.10.10
```

assuming 10.10.10.10 is the WINS server. Filter on the host ID of the Windows box, and look for the results in the firewall log. The nbstat should fail, and the attempt should register in the log.

Rule 23 is one of the few that requires more spoofing.

```
Rule 23:         SalesPartners   SalesReceiving  SalesInput     Accept
```

Assuming that 40.40.40.40 is one of the addresses in the SalesPartners group, and 220.220.221.65 is in the group SaleReceiving, nmap can be used to validate that the firewall will accept one of the specified connections. The nmap command:

```
nmap –D 40.40.40.40 220.220.221.65 –p 21
```

will spoof FTP traffic (FTP is one of the SalesPartners services) from 40.40.40.40, a legitimate SalesPartners address. The firewall should log and accept this traffic. More complete verification than this (that is, verification by actually using some of the SalesPartners services) will require the cooperation of one of the SalesPartners machines, or adding temporarily adding one of the external ABC workstations to the

SalesPartners group.

This concludes the discussion of implementing the assessment.

### Perimeter Analysis

While the Firewall Assessment identified a set of tactical issues that was a list of vulnerabilities based on specific hardware and software deployments, the perimeter analysis is concerned with the analysis and re-architecting of the perimeter for greater security. These recommendations are generally judgment calls – changes to the existing security architecture have both good and bad points. The list of specific recommendations follows.

The proxy server should be moved out of the DMZ and instead attached directly to the Cisco 720X switch. The primary firewalls should use NAT to offer the proxy machine an additional layer of protection.

Intrusion detection should be beefed up. If possible, IDSes should be implemented on the primary firewall machines, as well as one on the internal firewall. These IDSes should log to the NOC, and sufficient personnel resources should be made available to examine the logs on an hourly basis.

The security components must be checked regularly, and must be kept up to date with software upgrades. A list of relevant vendors and products should be created, and their sites checked for updates and vulnerabilities on a weekly basis, if not more frequently.

The security policy for the recent acquisition SDS should be brought into line with that of the other GIAC Engineering divisions. SDS should connect to the central switch via its own internal firewall, rather than directly.

Each of the divisions should have its own firewall between its internal corporate network and the central switch.

## Assignment 4: Design Under Fire

Assignment 4 is to choose another security architecture, and design attacks against it. It consists of three parts. The first is an attack on the firewall itself. The second attack is a denial of service attack using 50 cable modems. The third attack is a plan to compromise an internal system through the perimeter system.

Designing attacks is conceptually a much different undertaking than designing perimeter defense. Defense is by its nature total – a defense much cover ALL possible attacks, while the attacker will not waste time attacking the entire defense. Attackers are looking

for a single weakness (or a series of weakness through a network). In a sense, the attacker's job is simple. Attackers can afford to be specialists, knowing a lot and spending a lot of time working on a narrow specialty. Defenders, in contrast, are required to be generalists. They must know TCP/IP, routers and routing, Windows, DNS, multiple flavors of UNIX, NFS, Novell, … The areas of possible vulnerability are so broad that maintaining the required skillsets is a challenge.

This paper will use as a target the posted practical of Tomas Alex (http://www.sans.org/y2k/practical/Tomas_Alex_GCFW.doc). This architecture use a Checkpoint Firewall-1, with Cisco routers. The tomasalex.com architecture is very "generic", that is, the components and layout are ordinary. For this reason, the attacks detailed here will be against a generic Checkpoint firewall, and against Cisco routers.

**Attacking the Firewall**

The first attack is against the firewall itself. The target to attack is Checkpoint's Firewall-1. This is the Cadillac of firewalls, an expensive and full featured product from a company that specializes in large corporate firewalls.

The first step is to reseach Firewall-1. There is at least one book on FW-1[12] . A more hackerly approach, however, is to research FW-1 via BugTraq[6]. BugTraq is an open listing of thousands of software holes and vulnerabilities, and is a gold mine of security information.

A search on BugTraq for Firewall-1 yields an interesting list of vulnerabilities. The most recent (July of 2001) is a bypass vulnerability, which doesn't attack the firewall directly. However, there are a few more promising listings. The Firewall-1 Fast Mode TCP vulnerability allows attackers to bypass access controls and access blocked services. This includes services on the firewall itself. For the exploit to run, at least one TCP service on the firewall must be accessible to which a SYN can be sent legitimately. If the firewall is running DNS, NTP, or any other TCP services to the outside world, we can probe all the services on the box, perform TCP stack fingerprinting to determine the OS, and try to crack open one of the services.

This, combined with the footprinting, scanning, and enumeration techniques discussed above, offer a reasonable hope of gaining some sort of access. If the systems administrator is doing his job, the firewall will be regularly updated with the fixes for vulnerabilities posted on BugTraq, and only a short window of opportunity will exist between the posting of the weakness and the availability of a fix from the vender. In the attackers' advantage, however, is the expansion of that window caused by any delay in the deployment of the fix. Systems that haven't been properly upgraded represent the largest set of vulnerabilities on the Internet.

