GCFW Practical

David F. Severski

Table of Contents

Table of Figures

1 Security Architecture

Define a security architecture for GIAC Enterprises, an e-business which deals in the online sale of fortune cookie sayings. Your architecture must include the following components:

- filtering routers;
- firewalls;
- VPNs to business partners;
- secure remote access; and
- internal firewalls.

Your architecture must consider access requirements (and restrictions) for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

Include a diagram or set of diagrams that shows the layout of GIAC Enterprises' network and the location of each component listed above. Provide the specific brand and version of each perimeter defense component used in your design. Finally, include an explanation that describes the purpose of each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

1.1 Assumptions

For the purposes of this exercise, it will be assumed that GIAC Enterprises is restricted to a single geographic location. Only core elements of GIAC Enterprises' perimeter security infrastructure will be considered. Other concerns such as physical security, host-based security, distribution network infrastructure (such as switch configuration), etc., are outside the scope of this discussion, but may be mentioned for the reader's consideration when appropriate. For ease of reference, it is also assumed that GIAC Enterprises owns the giacenterprises.com domain name as well as the IP range 156.125.12.0 – 156.125.12.197.

1.2 Access Requirements

Four classes of external users will need to access GIAC Enterprises' corporate resources: Customers, Partners, and Suppliers.

1.2.1 Customers

Customers are the end consumers of GIAC Enterprises' fortune product. These customers connect to GIAC Enterprises via a web-based client for the purposes of previewing, selecting, purchasing, and viewing their fortunes online. These users are primarily concerned with being able to access GIAC Enterprises' web site and securely purchase fortunes without fear of compromising their payment information.

1.2.2 Partners

Partners are those entities that enjoy a special business relationship with GIAC Enterprises. Unbeknownst to the general public, GIAC Enterprises is actually a driving engine behind many stock research reports. When an analyst needs to offer a client advice about a stock, he or she often turns to GIAC Enterprises for financial advice, which is then resold to the analyst's clients. Partners require in-depth access to GIAC Enterprises' network via Virtual Private Network (VPN) connections for the purposes of sharing sales data, sending and receiving email, and accessing the fortune database for re-branding as stock advice.

1.2.3 Suppliers

Suppliers are teams of highly skilled researchers who comb sources ranging from Nostradamus' predictions to the major news tabloids in their quest for the most accurate, entertaining, and marketable fortunes. These suppliers submit nuggets of fate-laden prose to the GIAC Enterprises fortune system via a web-based client. A protected segment of the GIAC Enterprises' web site enables them to submit their data directly to the fortune database. Additionally, these suppliers must be able to run reports against the fortune sales database in order to determine how frequently their submissions are being served and how much they have earned in royalties. These reports are accessible via the suppliers-only section of the GIAC Enterprises' web site.

1.2.4 Remote Employees

GIAC Enterprises is a strong advocate of telecommuting, both as a means of reducing office space requirements and of improving employee moral and productivity. Employees are permitted to access the internal corporate network using private home Internet connections in combination with VPN software and hardware ID tokens. These remote users are granted the same level of access that they would enjoy as onsite users. GIAC Enterprises does not support the use of dial-up connections, preferring to subsidize DSL and Cable connections for approved telecommuters.

1.3 Proposed Design

The architecture diagramed below is recommended as the best means of ensuring maximum security for GIAC Enterprises' network infrastructure. It implements a multi-layered security solution, a strategy known as "defense-in-depth". Each layer offers protection against attacks, whether from internal or external sources, creating a network whose security is not dependent on any single component.

The following hardware and software manufacturers and equipment models have been selected as the core components of the GIAC Enterprises' security infrastructure:

Function	Brand	Version Information
Filtering Router	Cisco	3620 running IOS 12.1
External Firewall	Nokia Checkpoint	IP 330 running IPSO 3.4.1 Checkpoint FW-1 NG (Feature Pack 1)
Internal Firewall/ VPN Concentrator	Nokia Checkpoint	IP 330 running IPSO 3.4.1 Luna VPN Accelerator Card Checkpoint FW-1 NG (Feature Pack 1) Checkpoint VPN-1 NG (Feature Pack 1)
Network Intrusion Detection System (NIDS)	SourceFire	Snort 1.8.2 FreeBSD 4.4

Network Tap	Finisar Systems	Century Tap
Host-based Intrusion Detection System (HIDS)	Internet Security Systems	BlackIce Defender v2.9.cai
HTTP Load Balancer	F5 Networks	BIG-IP
Enterprise Database	Oracle Corporation	Oracle 9i
Authentication Server	Secure Computing	SafeWord Premier Access
Web Proxy Server	Duane Wessels	Squid 2.4-STABLE2

Table 1: Selected Security Equipment

1.3.1 Proposed Architecture Diagram

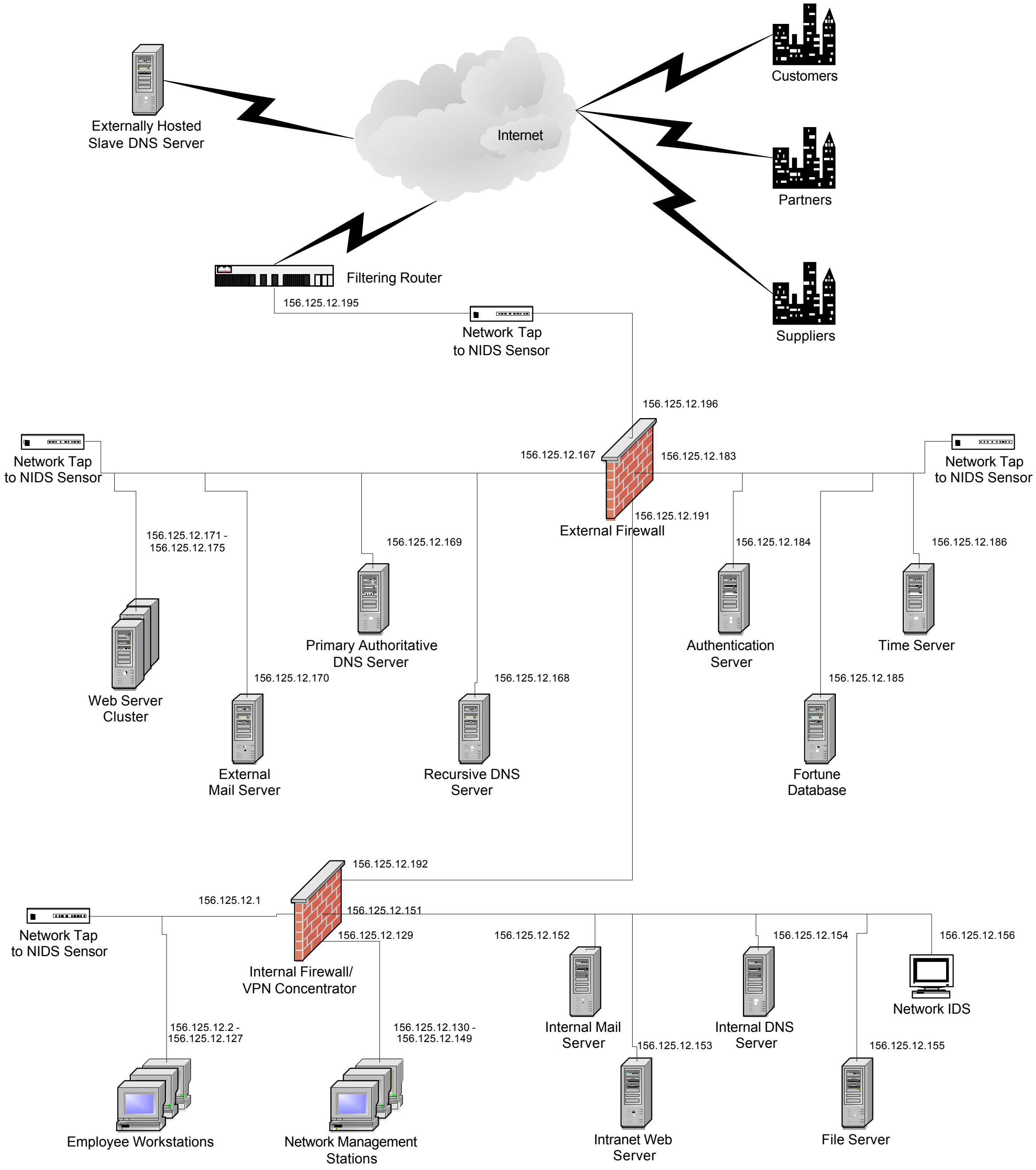
Externally Hosted
Slave DNS Server
Internet
Customers
Partners
Suppliers
Filtering Router
156.125.12.195
Network Tap
to NIDS Sensor
156.125.12.196
Network Tap
to NIDS Sensor
156.125.12.167
156.125.12.183
Network Tap
to NIDS Sensor
156.125.12.191
External Firewall
156.125.12.171 -
156.125.12.175
156.125.12.169
156.125.12.184
156.125.12.186
Web Server
Cluster
Primary Authoritative
DNS Server
Authentication
Server
Time Server
156.125.12.170
156.125.12.168
156.125.12.185
External
Mail Server
Recursive DNS
Server
Fortune
Database
156.125.12.192
156.125.12.1
156.125.12.151
Network Tap
to NIDS Sensor
156.125.12.129
156.125.12.152
156.125.12.154
156.125.12.156
Internal Firewall/
VPN Concentrator
Network IDS
156.125.12.2 -
156.125.12.127
156.125.12.130 -
156.125.12.149
Internal Mail
Server
156.125.12.153
Internal DNS
Server
156.125.12.155
Employee Workstations
Network Management
Stations
Intranet Web
Server
File Server

Figure 1: Network Security Architecture

1.4 Discussion

GIAC Enterprises, an e-business that deals in the online sale of fortune cookie sayings, is developing a security architecture for its data network. In order to accommodate GIAC Enterprises' customers, suppliers, and partners, a multi-zoned network infrastructure is recommended. The network zones to be isolated include the internal desktop network (or intranet), a network management subnet, the external public internet, and three separate demilitarized zones (DMZ) for servers that must be addressable either by internal desktop users, or by external internet hosts.

