Global Information Assurance Certification Paper

SANS GCFW Practical Assignment

Mark Fennig
Great Lakes SANS
Nov 5, 2001 – Nov 9, 2001
Version 1.6a
Submitted January 8, 2002

In This Document:

Security Architecture

Organization Overview

GIAC Enterprises is an e-business dealing primarily in the creation and distribution of fortune cookie sayings. The company itself consists of over 100 employees for its own internal operations. To actually create fortunes, GIAC uses the services of freelance writers who are paid a flat fee for each unique fortune submission and then royalties based on a fortune's distribution.

GIAC's primary customers consist of over 650 fortune cookie manufacturing companies in North America that lack the resources to produce accurate fortunes. Additionally, GIAC has two business partners in Brazil and Singapore who purchase fortunes at a discount, translate them and then resell them to fortune cookie manufacturers in South America, Southeast Asia, and Japan.

Access Requirements

In order to meet GIAC's operational needs, the following access requirements must be provided for.

GIAC Employees – Employees require the ability to send and receive email and access HTTP/HTTPS resources on the Internet. Ftp, telnet, and Secure Shell access will occasionally be needed too. However, being an e-commerce oriented business, GIAC generally desires its employees to have free access to most Internet resources as long as they conform to GIAC's acceptable use policies. The IT administrative staff requires the ability to perform traceroutes and pings over the Internet for debugging and testing purposes. Remote access to the GIAC network is required for employees on the road and for remote support by the IT administrative staff.

Fortune Writers – Anyone may become a fortune writer and submit fortunes to the GIAC fortune database for potential acceptance. To do this, a prospective writer must establish an account via a secure (SSL-enabled) website operated by GIAC. Once an account is established, the writer may submit fortunes online using this website.

Customers – Fortune cookie manufacturers (or anyone interested in fortunes) may select and purchase fortunes in lots of 10, 50, 100, or 1000 from a web catalog and ordering system operated by GIAC. Payment is exclusively by credit card or via purchase order that has been previously arranged for. All ordering and payment activity is done through a secure SSL-enabled web site operated by GIAC.

Business Partners – GIAC's business partners require direct access to the Fortune database so they can search for and extract fortunes that are relevant and

easily translated for customers in the various countries they service. To provide this access, a site-to-site (or, gateway-to-gateway) VPN will be established between the GIAC network and networks of the two business partners.

Network Security Design

The IT staff at GIAC has adopted a "defense in depth" stance to security and will therefore utilize several methods of securing their network and business data. This will include packet filtering at the border router, a firewall, anti-virus scanning, host hardening, and VPN technology when needed. All Internet access to GIAC services (e.g., email, web, and DNS) will be via a service network that is firewalled from both the Internet and the GIAC internal network. Intrusion detection sensors will also be placed at key network locations. Hosts that provide key services (firewall managemnt, email, syslog, database, DNS, web, etc) will be hardened by installing the latest security patches and using recommendations as found in guidelines such as the SANS step-by-step publications. This hardening will include eliminating services like telnet, ftp, and rlogin/rsh in favor of SSH (protocol 2).

Figure 1 on the next page diagrams the network design and shows all key components and subnets. Following are the details associated with each of these components.

Network Addressing

GIAC has procured a registered, public Class C address block for their service network and a 16-address block for their DMZ network. The network addresses for these networks are 111.2.2.0/24 (DMZ) and 111.1.1.0/28 (service network). Internally, GIAC will be using an unregistered private address space of 172.25.0.0/16, since it does not have enough registered addresses to cover its internal needs.

Note: The service and DMZ network addresses used for this document are actually from a currently reserved address block. They are being used for illustration only. For the purposes of this document, these addresses are to be considered valid and publicly routable.

Internet Connectivity/Network Bandwidth

GIAC's Internet feed consists of two 1.54 megabit circuits provided by a single ISP. Internally, most workstations and servers connect into a switched 100mb, full-duplex network. The service network and subnet just inside the firewall operate at 100mb, half-duplex to allow for the ready use of network sniffing tools by the administrative staff and the deployment of the network IDS devices.