BugTraq offers detailed information on which systems are vulnerable. In our case, we find that the Fast Mode TCP vulnerability applies only to Checkpoint Firewall-1 V 4.1 SP2. If

the systems adminstrator has upgraded to FW-1 V4.1 SP3 , then this attack will fail.

**The Denial of Service Attack**

Denial of service attacks are just too easy at present. While 50 cable modems is not a particularly large number, it's enough to knock a site off the air for awhile. The attack will be a cookie-cutter, script-kiddie knock-off of the series of attacks endured and analyzed by Steve Gibson, the recent victim of a DoS attack. The complete story of his attack is fascinating (and frightening) reading, and can be found at http://grc.com/dos/grcdos.htm.

The bandwidth of the Tomas Alex architecture is unknown, but it is almost certainly below 50 megabits. Assuming we can generate 1 megabit from each of our 50 captive cable modems, it should be relatively easy to swamp Mr. Alex's bandwidth, leaving him with little alternative but to get to know the incident response team at his ISP in a hurry.

Each cable-modem system will be supplied with a remote-controllable server, known as a bot. Each bot sends out a continous stream of huge (64K, the max size) UDP packets (which will get fragmented during delivery to the standard 1500 byte packet) to an arbitrary port on tomasalex.com. This results in a blizzard of fragmented packets, clearly enough to DoS tomasalex.com (or any other system with less than an OC-48 connection). This is a simple brute force flood – nothing tricky or elegant, just strongarming legitimate bandwidth uses into silence.

The countermeasure to this sort of brute force attack is relatively simple. By putting brute force filters on routers upstream that simply block all UDP, the UDP stream can be blocked, and normal TCP traffic will get through. Tomasalex.com pops back up on the internet as soon as the filters are applied at the ISP.

The story would be different if the cable-modem bot-boxes could send TCP packets. Then filtering on UDP wouldn't work, and tomasalex.com would just be off the internet. Raw-socket access for TCP is not currently available on Windows boxes. Steve Gibson is on a bit of a crusade on this at the moment (http://grc.com/dos/winxp.htm) and one is forced to conclude that the expected availability of raw socket access for TCP in Windows XP is a serious threat.

There are DoS possibilities beyond brute force, however. BugTraq lists three Firewall-1 DoS vulnerabilities, the SMTP Resource Exhaustion vulnerability, the 4.1 Denial of Service vulnerability, and the Fragmented Packets DOS vulnerability. The first applies only to FW-1 4.0 and 4.1 on Windows NT (who would run a firewall on NT? That's reason enough to learn UNIX right there!). The second attack is interesting. It tricks the firewall into thinking that many unlicensed addresses are behind the firewall, and swamps the firewall with its own error messages. The third attack is to send illegally fragmented packets to swamp the firewall processing capability.

These vulnerabilities have been fixed in recent upgrades and hotfix service packs. But if tomasalex.com hasn't been doing their firewall upgrades, they may be in serious trouble.

Another serious DoS vulnerability having nothing to do with bots or cable-modems is the risk of a compromised router. One of the fobvious things to try is to compromise tomasalex.com's border router. Cisco works hard to provide secure products (as well they should!), but in June of 2001 a serious vulnerability appeared. The Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability (BugTraq ID 2936) is fresh, and it's big. All Cisco routers of IOS 10.3 and later that haven't had an IOS upgrade since June are vulnerable. If tomasalex.com haven't flashed their router lately, it is an easy takeover target. A compromised router makes it trivial to shut down internet access until the router is upgraded or replaced with an non-vulnerable system.

**Attacking Internal Systems**

To attack systems inside the firewall, one must find a way around the firewall. Armed with the footprinting, scanning, and enumerating data from Assigment 3, the next step is to study Firewall-1 for bypass vulnerabilities. At this point it is expected that a list of employee names is known, along with some or all corresponding account names.

Owning the router could be very useful for attacking internal systems. For example, by corrupting the route table, a great deal of mischief can be done. With a bit of work, it could be possible to read all or part of the mail coming out of tomasalex.com. Since most mail is in cleartext, this would provide a treasure trove of account information and trusted correspondents to be used in compromising internal systems. Reading enough mail would probably deliver some passwords as well. Getting someone to run an trojan executable that has been faked to appear to be from a trusted source should be relatively easy. Snooped traffic could also be written to a log and moved to an attacker's system.

Another attack against the GIAC mail would be to send spoofed BGP packets to the ISP's routers, so that mail from tomasalex.com would by routed thru the attacker's system, where it could be perused at leisure.