A Cisco device will serve as a filtering router that feeds into a Nokia IP appliance running Checkpoint's firewall software. The Nokia appliance will be used to divert traffic into either the DMZ or internally facing zones. A second Nokia firewall is to be directly attached to the internal interface of the external firewall and will act as a third layer for screening network traffic. Network Intrusion Detection Systems (NIDS) will be deployed on the inside of the screening router, in the DMZ, and on the internal interface, providing comprehensive screening of all intrusion attempts.

1.4.1 Filtering Router

The filtering router serves as the termination point for GIAC Enterprises' link to its Internet Service Provider (ISP). It is to this device that the T-1, or other private circuit, would be connected. The primary function of the filtering router is to provide network connectivity and to act as a minimal sanity check on traffic, preventing some of the more obvious forms of erroneous data from entering the network perimeter. A Cisco 3620 access router running Cisco IOS 12.1 is recommended for this role.

Note that, as outlined in this presentation, GIAC Enterprises is connected to the Internet by a single network link. This represents a point of failure for the network. As GIAC Enterprises grows, it is recommended that the possibility of bringing in a second filtering router, with an independent ISP connection, be taken under serious consideration. This option is not implemented in the current configuration for the sake of streamlining the demonstration.

Typical outbound filters on filtering routers prohibit the transmission of any outbound (Internet-bound) traffic that does not carry a source address from within GIAC Enterprises' assigned range of IP addresses. Additionally, traffic bound for an invalid public IP address, such as RFC 1918 space, is also filtered at this point. These filters help to prevent GIAC Enterprises' resources from being hijacked for the purposes of launching Denial of Service (DOS) or other hacking attacks against outside parties.

Traffic entering GIAC Enterprises from the Internet would also be filtered in order to prohibit the entry of non-routable IP addresses, such as RFC 1918 private IP space, or broadcast IP traffic. While it might seem tempting to load additional filters onto the filtering router in the hopes of further limiting the incidence of malicious traffic, this impulse should be curbed. In the interest of both ease of management and the tracking of illicit traffic, this task will be delegated to a device dedicated to these particular tasks, the external firewall.

1.4.2 External Firewall

The external firewall is the main checkpoint for all traffic seeking to enter GIAC Enterprises' network. It is here that the bulk of enforcement of inbound network policies takes place. The external firewall recommended in this scenario is a Nokia IP 330 firewall appliance running Checkpoint's Firewall-1 software. The Nokia IP 330 is a dedicated hardware appliance that runs a commercially hardened version of the FreeBSD operating system known as IPSO.

The Nokia network appliance contains four physical network interfaces (three in its standard configuration, with an additional Ethernet connection optional). This configuration makes it convenient to separate, both physically and logically, groups of machines into distinct zones with different security classifications. The interface that connects to the filtering router is referred to as the external interface and, as the least trusted network, is subject to the most restrictive policies. The interface that connects to the internal network enjoys the least restrictive policies. The two remaining interfaces separate those networks whose services must be directly addressable by hosts on the public Internet. Separating public servers such as web and external mail relays from the rest of an organization's network is known as creating a Demilitarized Zone (DMZ).

The default policy of all network interfaces will be to deny all traffic. Only traffic explicitly allowed by GIAC Enterprises will be permitted to pass through the firewall. The Checkpoint Management Module, which, in addition to performing logging functions, is responsible for compiling the policy database into a rule set and installing that rule set on the firewall, will be located on a machine in the dedicated management network.

1.4.3 Internal Firewall and VPN Concentrator

Protection against malicious or accidental attacks from within the trusted network, whether on the part of disgruntled employees, viruses, application error, or other agents, is the responsibility of the Internal Firewall. This device serves to isolate and protect high value internal assets, such as payroll databases and personnel files. The rules for this device, like those for the external firewall, should default to a "deny all" policy state in which only explicitly permitted services are allowed. A second Nokia IP 330, with the optional fourth Ethernet interface installed, is recommended as the internal firewall. One interface will be allocated to the desktop network, one to the internet-facing connection, the third to the internal enterprise server network (which consists of internal mail servers, DNS servers, etc.), and the fourth to the dedicated network management LAN. This will facilitate the separation of services into different security classes, providing a secure infrastructure as well as a protected exterior.

In addition to its duties as a firewall host, this device also serves as the end point for VPN tunnels to GIAC Enterprises' remote employees and partners. Authentication and encryption capabilities will be added to this device by loading it with Checkpoint's VPN-1 software in conjunction with the FW-1 module. Because encryption is a CPU intensive process, the Luna VPN Accelerator Card, a drop-in addition to the VPN-1 package, may be installed in the Nokia IP 330, offloading some of the encryption load from the firewall's CPU to the dedicated hardware on the accelerator card. The authentication server will carry out authentication and authorization of user requests. The Management Module that is responsible for the external firewall will also control this device.

1.4.4 Network Intrusion Detection Systems

While a well-designed and conscientiously maintained firewall system can deter a large majority of the most commonly employed network-based attacks, new attack methods are constantly being developed. Firewall systems generally do not provide any information about the level of permissible activity -- such as valid HTTP sessions to a company's web server -- on a network. Indeed, firewalls tend to have weak logging mechanisms and do not collect data about the exact nature of the attacks they may have helped to preempt. For these reasons, a system capable of monitoring all of the traffic on a network segment and of reporting on suspicious traffic is being employed. These devices are called Network Intrusion Detection Systems (NIDS).

GIAC Enterprises wishes to exercise the utmost degree of vigilance against attacks and the company has therefore elected to monitor traffic on the outside of its external firewall as well as traffic that successfully penetrates its perimeter. The open source NIDS system known as Snort meets this requirement quite admirably. Snort is a free, high-performance NIDS in widespread use. As a result of Snort's high adoption rate among security-oriented members of the open source community, the attack signature repositories found at sites such ArachNIDS frequently contain detection signatures specifically written in Snort's internal syntax. These repositories, combined with the Snort development team's almost daily updates to the included rule set, have furnished Snort with an extremely robust set of detection signatures. The syntax of the Snort detection language is also well documented and is similar to tools familiar to many network administrators – for example, tcpdump – making it easy for a network administrator to create a custom rule for a particular new attack. Snort can run under both UNIX and Windows-based platforms: in the current configuration, Snort will be deployed on a FreeBSD 4.4 host, a selection based on this OS's high level of performance and robust security.

Finisar Systems' Century Tap devices permit the copying of traffic from the various monitored segments. This data can in turn be delivered to the Snort NIDS device in the protected LAN without any compromise of network security or performance. The Snort NIDS sensor device will log alerts of possible attacks to a central dedicated logging host on the management LAN.

1.5 Configuration of Internal Services

The reliability and security of services critical to ongoing operations at GIAC Enterprises must be guaranteed. It is important that these services be protected against attack, but they must also be made as reliable as possible for end users, promoting a more efficient and productive work environment. Further review of each of these support services – both individually and as a part of GIAC's total network infrastructure – will demonstrate the best means for further enhancing their performance.

1.5.1 Web Server Configuration

Web-based services are the lifeblood of GIAC Enterprises' business. Customers purchase fortunes directly via the web interface and suppliers connect to a secured access area when they wish to submit new fortunes. To meet the needs of these varied users, system hardware and software capable of providing a secure and readily available platform must be selected.

For GIAC Enterprises' web farm, multiple FreeBSD 4.4 based machines, each running the Apache 1.3.22 web server, will be deployed. This cluster of machines will then be placed behind a BIG-IP load balancer from F5 Networks. The BIG-IP platform is designed to make intelligent decisions about which web server is currently carrying the lightest load, and it can direct new requests to that server, thereby providing the fastest possible connections. End users see only one GIAC Enterprises web site, but that one web site may, in fact, be made up of dozens of machines, each contributing to the total web horsepower of GIAC Enterprises.

To ensure the security of e-commerce transactions and supplier submissions, all purchasing transactions and similarly sensitive activities are encrypted using the TLS protocol. This provides additional assurance that information such as credit card numbers and new fortunes may be transmitted without any fear that they will be tampered with or intercepted.

It is important to note here that, while perimeter and infrastructure security can do much to help secure sensitive information, the code running on the web server itself, such as scripts or other custom executable code, must be closely audited for security risks. Securing the communication channel between parties is less than useless; it presents a false sense of security, if the parties to that communication do not take precautions to secure the data once they have received it.

1.5.2 Database Configuration

The HTTP front-ends retrieve data from a single database. Because this database is the central repository of GIAC Enterprises' customer information and fortune data, it is crucial that this system component be secured. Oracle Corporation's Oracle 9i database server, running on a Sun Enterprises server, is the preferred platform for this duty, owing to its mature and secure functionality. Only connections from the web servers and from the intranet web server, which contain predefined and sanitized querying and reporting tools, will be permitted to this system. Additionally, the Oracle Advanced Security (OAS) product will be used to encrypt all database transactions across the network with the Triple DES algorithm, regardless of whether or not the requesting client is internal or web-based. User access to the database will be authenticated against the dedicated authentication server. As an optional further enhancement to the reliability of this service, a clustered database approach might also be implemented.

1.5.3 Domain Name Services

The Domain Name Service (DNS) provides the translation between IP addresses (e.g. 152.136.13.1) and more easily remembered host names (e.g. mail.giacenterprises.com). This service is necessary to external users, who must be able to access GIAC Enterprises' various public services (external DNS), to internal clients, who will be seeking resources within the private network (internal DNS), and to internal hosts, who will need to resolve the host names of hosts on the external Internet (recursive DNS). Considered from both a service and a security perspective, each type of DNS service has its own unique needs.

1.5.3.1 External DNS Services

In the interest of maintaining a high level of availability to external customers, partners, and suppliers, GIAC Enterprises is employing a multiple server configuration that places all externally facing DNS entries, such as www.giacenterprises.com, on two separate servers. The first server is located in the DMZ of GIAC Enterprises' network and is the primary domain name server for the giacenterprises.com zone. A third party ISP in a different geographic location hosts a secondary server. This helps to ensure that any local server or network problems will not affect the resolution of GIAC Enterprises' servers, which could result in negative cache entries being stored across the Internet. GIAC Enterprises will need to work closely with the hosting party to ensure that the same high security standards are applied to this remote, third-party server as are applied to company-controlled servers.