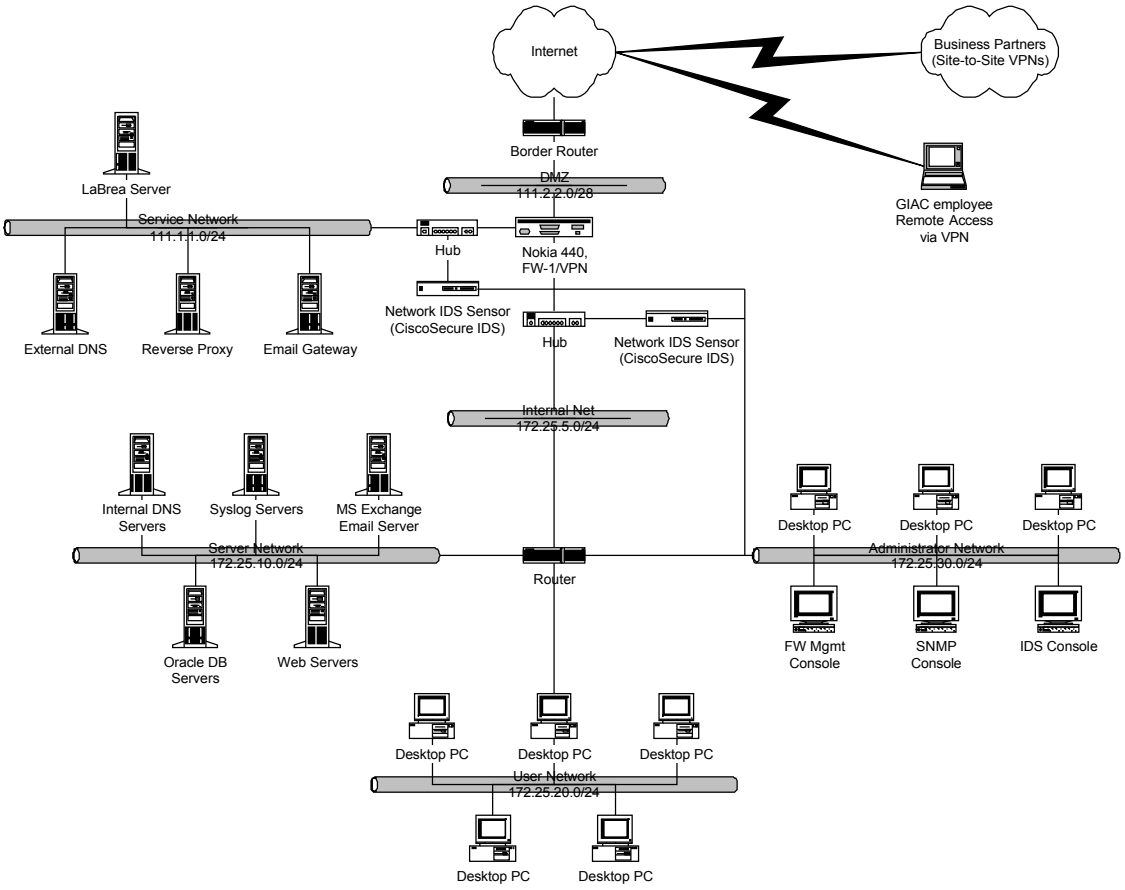

Figure 1

Border Router

A Cisco 7200vxr model router running IOS 12.2 will be deployed at the boundary connecting GIAC's networks and their ISP. Although Internet connectivity and routing is the primary purpose of this router, GIAC will also utilize the router's filtering capabilities to eliminate at least some of the obvious undesirable inbound and outbound traffic (ingress and egress filtering). For example, all inbound traffic must have a valid, publicly addressable source address. And outbound traffic must contain source addresses from GIAC's public address block.

DMZ Network

The network segment connecting the border router and primary firewall is the DMZ. There are no services intended to be deployed on the DMZ. However a LaBrea host (described later) will be placed on this subnet.

Firewall

The firewall consists of a Nokia i440 firewall appliance running IPSO 3.4.1 as its operating system and Checkpoint Firewall-1 version 4.1, service pack 5 for the firewall services. SSH (protocol 2) and HTTPS will be the only remote access services started on the firewall for providing administrative access. The firewall appliance will be configured with a third network interface to support a service network.

All traffic originating from the GIAC internal network will use network address translation (NAT) to "hide" behind the IP address of the firewall's external interface. This is necessary since GIAC does not have a large enough registered IP address block to cover its internal needs. It also has the benefit of keeping its internal devices from being addressable from the Internet. NAT will not be applied to traffic passing from the internal network to the service network or from the service network to the Internet.