Even without attacking the routers, however, there are plenty of bypass attacks to use against internal systems. Again, most are defeated by an updated firewall. The first bypass vulnerability is the Checkpoint Firewall-1 RDP bypass vulnerability. This allows arbitrary eitherbound RDP packets to pass through the firewall. RDP, the Reliable Data Protocol, is used by FW-1 as a layer above UDP to establish encryption sessions. By adding a faked RDP header, content from either side can walk through the firewall unless is has been upgraded in the last month.

Most servers aren't listening on port 259,however, so while this bypass vulnerability makes a great covert channel once internal systems are owned, it isn't going to help compromise internal systems.

More useful for attacking internal systems will be the Unauthorized RSH/REXEC Connection vulnerability. This allows unauthorized connections by sending crafted packets

to request an RSH/REXEC connection, and communicating with clients behind the firewall on an arbitrary port. This vulnerability only works if the administrator enabled RSH/REXEC with stderr support. If this has been done and the firewall hasn't been upgraded to FW-1 V 4.1 SP3, it should be relatively straightforward to probe and compromise internal systems – that is, it will be as if the firewall isn't there.

BugTraq lists one more bypass vulnerability, the FTP "ALG" Client vulnerability. This attack uses crafted emails to open port 139 (a major target on Windows boxes) and other ports on the target to the origin address. Checkpoint FW-1 4.1 and earlier versions are vulnerable.

**Conclusion**

As has been detailed above, there are a lot of possible attacks into tomasalex.com, or for that matter, any reasonably complex site. All of the attacks explained in this section can be defeated by timely application of the appropriate security patches – which often never happens in the real world. Witness the current CodeRed fiasco. Tomasalex.com will be vulnerable and owned if they have not upgraded their firewall lately. If they have, then penetration is made much harder, perhaps impossible given only the list of vulnerabilities mentioned above.

Something no upgrade can fix, however, is mis-configuration. Firewall-1 is a complex piece of software, with hundreds of setting in a reasonable sized ruleset. A thorough and methodical attacker may be able to identify vulnerabilities even in fully current firewall. For this reason, regular audits of the firewall properties and rulesets are most important.

It's a dangerous world. Be careful out there.

## References


[1] Sans Institute, The. Windows NT Security: Step-by-Step 1998. http://www.sans.org/newlook/publications/ntstep.htm.

[2] OpenBSD Project, The. OpenSSH. V. 1.115. http://www.openssh.com/ (August 9, 2001).

[3] CryptoCard Corporation. CRYPOTCARD. http://www.cryptocard.com/index.cfm?CID=4&NAVCID=4&PageName=Products (August 9, 2001).

[4] Scambray, Joel, Stuart McClure, and George Kurtz. Hacking Exposed, 2nd Ed. New York: McGraw-Hill Professional Publishing, 2000.

[5] American Registry for Internet Numbers. American Registry for Internet Numbers ( ARIN ). http://www.arin.net/ (August 9, 2001).

[6] SecurityFocus.com BugTraq. http://www.securityfocus.com/ (August 9, 2001).

[7] Spencer, Mark. Cheops Network User Interface. http://www.marko.net/cheops/ (August 9, 2001).

[8] Bindview Corporation. BindView Corporation. http://www.bindwiew.com/ (August 9, 2001).

[9] PGP Security. CyberCop Scanner. http://www.pgp.com/products/cybercop-scanner/default.asp/ (August 9, 2001).

[10] SamSpade.org. SamSpade.org. http://samspade.org/ssw/ (August 9, 2001).

[11] Sandstorm Enterprises. Sandstorm Phonesweep. http://www.sandstorm.net/phonesweep/ (August 9, 2001).

[12] Goncalves, Marcus, and Steven Brown. CheckPoint Firewall-1 Administrator's Guide. New York: McGraw-Hill Professional Publishing., 1999.


## Bibliography


Frisch, Aileen. Essential System Administration. Sebastopol, California. O'Reilly & Associates, Inc. 1995.

Gregory, Peter. Solaris Security. Upper Saddle River, New Jersey: Prentice Hall, 2000.

Lammle, Todd. Cisco Certified Network Associate. San Francisco, California. Sybex, Inc, 2000. 2001).

Parent, Florent. Managing Cisco Network Security. San Francisco, California: Syngress Media, Inc, 2000.

Scambray, Joel, Stuart McClure, and George Kurtz. Hacking Exposed (2nd Edition). Berkeley, CA. McGraw-Hill. 2000.

## URLs of Posted Sans Practicals

Arthiabah, Koki. GIAC Firewall and Perimeter Protection. http://www.sans.org/y2k/practical/Kofi_Arthibah.zip (August 10, 2001)

Alex, Tomas. GIAC Firewall and Perimeter Protection Curriculum Practical Assignment. http://www.sans.org/y2k/practical /Tomas_Alex_GCFW.doc (August 10, 2001)

Stuckless, Colin. SANS GIAC Firewall and Perimeter Protection Practical Assignment. http://www.sans.org/y2k/pratical/Colin_Stuckless.doc. (August 10, 2001)