BIND, the de facto standard DNS server, has a long history of serious security flaws, up to and including sacrificing total control of the server to a remote attacker. While recent revisions to this old standby have sought to correct these problems, this product's track record is decidedly less than reassuring. As a result, an alternative DNS server, djbdns, is being used to satisfy GIAC Enterprises' name resolution needs. Written by Dan Bernstein, this software is designed to provide standards-compliant name resolution without the addition of extra features that might contribute to inefficiencies and security flaws. For the last several years, Mr. Bernstein has offered a $500 bounty to anyone who successfully attacks the security of this software – and he has yet to make a payment.

Djbdns does not utilize DNS zone transfers to synchronize data between servers. Encrypted SCP transactions are used as a replacement mechanism in GIAC's DNS security architecture.

1.5.3.2 Internal DNS Services

In addition to serving external entities such as www.giacenterprises.com and mail.giacenterprises.com, GIAC Enterprises, like most corporations, wishes to assign easy-to-remember names to internal resources such as file and mail services. These internal host names are to be placed in a segregated portion of the giacenterprises.com zone, corp.giacenterprises.com, which is hosted on protected internal djbdns-based servers.

1.5.3.3 Recursive DNS Services

Separate DNS servers, also running djbdns, will be dedicated to the task of satisfying GIAC Enterprises' recursive DNS needs. Maintaining two distinct servers makes it possible to separate the duties of the recursive and authoritative DNS servers and also provides a simpler model for administration and firewall-ing of traffic. Because recursive servers are located in both the DMZ and internal networks, these servers can be configured to return internal names from the protected corp.giacenterprises.com zone to hosts on the internal network, while not leaking this information to external machines.

1.5.4 Time Synchronization Services

It is important that all of the logging and infrastructure devices on GIAC Enterprises' network have the same internal clock settings. Failure to maintain correct time can result in the generation of logging information that is impossible to correlate and may even lead to the failure or compromise of any time-based security mechanisms. A dedicated time server that maintains its clock via a Global Positioning System (GPS) connection will supply GIAC's time synchronization services. All devices that use network time services will use the authentication capabilities of the Network Time Protocol (NTP) to ensure that they are in communication with the official time server and not a hostile server masquerading as the correct server.

1.5.5 Mail Services

All Simple Mail Transport Protocol (SMTP) traffic between internal mail servers and Internet hosts is to be relayed via a mail relay located in the DMZ. This dedicated server will be the only server permitted to receive or send SMTP traffic through the external interface of the primary firewall. The mail server will run the Postfix mail server (version 20010228-pl-07) on a FreeBSD 4.4 machine. Developed by Wietse Venema as a replacement for the sendmail program, Postfix is a high-performance and high-security mail server. It is not vulnerable to mail relaying in its default configuration and it is loaded with multiple anti-spam options, including the capability of interfacing with DNS-based Realtime Blackhole Lists (RBLs) such as Open Relay Blackhole Zones (ORBZ) and the Spam Prevention Early Warning System (SPEWS). The AMaViS anti-viral mail interface will be used in conjunction with Postfix to provide thorough scans of both incoming and outgoing mail for potential viruses. Note that, while this is not documented in this particular architecture, additional capacity and enhanced resiliency against mail bomb attacks could be procured by establishing multiple mail servers within the DMZ.

All SMTP and POP3 traffic running between mail servers and clients will be encrypted using the Transport Layer Security (TLS) tunneling protocol, which also allows the interchange of digital certificates as proof of identity. All POP3 clients will be issued digital certificates by an internal GIAC Enterprises certificate authority. Both clients and servers will be able to authenticate the identity of the machines with which they are in contact through verification of these digital certificates. Because SMTP transactions with mail servers outside of GIAC Enterprises' jurisdiction must be allowed, digital certificates will be optional in server-to-server communications, but will remain mandatory for all users who wish to send mail from within GIAC Enterprises, further reducing the likelihood that corporate resources will be used to transmit spam mail.

1.5.6 HTTP Proxy

No direct connections between protected internal hosts and external web servers will be permitted. All internal users wishing to surf external web sites must use the web proxy server located in the DMZ, which will be running Squid V2.4 on a FreeBSD 4.4 machine. The web proxy alone will be allowed to establish HTTP and HTTPS sessions to Internet web sites. This proxy server limits the number of holes that may be opened in the firewall, provides caching services that help to reduce bandwidth usage and increase end user performance, and also provides an audit and enforcement location for policing and limiting the URLs that may be visited by internal users. In order to enjoy external connectivity, internal web browsers must be configured to point to the web proxy. Optionally, the Network Address Translation (NAT) capabilities of the Checkpoint FW-1 modules may be used to transparently redirect web traffic to the proxy server.

1.5.7 Backup and Disaster Recovery

While it has become increasingly common practice to subject servers and network infrastructure equipment to a thorough security review, all planning would be for naught if data and hardware were to be destroyed in the event of an incident such as a fire in a data center. Designing a complete backup solution and disaster recovery plan is outside the scope of this discussion, but both backup and recovery should be considered in any thoroughgoing security discussion and are, for this reason, simply mentioned here.

1.5.8 Configuration Control

The increasingly complex configurations of modern network implementations bring with them the problem of managing multiple sets of configuration files and scripts. If a system for tracking changes to files and rolling out such changes in a controlled manner is not implemented, chaos can quickly overwhelm a network. Open Source tools such as the Concurrent Versions System (CVS) can play an important role in a well-structured change management program. Such programs are complex and can only be mentioned here, but they do provide valuable services and are deserving of a security practitioner's attention.

1.5.9 Authentication Services

A separate server running Secure Computing's SafeWord Premier Access product will be used to centralize all user authentication services on the DMZ network. This product offers strong Authentication, Authorization, and Accounting (AAA) services, along with a variety of protocol interfaces for the firewalls and for other software in use on the network. SafeWord's hardware token facilities provide extremely secure network logins, precluding any compromise of password information. Centralizing authentication also increases ease of management, reducing the chance that unknown active accounts might be scattered across multiple systems.

1.5.10 Network Management

All network management workstations are located on a separate network segment of the internal GIAC Enterprises' LAN. Only hosts from this network segment will be permitted to exchange management and logging information with infrastructure equipment. All logging functions from network infrastructure equipment will be directed to dedicated machines within this network, providing a central location for the correlation of data. Whenever possible, SSH V2 or similar encrypted forms of communication will be used to carry out network management functions. The Checkpoint Management Module for both the external firewall and the internal firewall/VPN concentrator will be located on this network.

2 Security Policy

2.1 Part 1 - Define Your Security Policy

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense-in-depth or to separate business functions.

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

You **must** include the complete policy (ACLs, ruleset, IPSec policy) in your paper. It is not enough to simply state "I would include ingress and egress filtering…" etc. The policies may be included in an Appendix if doing so will help the "flow" of the paper.

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

2.1.1 Filtering Router

This router's sole function is to provide connectivity to GIAC Enterprises' ISP of choice. The configuration policies on this router are deliberately designed to be as simple as possible, since the majority of filtering will be executed on the external firewall.

This router does not run any routing protocols and makes all routing decisions solely on the basis of statically defined routes. On the internal side, only traffic from authorized machines in the DMZ IP address range will be permitted. All other traffic will be denied.

Administrative access to this box will be permitted only from the segregated management network and direct physical console connections. User authentications and permissions on the router will be managed via the SafeWord authentication server, using the Cisco TACACS+ protocol.

The following policy (ACL settings) is implemented on the filtering router:

```
interface serial 0
      ip address 156.12.1.1 255.255.255.252
      ip access-group 101 in
access-list 101 deny ip 10.0.0.0 0.255.255.355 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 224.0.0.0 7.255.255.255 any
access-list 101 deny ip 240.0.0.0 63.255.255.255 any
access-list 101 deny ip 255.0.0.0 63.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 permit ip any any
access-list 102 permit ip 156.125.12.0 0.0.0.127 any
access-list 102 permit ip 156.125.12.128 0.0.0.63 any
access-list 102 permit ip 156.125.12.192 0.0.0.7 any
interface ethernet 0
      ip address 156.125.12.195 255.255.255.252
      ip access-group 102 in
```

Table 2: Filtering Router Ruleset

2.1.2 Checkpoint Firewalls

The Checkpoint FW-1 software uses an easy to navigate graphical depiction of the network in its management interface. Once the network topology has been defined through this interface, a network administrator may define firewall rule sets using network infrastructure labels rather than more arcane IP addresses. (For the reader's reference, both the label definitions and the combined rule set for the firewall devices are listed in the appendix.)

2.1.2.1 External Firewall

As the primary choke point, the external firewall will be set to a deny-all state by default. All traffic that passes through this firewall must be allowed explicitly by a pre-defined rule. Web browsing traffic emanating from the internal network will be permitted only via the designated proxy machine, whereas web transactions initiated from the external network will be permitted only to the web server cluster on the DMZ. SMTP transactions with the external network will be allowed to originate from, and terminate at, the mail relay host on the DMZ. DNS traffic will be limited strictly to UDP queries and responses: the authoritative DNS server will only accept incoming queries, while outbound queries will only be permitted from the recursive server. In support of the transfer of updated DNS zone files between the primary DNS server and the externally hosted secondary server, outbound SCP copies will be allowed when established by the primary DNS server to the secondary server. Finally, traffic from VPN clients will be authenticated at the external firewall against the authentication server before being permitted to pass to the internal firewall for encryption purposes. All other traffic will be explicitly prohibited.

2.1.2.2 Internal Firewall and VPN Concentrator

VPN connections will be allowed from authorized partners and GIAC Enterprises' employees using IPSEC with Triple-DES encryption. Prior to being granted VPN access, all partners and GIAC Enterprises employees must complete security awareness training, which will include thorough coverage of threat awareness and of company-established acceptable usage guidelines.

Checkpoint's Secure Client VPN software will be used to enforce a uniform security policy on remote hosts wishing to initiate VPN connections with GIAC Enterprises. This policy will include the disabling of split tunneling, so as to prevent remote machines from concurrently connecting to the GIAC internal network and a third-party network. Virus software, with current anti-viral signatures installed, is also required on all VPN-enabled machines. Finally, a host-based intrusion detection system such as BlackIce will be required on all VPN candidate machines, providing an added layer of protection for these highly vulnerable machines.