GIAC will utilize the VPN capabilities of Firewall-1 to provide remote access for authorized employees and to establish site-to-site VPN tunnels with business partners.

Firewall Management Console

The Firewall-1 management console will be installed and operated from a Sun UltraSparc 2 workstation placed on an internal administrator's subnet. All firewall policy management will be controlled from this console. In addition all firewall logs will be directed to this console. Log files will be rotated on a daily basis at 23:59CST. There will be enough disk space available to retain at least 45 days worth of logs.

Intrusion Detection Sensors

GIAC will deploy two CiscoSecure IDS (version 3.0(2)-s11) sensors to detect suspicious or malicious network traffic. One sensor will have its promiscuous-mode sensing interface connected to the service network and the other sensor will have its interface on the network path just inside the firewall. Each sensor has a second interface connected to the internal network. These "internal" interfaces are used to administer and monitor the sensors and for the sensors to report data and alarms to an IDS console. There is no IP forwarding between the promiscuous interfaces and internal interfaces. The IDS console is a Sun Sparc Ultra-2 running Solaris 8. The console software consists of CiscoSecure Director (version 2.2.3-s11) and HP Openview (version 6.1).

Service Network

The service network is a separate subnet off it's own firewall interface. Inbound traffic from the Internet will only be allowed to connect to devices on this network. However, devices on the service network will have to communicate with

the internal server network to read or write data or complete various transactions. No permanent business data will be stored anywhere on the service network.

An intrusion detection sensor will be placed on the service network since it and its hosts are likely targets for an attack.

DNS Servers

GIAC will utilize a split-DNS configuration in order to hide its internal address space and servers, and to avoid extending DNS-related attacks into the internal network. The primary external DNS server will be hosted on the service network. GIAC has arranged with its ISP to host a secondary external DNS server. GIAC's primary DNS server will be configured to only allow zone transfers to the ISP's DNS server. It will also be configured to only provide recursive lookups for hosts on GIAC's service network.

> **Tips, Hints, Gotchas:** If your ISP is hosting a DNS service for your organization you should check with them to ensure they are configured so no one may transfer your zone information from their DNS server.

Internally, GIAC will host primary and secondary DNS servers. The zones for these DNS configurations will include all internal hosts and hosts on the service and DMZ networks.

All DNS services will run on Sun Sparc Ultra-2 servers, running Solaris 8. As part of the host hardening however, the DNS package (BIND) shipped with Solaris will be replaced with the most current release (currently 9.2.0) found at http://www.isc.org/products/BIND.

Reverse Proxies

All Internet-accessible GIAC websites are hosted on the service network by reverse proxies that map theirURLs to an internal web server. This allows all servers containing the actual web content to remain behind the firewall. Additionally, any communication between those web servers and associated application, database, or other back-end servers can remain behind the firewall. Use of reverse proxies also leaves open the possibility of performing some filtering on connections to the service network. A network diagram showing the relationships between Internet clients, proxies, web, application, and back-end servers is shown in figure 2 below.

All proxy instances for websites handling customer orders, business transactions, or other sensitive data will be SSL-enabled. GIAC will create these proxy instances using I-Planet Proxy Server 3.6 on Sun Sparc Ultra-2 servers, running Solaris 8.

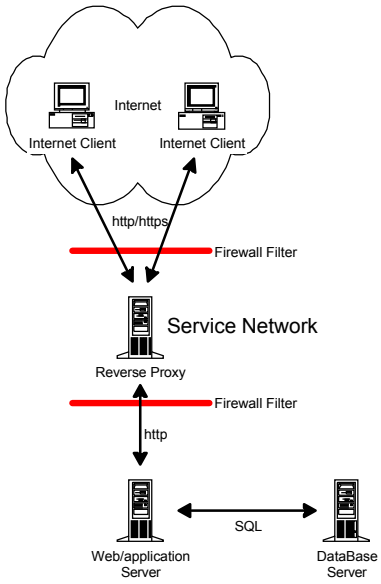

Figure 2

Email Gateway

GIAC's email (SMTP) gateway will be hosted on a MS Windows 2000 server running Content Technologies/Baltimore MailSweeper version 4.25. MailSweeper will filter incoming and outgoing email for spam and other undesirable content. In addition, the email gateway will utilize a plug-in module (Sophos AntiVirus AVI version 3.5.3) to filter out virus-infected email. Special care will be taken to ensure this gateway is not configured to be an open SMTP relayer. All email entering and leaving the GIAC network must go through this gateway. See figure 3 for a diagram showing the dataflow between this gateway and the Internet and GIAC's MS Exchange email server.