The authentication server, located in the protected DMZ, will administer all VPN user authentications. True two-factor user authentication will be achieved through combining SecureID tokens with user passwords. If an even higher level of security is desired, biometric devices might be investigated as an option. One of the advantages of SafeWord is that it already supports many such three-factor authentication schemes, should they be desired in the future.

2.2 Part 2 – Security Policy Tutorial

Select **one** of the three security policies defined above and write a tutorial on how to implement the policy. Use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

A general explanation of the syntax or format of the ACL, filter, or rule for your device.

A general description of each of the parts of the ACL, filter, or rule.

A general explanation of how to apply a given ACL, filter, or rule.

For each ACL, filter, or rule in your security policy, describe:

The service or protocol addressed by the rule, and the reason this service might be considered a vulnerability.

Any relevant information about the behavior of the service or protocol on the network.

If the **order** of the rules is important, include an explanation of why certain rules must come before (or after) other rules.

Select three sample rules from your policy and explain how you would test each rule to make sure it has been applied and is working properly.

Be certain to point out any tips, tricks, or potential problems ("gotchas").

2.2.1 Filtering Router Policy Description

On the frontlines of all Internet traffic, both friendly and hostile, sits the filtering router, in this case, a Cisco 3620. While its primary duty is to ensure the smooth flow of traffic, it is flexible enough to allow us to also use it to implement a minimal amount of traffic filtering. It is particularly important to ensure that administrative access to the filtering router be secured. CERT reports on recent trends in network attacks reveal that attacks directed at routers, rather than at the workstations they serve, are on the rise.

The policy for this device will be implemented in the steps detailed below. The purpose of this procedure is to secure the filtering router from hostile takeover and to implement secure logging functions, in addition to performing a minimal level of traffic screening. (As has been noted above, the filtering router should not be responsible for anything other than the most rudimentary traffic filtering.)

2.2.1.1 Name configuration

Before any other configuration steps have been taken, the router should be assigned the DNS name of “cborder” within the GIAC Enterprises internal DNS zone of corp.giacenterprises.com. This name is used by logging functions and will also be required for creating secure tunnels to management devices later in the configuration process. DNS name resolution should then be disabled, since this device does not need to look up DNS entries for any other entity. The Network Time Protocol (NTP) should also be configured to synchronize this device’s clock with the reference standard. This step is important because it ensures that logging messages from different devices can be correlated.

The first set of configuration commands reads as follows:

```
hostname cborder

ip domain-name corp.giacenterprises.com
```

```
no ip domain-lookup
```

2.2.1.2 Setting Passwords

Next, a password should be set for the router's protected, or "enable", mode. The service password-encryption command should always be included in the configuration of any Cisco device. This command encrypts all passwords entered during the configuration process. If this step is omitted, passwords are stored in a clear-text format, making them an easy target for any attacker who is able to retrieve even a read-only copy of the configuration file.

```
enable secret Fi1t3rZekret1

service password-encryption
```

2.2.1.3 Time Synchronization

Next, the following commands may be used to establish the time server, located at 156.125.12.186, as the filtering router's time and date source. These commands first specify that all NTP traffic must be authenticated through the use of the MD5-hashed authentication key "GIACtimeKey". The reference NTP server is then specified and the newly configured key is associated with it. The filtering router verified that it is receiving NTP traffic from the actual time server by looking for the presence of this authentication key. Packets not containing the authentication key are rejected by the router. This procedure helps to deter attacks against the NTP service. Finally, the NTP protocol is permitted to update both the system calendar and the time of day clock.

```
ntp authenticate

ntp authentication-key 10 md5 GIACtimeKey

ntp trusted-key 10

ntp server 156.125.12.186 key 10

ntp update-calendar
```

2.2.1.4 Authentication and Authorization

GIAC's security policy specifies that the authentication server, located at 156.125.12.184, should be used to authenticate logins as well as to authorize the actions users are permitted to take after they have been authenticated. The following commands must be used to configure the TACACS+ protocol (which is used to communicate with the authentication server) and to establish the shared encryption key of "`s00p3rs3krit`".

Cisco IOS based devices are able to break commands down into 16 levels of escalating privilege, ranging from 0 (unprivileged) to 15 (maximum privilege). By specifying authorization via the TACACS+ connection to the authorization server for each level, the security engineer ensures that all levels of command access are screened for authorization.

By mandating an external server be present for access to the filtering router, the potential for a denial of service attack, whether inadvertent or deliberate, is introduced. Should the authorization server become unavailable, perhaps due to a network outage or an attack, the fall back procedure of the filtering router needs to be carefully weighed so as to not introduce added vulnerabilities, but while still providing access to the device. In the case of GIAC's filtering router, the decision has been made that authentication via the enable password should still be possible, and that authorization of individual commands will failover to an allow-all state. In an architecture with more stringent security concerns, the router could be configured such that no access is possible without the presence of the external authentication server. The fallback mode in this case is configured by adding "enable" to the authentication line, and the "none" key phrase to the authorization lines that follow.

```
aaa new-model

tacacs-server host 156.125.12.184

tacacs-server key s00p3rs3krit

aaa authentication login AUTHGROUP group tacacs+ enable

aaa authorization commands 0 restrict group tacacs+ none
aaa authorization commands 1 restrict group tacacs+ none

aaa authorization commands 2 restrict group tacacs+ none

aaa authorization commands 3 restrict group tacacs+ none

aaa authorization commands 4 restrict group tacacs+ none

aaa authorization commands 5 restrict group tacacs+ none

aaa authorization commands 6 restrict group tacacs+ none

aaa authorization commands 7 restrict group tacacs+ none

aaa authorization commands 8 restrict group tacacs+ none

aaa authorization commands 9 restrict group tacacs+ none

aaa authorization commands 10 restrict group tacacs+ none

aaa authorization commands 11 restrict group tacacs+ none

aaa authorization commands 12 restrict group tacacs+ none

aaa authorization commands 13 restrict group tacacs+ none

aaa authorization commands 14 restrict group tacacs+ none

aaa authorization commands 15 restrict group tacacs+ none

line vty 0 4

      login authentication AUTHGROUP

      authorization commands 0 restrict

      authorization commands 1 restrict

      authorization commands 2 restrict

      authorization commands 3 restrict
```

```
          authorization commands 4 restrict

          authorization commands 5 restrict

          authorization commands 6 restrict

          authorization commands 7 restrict

          authorization commands 8 restrict

          authorization commands 9 restrict

          authorization commands 10 restrict

          authorization commands 11 restrict

          authorization commands 12 restrict

          authorization commands 13 restrict

          authorization commands 14 restrict

          authorization commands 15 restrict
```

2.2.1.5 Ingress Filtering

Moving next to configuring ingress filtering, the following commands should be used to block all traffic coming from non-routable (RFC 1918) and broadcast IP addresses:

```
interface serial 0

      ip address 156.125.1.1 255.255.255.252

      ip access-group 101 in

access-list 101 deny ip 10.0.0.0 0.255.255.355 any

access-list 101 deny ip 172.16.0.0 0.15.255.255 any
```

```
access-list 101 deny ip 192.168.0.0 0.0.255.255 any

access-list 101 deny ip 127.0.0.0 0.255.255.255 any

access-list 101 deny ip 224.0.0.0 7.255.255.255 any

access-list 101 deny ip 240.0.0.0 63.255.255.255 any

access-list 101 deny ip 255.0.0.0 63.255.255.255 any

access-list 101 deny ip host 0.0.0.0 any

access-list 101 permit ip any any
```

This set of configurations will cause the router to reject all inbound IP traffic with a source IP address in any of the RFC 1918 ranges (10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0 – 192.168.255.255). In addition to this, they will also block broadcast and multicast traffic. (Note that commands that relate only to configuring the dedicated link [T-1 or any other class of circuit] have been omitted.)

The syntax used to specify access control lists (ACLs) for Cisco devices is reasonably intuitive. The basic format is "**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard destination destination-wildcard* [**log**]". The *access-list-number* groups individual actions into a combined list, while each individual element of the group may specify either a deny or permit action. The source and destination identify the IP addresses, while the wildcard flags are used to set the wildcard bits of the netmask.

2.2.1.6 Egress Filtering

Conversely, attacks on other systems must not be allowed to be launched from within the GIAC Enterprises' network. Traffic leaving GIAC Enterprises in the direction of the Internet must also be subjected to egress filtering. The following commands should be used to implement this filtering:

```
interface ethernet 0
```

```
      ip address 156.125.12.195 255.255.255.252

      ip access-group 102 in

access-list 102 permit ip 156.125.12.0 0.0.0.127 any

access-list 102 permit ip 156.125.12.128 0.0.0.63 any

access-list 102 permit ip 156.125.12.192 0.0.0.7 any
```

This access list only allows traffic emanating from a legitimate GIAC Enterprises' IP address to exit to the public Internet. This prevents an inside agent from using GIAC network resources to launch anonymous attacks against the outside world. The destination addresses of all traffic are also checked to ensure that they do not contain invalid RFC 1918 addresses.

2.2.1.7 Secure Management

We now turn our attention to protecting the filtering router itself. Telnet, the most commonly used protocol for remote administration of a Cisco router, sends all traffic, including passwords, as clear text, which is easily intercepted by eavesdroppers. After the portion of the rule set listed below is implemented, only connections from the GIAC Enterprises' protected management LAN (156.125.12.128/27) will be allowed, and even then, only when the SSH encrypted protocol is used. It is important to note that while Cisco devices support the SSH V1 protocol, they do not support SSH V2, which may leave them open to some of the more recently developed SSH exploits. Administrators should monitor this situation carefully, most notably by staying abreast of advisories and IOS updates from Cisco. The price of security is eternal vigilance!

```
access-list 10 permit 156.125.12.128 0.0.0.64

line vty 0 4

         transport input ssh

         access-class 10 in
```

```
              login
```

2.2.1.8 SNMP

The Simple Network Management Protocol (SNMP) is frequently used for gathering statistics such as bandwidth utilization, CPU load, etc., from remote devices. While this protocol is highly useful from a monitoring standpoint, the most widely deployed versions of SNMP – V1 and V2 – are clear-text based protocols endowed with negligible security features. An attacker may gain access to the router -- and may even change the router's configuration via SNMP – by sniffing the traffic or by launching a brute-force attack. To prevent information leakages and attacks of this nature, SNMP V3, with its support for DES encryption of packets and passwords, is being utilized.

The following set of configuration commands enables the SNMP engine on the filtering router. It establishes a user "MonitorUser" in the group "GIACmonitors." This user authenticates to the router using both the SHA authentication scheme (password "ud0ntkN0wm3") and DES privacy protection (password "uSt3lld0ntkN0w"). Assuming this user is authenticating from within the 156.125.12.128/27 network, he or she may then read SNMP settings from the router.

```
      access list 11 permit host 156.125.12.128 0.0.0.64

      snmp-server engineID local filterengine

      snmp-server group GIACmonitors v3 priv read access 11

      snmp-server  user  MonitorUser  GIACmonitors  v3  auth  sha  ud0ntkN0wm3
priv des56 uSt3lld0ntkN0w
```

2.2.1.9 Source Routing

Source routing, which allows a transmitting station to enumerate the specific path a packet is to take through a network, should be disabled. Source routing has almost no legitimate purpose, especially as regards Internet traffic, and it can be used to make it seem as though packets are coming from a trusted source. This function may be disabled with the following command:

```
      no ip source-route
```

2.2.1.10 Miscellaneous Services

Routers, like servers and other host systems, should never run services that are not necessary to the performance of the routers' designated function. Failure to remove unnecessary services opens additional avenues of attack to intruders. In the case of our filtering router, a number of services – such as echo, discard, chargen, and daytime – are typically enabled only because they provide a means for a network administrator to verify network connectivity. These services should all be disabled with the following configuration commands:

```
no service tcp-small-servers

no service udp-small-servers
```

Finger is another extraneous service. Because it allows attackers to determine who is logged into a system, it can be the source of potentially dangerous information leaks. This service may be explicitly disabled with the command:

```
no service finger
```

HTTP, BOOTP, and IDENT services are not needed on this device and should therefore be disabled in compliance with the principal of running only required services. These three services are disabled using the following commands:

```
no ip http server

no ip bootp server

no ip identd
```

2.2.1.11 Directed Broadcast

Directed broadcasts are often used in denial of service attacks and they may be disabled in the same way as the miscellaneous services mentioned above:

```
no ip direct-broadcast
```

2.2.1.12 Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP), a Cisco proprietary link-layer protocol used for determining nearby Cisco hardware configurations, must be disabled insofar as it is not desirable that hardware configuration information be broadcast on the wire:

```
      no cdp run
```

Similarly, the option of downloading a new configuration from a remote device presents a major security vulnerability and should therefore be disabled with the following command:

```
      no service config
```

2.2.1.13 Login Banner

A warning banner publicizing GIAC's policies on authorized use should be displayed to all users attempting to access the router:

```
      banner   login   |Warning!    Unauthorized   use   of   this   device   is
prohibited.  If you are not certain that you are authorized to connect to
this system, disconnect immediately.  Accessing this device implies consent
to monitoring!|
```

2.2.1.14 Logging

The filtering router should be configured to send all logging information to a dedicated host on the internal management LAN via the following commands:

```
      logging on

      logging 156.125.12.130
```

2.2.1.15 IKE Configuration

Internet Key Exchange (IKE) may be used to establish a secure, anti-replay protected tunnel between the filter router and the logging station and to provide a mechanism for the exchange of digital certificates, as issued by the authentication server. By means of the following commands, IKE, with SHA authentication and triple DES encryption, is configured to exchange digital certificates with the authentication server at 153.125.12.164.

```
crypto isakmp policy 1

      authentication rsa—sig

      hash sha

      encryption 3des

      lifetime 43200

ip host auth_server 153.125.12.164

crypto ca identity auth_server

      enrollment url http://auth_server

      query url ldap://auth_server
```

2.2.1.16 IPSEC Configuration

Once IKE has established a security association (SA) with the remote peer, IPSEC SAs can in turn be established. The following steps create an encryption of triple DES and SHA authentication that will be used when the router attempts to communicate with the 153.125.12.130 host. Note that the access list utilized ensures that only traffic originating from the router itself will be encrypted. Failure to make this distinction would result in all traffic that transits the router for the logging station to be encrypted.

```
access-list 103 permit ip 156.125.12.195 host 153.125.12.130 host

crypto ipsec transform-set TRANS-ESP esp-3des esp-sha-hmac

      mode transport
```

```
crypto map LOG-MAP 10 ipsec-isakmp

      match address 103

      set transform-set TRANS-ESP

      set peer 153.125.12.130

      set pfs group2

interface e0

      crypto map LOG-MAP
```

2.2.2 Rule Test

Once the router configuration has been established and loaded, the effectiveness of these hardening steps and access control mechanisms can then be tested. To demonstrate the testing of the router's configuration, the ingress filtering rule set and the SNMP and Secure Management configurations will be tested.

2.2.2.1 Anti-spoofing Rule Test

The hping tool can be used to test the rules preventing spoofing on the external interface. Hping allows the generation of arbitrary IP packets and these false packets can then be directed to the firewall. The command "`hping 156.12.1.1 –s 192.168.0.1`" causes ping ICMP packets with a bogus IP address of 192.168.0.1 to be generated at the external interface of the filtering router. These packets are within RFC 1918 reserved space and are therefore not valid general Internet packets: they should be dropped by the access-list 101 rule set. When a packet sniffer is run between the traffic generator and the filtering router, the bogus packet can be observed transiting to the filtering router. However, no return traffic is generated, demonstrating that the packet has indeed been silently dropped at the router. If further verification of this rule set is desired, the access list may be modified to include the optional log keyword, which prompts the router to create log entries for every packet dropped. The modified rule would read "`access-list 101 deny ip 192.168.0.0 0.0.255.255 any log`." Because this logging function substantially increases the load on the filtering router, it is not typically enabled.

2.2.2.2 SNMP Rule Test

The SNMP rules can easily be tested by hooking up a test workstation to the internal Ethernet interface and then using an SNMP query tool such as snmpwalk to query the router's SNMP service. While a command utilizing an incorrect user name and password, such as:

```
      snmpwalk  -v  3  -l  authPriv  -u  baduserID  -a  SHA  -A  badpassword
156.125.12.1
```

will fail, a command including the correct login information, such as:

```
      snmpwalk -v 3 -l authPriv -u MonitorUser -a SHA -A ud0ntkN0wm3 -x DES
-X uSt3lld0ntkN0w 156.125.12.195
```

will generate a full list of available SNMP registers. Entering various combinations of invalid and valid authentication credentials will allow the administrator to verify that access to the router's SNMP service is only possible when correct user information has been provided.

For a more thorough scan of the security provided by V3 of SNMP, a simple brute force attack may be run against the Cisco router. During such an attack, an SNMP agent tries all possible combinations of community strings until a successful match is found. SNMP brute force attacks can be produced by commercial products such as SolarWinds or open source tools such as those found at SecuriTeam.com. However, SNMP V3 makes these attacks much more difficult insofar as it requires that two passwords be employed in combination with the correct authentication and encryption algorithms before data may be retrieved from the filtering router. Indeed, even if the passwords and algorithms were to be compromised, the ACL applied to the filtering router only permits those workstations that are on the management segment to communicate with the SNMP service, further reducing the available points of attack against this device.

2.2.2.3 SSH Rule Test

The rule requiring that SSH be used for remote management is a fairly easy one to test. Simply utilizing an SSH client on the management network should verify that it is possible to logon to the Cisco router with a valid account. Attempts to login with SSH to the filtering router from either an external host, or any internal host not on the management LAN, should fail. To further verify that only these encrypted communications are being permitted, connections should also be attempted via the unsecured telnet protocol from both external and internal interfaces. These connections will fail because telnet has not been defined as an allowed protocol for terminal line access.

3 Audit Your Security Architecture

You have been asked to conduct a technical audit of the **primary firewall** (described in Assignments 1 and 2) for GIAC Enterprises. In order to conduct the audit, you will need to:

Plan the audit. Describe the technical approach you recommend to assess the firewall. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

Conduct the audit. Using the approach you described, validate that the primary firewall is actually implementing GIAC Enterprises' security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

Evaluate the audit. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

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

3.1 Audit Plan

Before performing a security audit on a device such as a primary (or external) firewall, written permission from senior management must be obtained. Security audits can be extremely intrusive and can, in and of themselves, result in system crashes, exposures, and other detrimental effects. For this reason it is imperative that the support of senior management be obtained well in advance and that the parameters of the audit be carefully established before any activities are undertaken by the audit team. The audit team itself should *not* include anyone who is responsible for maintaining the device. A third-party consulting firm, for example, should be preferred over internal GIAC Enterprises employees.

If the make and model of the firewall are readily identifiable, the first step of the audit should consist of a search for all patches and updates to the existing software and hardware. It is critical to verify that all of the most recent security patches have been applied. Given the multitude of vendors whose products are included in a typical perimeter security system, it is very easy for a harried IS team to overlook the latest and greatest software revisions. If the model of the target system is unknown, tools such as nmap should be used to attempt to fingerprint the device for identification.

A security scanner, such as the open source Nessus product or the commercial ISS Security Scanner, can be used to scan the firewall for known vulnerabilities and to verify system performance against attacks. These tools provide an excellent means of simulating a large number of known forms of attacks against a firewall or other host. This is one of the most intrusive portions of a security audit and care should be taken to ensure that this procedure not effect production traffic. In the interest of minimizing the chances of disrupting business operations, these scans are typically performed during non-business hours.

In conjunction with performing the security scan against the firewall, the logs generated by that firewall should be reviewed to ensure that these forms of (hopefully) denied traffic are being logged as expected. Without proper logging, a network administrator may never know that his or her network was being attacked and would not be able to respond appropriately to incidents of this nature.

Security websites and mailing lists such as Bugtraq should be consulted for updates on recently discovered vulnerabilities in the firewall system – vulnerabilities which may or may not have been acknowledged and/or patched by the system's vendors.

Again, during non-business hours, a system reboot of the firewall system should be performed to ensure that the system could recover from a power outage or other system failure in an automated and secure fashion. All relevant boot logs and startup scripts should be reviewed to ensure that the appropriate firewall rule sets and scripts are being executed with the desired effects. A key rule may have been added to or modified on the firewall and never saved to disk. Upon reboot, rules that prevent known attacks or malicious traffic may not be present!

If the firewall system is a general-purpose operating system, it should be audited for any privileged programs and utilities. If any such utilities are found, they should then be evaluated on a case-by-case basis to ensure that their particular privileges are necessary to proper system operation and do not constitute a security vulnerability. The system audit must also check to see that no extraneous services, such as http, mail, or news servers, are running on the firewall system. The firewall must be dedicated solely to its policy enforcement function: extraneous services greatly increase the number of attack vectors present on the system.

In a real-world scenario, the audit team would also be expected to complete a physical security assessment of the firewall's environment to determine whether physical access to the device can be obtained. Gaining physical access to the network is a trump card to an attacker. Firewall rules become irrelevant when an outsider can plug directly into the internal network or otherwise circumvent the firewall device in the attacker's connection path.

A review of all GIAC Enterprises employees with access to the firewall should also made in order to establish that only those individuals with current management responsibilities enjoy authorization privileges. Procedures for dealing with transferred or terminated employees must be audited to ensure that they are current and are being applied as a matter of course. Many corporations suffer from "authorization creep": individual employees gradually accumulate more and more access privileges as they transfer from one position to the next without relinquishing access to resources that they no longer need. A security audit provides an opportunity to stem the tide of this proliferation of unnecessary authorizations. It is also a good moment to make sure that training guidelines are being followed and that knowledge transfers are being effected in such a manner as to promote a skilled operator set.

Finally, a report will be drafted that documents the findings of the auditors. This report should be revisited on a regular basis and should be used as a baseline for comparison against subsequent audits, which should be performed every six months. When used proactively, an audit report can be a powerful tool for maintaining the long term health and security of a corporate firewall system.

The labor required to run an automated scan tool such as Nessus may be estimated at two hours for a single host. A review of the documentation of the written security policy of a company by an independent auditor may be estimated at four hours. An additional four hours will be required for research on patch availabilities and recent exploits, while an additional four hours will be dedicated to documentation. The audit as a whole may be estimated to require approximately 14 hours of a security engineer's time.

3.2 Conduct Audit against the External Firewall

To initiate our evaluation of the external firewall, Nessus v1.0.9 has been loaded on a machine connected to the external interface of the firewall. Nessus contains a large suite of pre-compiled tests in its default installation. These plugins are being continually enhanced and expanded as new exploits are developed. To ensure that the most recent set of tests and audits has been installed, the `nessus-update-plugins` script is used to retrieve the most current set from the Nessus web site.

After the Nessus run has been completed, the logs from the firewall are checked to ensure that proper logging of the intrusion attempts has occurred.

Exploit websites such as Bugtraq, Incidents.org, and ArachNIDS, and vendor websites – in this case Checkpoint and Nokia – should be checked for recently released patches, exploits, or configuration pratfalls.

On a typical host OS, the external firewall would then be rebooted and the contents of the dmesg and /var/log/messages files reviewed for any potential vulnerabilities or unexpected system behavior. A "find / -perm +6000 -ls" would also be executed on the firewall to look for any setgid or setuid binaries. These two UNIX permissions enable programs to run with elevated permissions and constitute a potential security risk. Any binaries found to have these permissions must be evaluated on a case-by-case basis to determine whether or not their elevated privileges are necessary to their proper operation. A check against the /etc/passwd file would also be carried out to ensure that no unknown or unauthorized users have permission to log into the firewall. Any unnecessary entries should be disabled. Finally, a check is made to ensure that all unnecessary network services, such as NFS, http, news, etc. are disabled in all system boot scripts.

The results of this audit are then summarized, signed by company officers and the outside agency conducting the audit, and then stored in hard copy format. This provides legal assurance to both GIAC Enterprises and the auditing parties that the security audit has in fact been conducted.

3.3 Summary of Results

Because a Nokia IPSO hardened operating system has been adopted, services that would be available on a more generic multi-purpose OS, such as UNIX or Windows, are not present. Nokia's IPSO is a pre-audited system that has already been subject to a great deal of commercial hardening. Nessus scans against the external firewall would be inconclusive because the Checkpoint FW-1 product implements a set of implied "stealth rules" that silently drop any traffic that is destined for the IP address of the firewall itself.

Overall, the results of the audit cast a favorable light on GIAC Enterprises' security policies. Searches on the Security Focus, Checkpoint, and Nokia websites confirm that no exploit or flaws are currently available for the deployed architecture. However, close tabs must continue to be kept on the relevant Checkpoint and Nokia announcement lists, with an eye out for security advisories as new exploits and patches are developed. The staff of GIAC Enterprises should repeat the audit against the firewall and all security infrastructure equipment on a regular basis, in order to guarantee that the company's security policy keeps abreast of changing configurations and technologies.

Alternative security technologies that GIAC Enterprises may wish to investigate include the use of Network Address Translation (NAT) to conceal all internal hosts and services behind a limited pool of public IP addresses. NAT provides a layer of independence from IP addressing issues and it also offers a layer of indirection against external snoopers who might attempt to map and access internal services.

In addition, switching from Triple-DES encryption to the AES encryption standard could further strengthen the encryption used in the VPN architecture. This new standard is regarded as both more secure and more efficient than DES encryption variants. While both the Checkpoint VPN-

1 and Secure Client software support AES, there is currently no card on the market that can perform hardware acceleration of the AES algorithm. For this reason, any move from accelerated Triple-DES to AES should be carefully tested to ensure that the existing Nokia devices are capable of handling the increased load.

Reliance on a single connection from GIAC Enterprises to the public Internet represents a weakness in the proposed design. For true redundancy, GIAC Enterprises should consider separate physical circuits to independent connectivity providers. An alternate architecture providing this additional layer of redundancy might look like this:

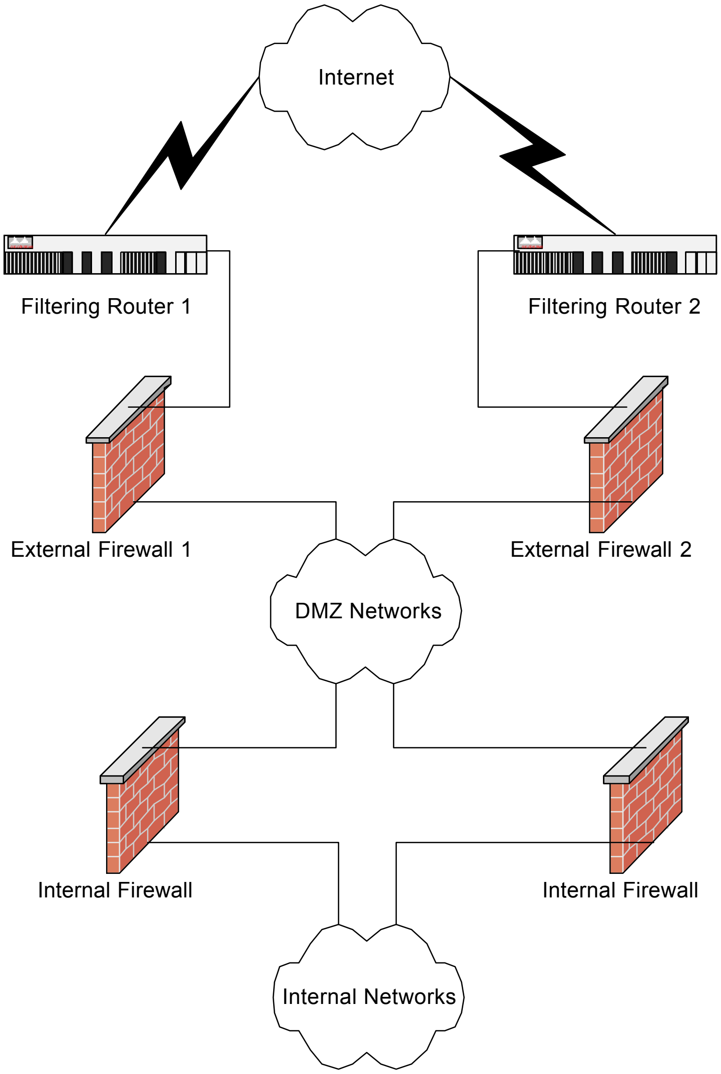

Figure 2: Redundant Network Architecture

The existence of multiple ingress and egress points introduces substantial additional complexity of design and configuration and this has therefore not been implemented in the current design.

None of the architectures discussed thus far address the issue of managing quality of service (QOS) on existing network links. Without implementing QOS controls, it is possible for less important traffic, such as internal web surfing, to starve business-critical traffic, such as customer secure web traffic, of bandwidth. To provide a consistent level of service under a multitude of conditions, a QOS shaping product such as Checkpoint's Floodgate-1 may be used to monitor and enforce appropriate classes of service on inbound and outbound traffic.

4 Design under Fire

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

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

An attack against the firewall itself. Research and describe at least **three** vulnerabilities that have been found for the type of firewall chosen for the design. Choose **one** of the vulnerabilities, design an attack based on the vulnerability, and explain the results of running that attack against the firewall.

A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.

An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

In designing your attacks, keep the following in mind:

The attack should be **realistic.** The purpose of this exercise is for the student to clearly demonstrate that they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

The attack should be **reasonable.** The firewall does not necessarily have to be impenetrable (perfectly configured with all of the up-to-the-minute patches installed). However, you should not assume that it is an unpatched, out-of-the-box firewall installed on an unpatched out-of-the-box OS. (Remember, you designed GIAC Enterprises' firewall; would you install a system like that?)

You **must** supply documentation (e.g., a URL to the security bulletin, bugtraq archive, or exploit code used) for any vulnerability you use in your attack.

The attack does not necessarily have to succeed (though a successful attack is often the more interesting approach). If, given the perimeter and network configuration you have described above, the attack would fail, you can describe this result as well.

4.1 Chosen Baseline System

Susan Caskey's network perimeter security design, available at http://www.sans.org/y2k/practical/Susan_Caskey_GCFW.zip, is the reference implementation for the attack portion of this exercise. Susan's architecture is very robust and it will prove a difficult nut to crack! The reader is encouraged to don his or her black hat as we investigate potential vulnerabilities in this particular design.

Susan's proposed architecture is diagrammed below:

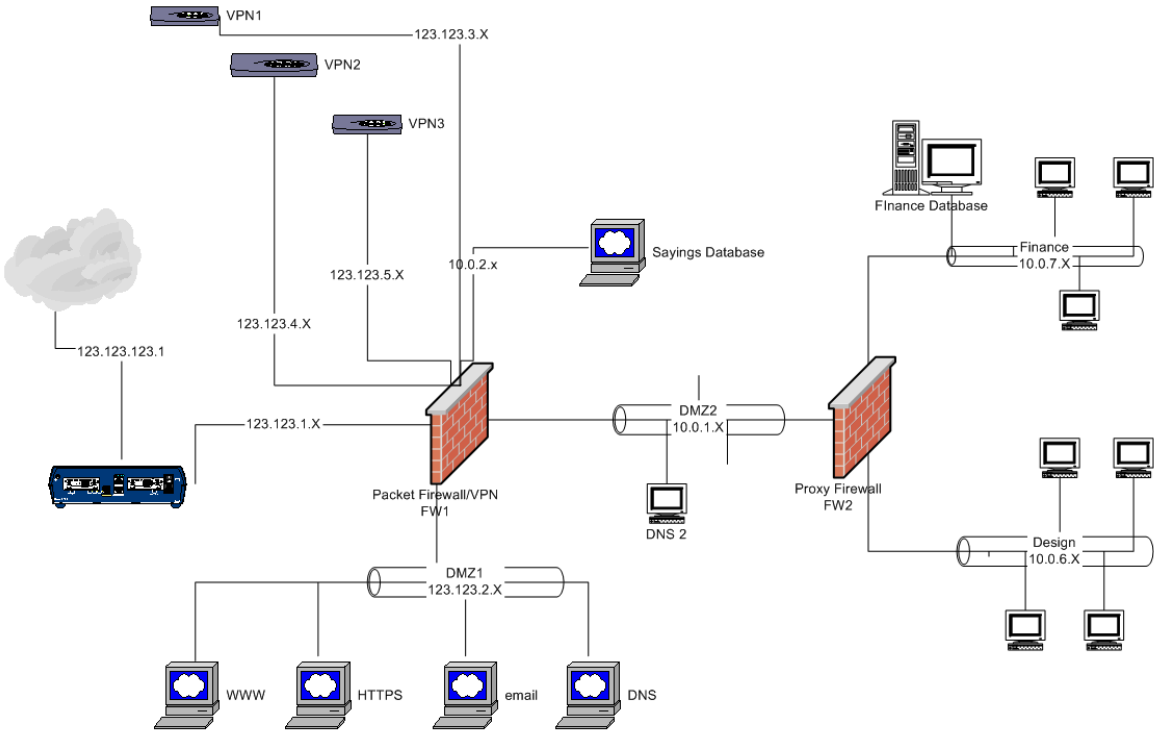

Figure 3: Attack Network Diagram

4.2 Firewall Attack

Susan's external firewall is a Checkpoint FW-1 firewall running on a Solaris 7 machine. The precise version of FW-1 is not specified, but based on the screen shots provided in the architecture, it would appear to be 4.1. It is also not possible to determine the patch level based on the assignment write-up. Solaris 7 was chosen as the host OS. Solaris is a full-fledged multi-user operating system. Failure on the part of an administrator to fully harden the OS, whether through neglecting to implement all of the current security patches or through failing to remove unneeded services, can result in a vulnerable system.

4.2.1 Attack 1 – Fragmented Packets DOS Attack

A recently reported DOS attack -- posted on Bugtraq (http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1312) -- can affect Checkpoint's Firewall-1 product. By sending ICMP packets with illegal packet fragmentation flags set, it is possible to lock up the FW-1 logging module, causing the FW-1 host to consume all CPU resources and halting all further logging of traffic. This attack could be launched to slow down processing on the firewall or, alternatively, the attack could be launched as a distraction against a second attack, which would then not be logged. This exploit was patched in Service Pack 2 of Checkpoint's 4.1 Firewall-1 product. Because this service pack was released in October of 2000, it is likely to have been deployed in Susan's architecture, but verifying its installation would be advised.

4.2.2 Attack 2 – Valid Username Vulnerability

An additional open vulnerability in Checkpoint FW-1 has been reported, also on Bugtraq (http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=1890). Directing bogus login attempts to the FW-1 box can permit would-be intruders to determine whether a user name is valid or invalid. This is an information leak that may be exploited to establish a list of valid usernames on a system. Once this list has been generated, an attacker may then proceed with a brute force hack against those usernames. This exploit behavior has been corrected with the NG (Next Generation) version of Checkpoint's FW-1 product. However, no fix has been issued for the 4.1 generation of Checkpoint's software, and this represents an active exposure in Susan's architecture.

4.2.3 Attack 3 – RDP Communication Vulnerability

In June of 2001, Checkpoint reported (http://www.checkpoint.com/techsupport/alerts/rdp) a potential exploit in their proprietary RDP protocol that may enable a hacker to craft packets that bypass an installed rule base, allowing otherwise blocked traffic to pass through a Firewall-1 platform. This behavior was first corrected in a version 4.1 SP 4 hotfix, yet Checkpoint has continued to roll out additional post SP 5 revisions of this patch, the most recent of which was made available as recently as Oct 25th. Unless the GIAC administrative team remains very vigilant, this could pose an active exploit for Susan's network.

4.2.4 Hypothetical Attack

An outside attacker seeking to penetrate Susan's architecture might attempt to "fingerprint" the systems being used at GIAC Enterprises with the help of a scan tool such as nmap. However, such a scan would likely reveal very little about the primary firewall because the policies installed on the external firewall in Susan's architecture deny all traffic from the outside networks that is directed at the firewall itself. Owing to the large installed base of Checkpoint products in enterprise environments, an attacker may attempt to crack the VPN connection. Through the use of a command line telnet client, a connection may be established to the VPN concatenator in Susan's architecture. Entering a login ID for an account that does not exist on GIAC Enterprises' authorized VPN users list will generate a "User ID invalid" message. Attempting to login with an existing user ID using an incorrect password generates a "Login incorrect message". Once the attacker has a valid user ID, it simply becomes a matter of brute forcing the password, trying various common passwords and their permutations, until access is gained. Given the computing horsepower and bandwidth available to even a casual home user, this is a relatively trivial task. Once the password has been obtained, the intruder will then have all of the rights and privileges needed to tour GIAC Enterprises' internal network.

4.3 Denial of Service (DOS) Attack

Under Susan's architecture, a DOS attack of middling sophistication launched against the primary GIAC Enterprises Internet connection could result in a loss of connectivity between GIAC and the public Internet. As was demonstrated during the highly publicized DOS attacks of Feb. 2000, denial of services attacks are a problem for which there is no easy solution. Assuming that 50 home machines equipped with cable modems were to be compromised, the sustained maximum data throughput of these machines would exceed 6 Mbps (50 stations @ 128 kbps). With only two T1 channels, this attack network might easily saturate GIAC Enterprises' 3.088Mb (1.544 Mb per T-1 circuit) of aggregate capacity, cutting GIAC Enterprises off from the Internet. While this traffic would be rejected by the firewall, by that time the pipe feeding the GIAC network would already have been flooded with the attack traffic.

So long as control is exercised only at the narrow end of the bandwidth choke point, there is no way for GIAC Enterprises to effect a remedy. Combating such a DOS attack would require the assistance of the connecting ISP, which might selectively block traffic or even implement rate limiting on the traffic flow. Because many of the common DOS attack clients, such as mstream and TFN2K, utilize spoofed source IP addresses, this entire class of attacks would be made much more difficult to implement if all ISPs implemented rudimentary anti-spoofing filtering on their local networks. Unfortunately, it does not appear likely that this will happen any time soon, and the victims of these attacks are left with few options other than to contact their upstream providers when a attack occurs or, alternatively, to provision their network connections with an excess of bandwidth at all times.

In demonstration of this form of attack, consider the following scenario. Residential cable modem users are a frequent target of would-be attackers. This population shares a set of characteristics that make it highly attractive to an attacker, including substantial bandwidth (up to 1.4 Mbps per computer), a less vigilant security posture, and a high percentage of users running systems that are not well secured. If our would-be intruder had been able to compromise approximately 50 of these clients using an automated tool such as the NIMDA virus, he or she might then proceed to install a DDoS tool such as Wintrinoo.

The current generations of DDoS tools capitalize on the multi-tiered computing hierarchies that have served legitimate e-businesses so well. With Wintrinoo, an agent program is installed on multiple compromised machines. These clients, commonly referred to as zombies, can then be controlled remotely via a separate host, or controller, machine, thereby isolating the attacker from ever direct participation in an attack on a system. When activated from their control source, the zombies awaken and can be used to flood a target system with traffic. This architecture is outlined in the diagram below:

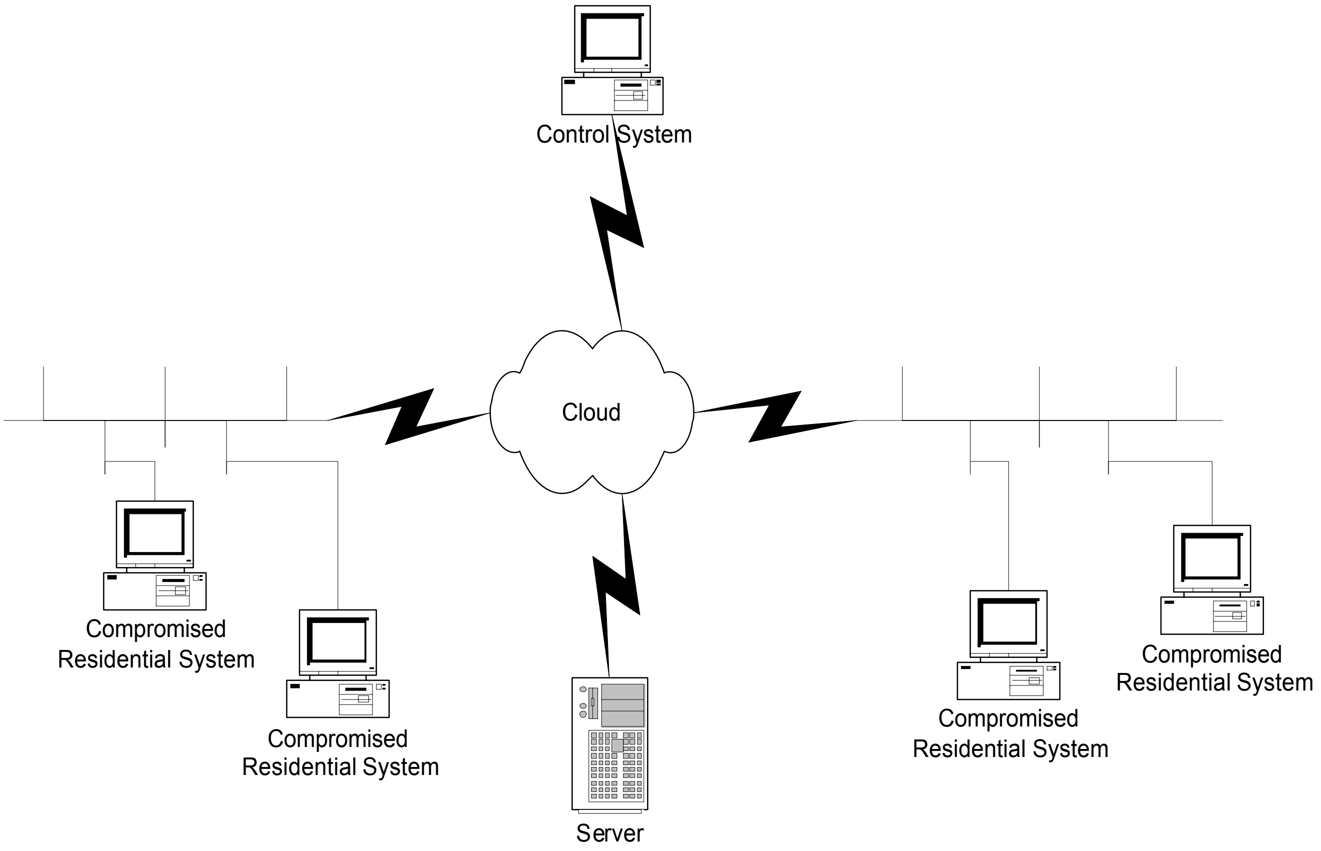
Control System
Cloud
Compromised Residential System
Compromised Residential System
Server
Compromised Residential System
Compromised Residential System

Figure 4: DDoS Architecture

In the case of Wintrinoo, the most common variant of DDoS attack is a simple UDP flood: packets of garbage data are encapsulated in UDP datagrams and thrown at random ports on a target system. Fifty compromised systems averaging a very conservative 100 Kbps of traffic generation capability per second would generate a flow of over 5 Mbps of attack traffic. This would completely saturate Susan's dual T-1 links, starving legitimate traffic of any opportunity to even enter the pipe to GIAC Enterprises and effectively cutting GIAC Enterprises off from the Internet.

4.4 Internal System Compromise through Perimeter System

Reviewing Susan's architecture, the BIND DNS servers intended to handle DNS needs present a particularly attractive target. A potential black-hat attacker might easily run a whois query against the GIAC Enterprises' domain name, quickly returning the name and IP addresses of the DNS servers involved. Susan does not specify the particular version of BIND that is being run in her architecture, but there is a strong chance that BIND 8.x, the most widely deployed version of this daemon, is being run. BIND 8.x has a spotty history and its various incarnations are known for their security vulnerabilities. Many of these weaknesses have been incorporated into automated scanning tools used by "script kiddies" running pre-written hacking tools, often with little or no knowledge of how or why these tools function.

A quick check on Bugtraq (http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=exploit&id=2302) reveals a major flaw that is still receiving attention. This buffer overflow exploit thoughtfully includes exploit code. Because the proposed BIND architecture allows both UDP and the more complex TCP protocol to be used for queries, this code could be run against the DNS server to compromise the system. BIND typically runs as root and any compromise of this service therefore grants the attacker root access on the target system.

Assuming that a perimeter system has been compromised, the internal defenses of GIAC Enterprises are then put to the test. The most obvious vulnerability in the perimeter systems is the fact that all internal traffic is unencrypted. As a result, potentially sensitive information, including login ids, passwords, and email, is transmitted in the clear. In the target design, the VPN connections from the Internet are terminated at the external firewall. Once traffic leaves this point, it is an easy target for potential eavesdroppers on either the DMZ or internal networks. A particular vulnerability lies in the POP3 traffic that the VPN users utilize for mail retrieval. The POP3 protocol transmits unencrypted passwords across the network. This enables any eavesdropper to harvest email IDs and passwords, which are often the same as users' login credentials. The mail itself is also being sent in the clear between the VPN tunnel end points and the internal mail servers, which exposes it to alteration or copying along the way. Moving the encryption end point to an internal system, and mandating that all transactions also be encrypted, would alleviate this problem. A thorough evaluation of all traffic on the DMZ should be performed to identify any other traffic sources that may also be unencrypted.

5 References

AMaViS URL: http://www.amavis.org/ (31 Oct. 2001)

ArachNIDS URL: http://www.whitehats.com/ids/index.html (30 Oct. 2001)

Bugtraq URL: http://www.securityfocus.com/archive/1 (30 Oct. 2001)

CheckPoint URL: http://www.checkpoint.com/ (29 Oct. 2001)

Concurrent Versions System URL: http://www.cvshome.org/ (24 Nov. 2001)

Djbdns URL: http://cr.yp.to/djbdns.html (20 Oct. 2001)

F5 Networks URL: http://www.f5networks.com/ (22 Oct. 2001)

Finisar Systems, In-Line Taps URL: http://www.finisar-systems.com/htdocssh/products/taps/index.html (16 Nov. 2001)

FirstVPN Virtual Private Networks URL: http://www.firstvpn.com/products/prod10-1.html (08 Nov. 2001)

Hping home page URL: http://www.hping.com (11 Nov. 2001)

Houle and Weaver, "Trends in Denial of Service Attack Technology" URL: http://www.cert.org/archive/pdf/DoS_trends.pdf (Oct. 2001)

Incidents.org URL: http://www.incidents.org/ (30 Oct. 2001)

Insecure.org URL: http://www.insecure.org/ (08 Nov. 2001)

Internet Security Systems, Inc. URL: http://www.iss.net/ (31 Oct. 2001)

NET-SNMP Project URL: http://www.net-snmp.org/ (16 Nov. 2001)

Nokia Security Solutions URL: http://www.nokia.com/securitysolutions/pdf/IP330_global.pdf (20 Oct. 2001)

Oracle Corporation URL: http://www.oracle.com/ (23 Oct. 2001)

RFC 1918 URL: http://sunsite.dk/RFC/rfc/rfc1918.html (29 Oct. 2001)

SecuritTeam.com, Brute Force SNMP Scanner URL: http://www.securiteam.com/tools/5VP0I000AO.html (18 Nov. 2001)

SNMP Brute Force Attack URL: http://www.solarwinds.net/Tools/Security/SNMP_Brute_Force/ (18 Nov. 2001)

Snort URL: http://www.snort.org/ (28 Oct. 2001)

Squid URL: http://www.squid-cache.org/ (28 Oct. 2001)

VanMeter, Charlene. "Defense in Depth: A Primer" URL: http://www.sans.org/infosecFAQ/start/primer.htm (10 Nov. 2001)

Wintrinoo URL: http://www.jmu.edu/computing/info-security/engineering/issues/wintrino.shtml (08 Nov. 2001)

6 Appendix 1: Checkpoint Object Definitions

Object	Definition
Authentication_Server	SafeWord authentication server.
Filtering_Router	Filtering Cisco router.
Fortune_Database	Oracle database server.
Gateways	External and internal firewalls.

Internal_Firewall	Internal firewall and VPN concentrator
Internal_Net	Devices on the employee or management sides of the Internal Firewall.
Internal_SMTP_Server	Internal mail server.
Intranet_Server	Intranet web server located on the internal services network.
Management_Network	Dedicated network management segment.
Primary_DNS_Server	Authoritative DNS server located in DMZ.
Relay_SMTP_Server	Relay mail server located in the DMZ.
Secondary_DNS_Server	Authoritative DNS server hosted by third-party.
Time_Server	Master time server located in the DMZ.
Web_Cluster	Web servers and load balancer.
Web_Proxy_Server	Squid web proxy located in the DMZ.

Table 3: Checkpoint Object Definitions

7 Appendix 2: Checkpoint Ruleset

[DNS Queries are allowed by the global properties definition and are therefore not listed in the ruleset. The FW-1 product also has the ability to specify a time period during which a particular rule is to be applied. Because all of GIAC Enterprises' rules are enforced around the clock, this option is not listed here.]

Source	Destination	Service	Action	Track	Install On
Partners@Any Remote_Employees@Any	Internal_Net	FTP HTTP HTTPS POP3 SMTP SSH	Encrypt	Long	Internal_Firewall
Management_Network	Gateways	FW1	Allow	Long	Gateways
External	Web_Cluster	HTTP HTTPS	Allow	Long	Gateways
External	Internal_Firewall	IPSEC IKE	Allow	Long	Gateways
Internal_Net	Any	SSH	Allow	Long	Gateways
External Relay_SMTP_Server	Relay_SMTP_Server External	SMTP	Allow	Long	Gateways
Web_Proxy_Server	External	HTTP HTTPS	Allow	Long	Gateways

Primary_DNS_Server	Secondary_DNS_Server	SSH	Allow	Long	Gateways
Filtering_Router	Management_Network	IPSEC IKE	Allow	Long	Gateways
Filtering_Router Internal_Net	Authentication_Server	Tacacs+ LDAP	Allow	Long	Gateways
Filtering_Router Internal_Net	Time_Server	NTP	Allow	Long	Gateways
Internal_Net	Intranet_Server Web_Proxy_Server	HTTP HTTPS	Allow	Long	Gateways
Internal_SMTP_Server Relay_SMTP_Server	Internal_SMTP_Server Relay_SMTP_Server	SMTP	Allow	Long	Gateways
Intranet_Server Web_Cluster	Fortune_Database	Sqlnet	Allow	Long	Gateways

Table 4: External Firewall Ruleset