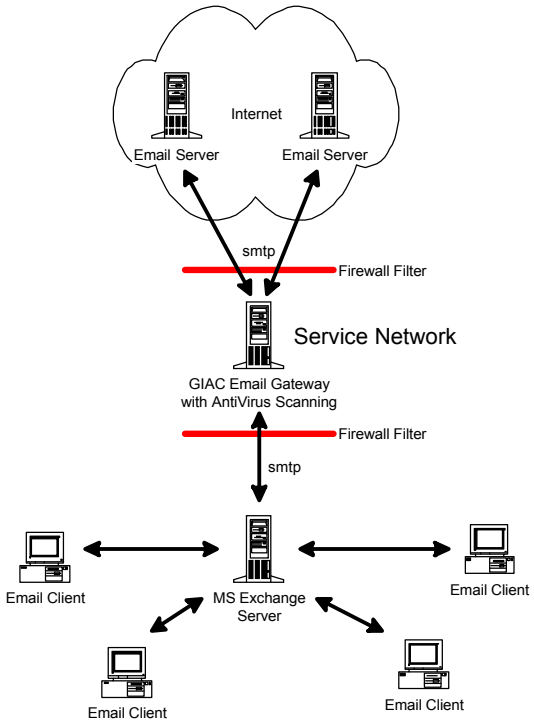

Figure 3

LeBrea Server

A PC running Trinux with the LaBrea package will be connected to both the service network and DMZ. These devices will create "virtual hosts" for all unused addresses on these networks. The LaBrea server will respond to all connection attempts to these virtual hosts in such a way that the connections are kept open and the connecting host is left waiting for a response. The goal here is to bog down or "tarpit" scan attempts or worm proliferation against the GIAC network. Since GIAC's DMZ address space is small and most of the service network addresses will be filtered, the tarpitting feature may not provide a huge benefit. However, the LaBrea connection logs should provide information to augment or complement the data picked up by the network IDS sensors.

Email Server

The internal email server for GIAC is MS Exchange 2000 running on an MS Windows 2000 server. Most internal users will use Microsoft Outlook for a mail client. Due to the MS Exchange/Outlook track record in attracting viruses and other malicious code, MailSweeper will also run on this server to filter and reject email containing certain filetypes (e.g., *.exe, *.vbs, etc).

Syslog Servers

All networked devices on the DMZ, service network, and internal network will forward their syslog data to two internally hosted syslog servers. These servers will be Sun Sparc Ultra-2's with Solaris 8, using the standard syslog package. Swatch will be used on each server to monitor the logs and generate alerts or alarms for various situations.

Web Servers

Due to the requirements of GIAC's web applications and its developers, MS IIS 5.0 web server running on MS Windows 2000 Servers will be used to provide web services. Because of the large number of historical exploits against IIS, special care will be taken to harden these devices and to keep their patch levels current.

Integrity Checking

Tripwire version 2.4.2 will be installed on all Unix and NT servers to help verify the data integrity of those systems. Any detected integrity events will reported by way of an SNMP trap and a syslog entry.

Backups

Backups of data at GIAC are handled by the operations staff and are performed daily. Full backups are done every Saturday, with incremental backups done on all other days. Backups of servers on the internal network are done over the network to a central backup server and tape jukebox. All backups of devices on the service network are done to locally attached tape drives.

Anti-virus Protection and Scanning

All MS Window-based servers and desktop devices will be protected by Symantec AntiVirus Corporate Edition 7.6 software. Virus definitions for both servers and workstations will be rolled out on a regular basis by the administrative staff.

Security Policy

GIAC's security policy can be enforced at several points on the infrastructure. In this section, we look at how the policy is enforced at the border router, primary firewall, and VPN gateway.

Border Router

The border router will be configured with an ingress filter to block packets with invalid source addresses and source addresses from GIAC's public address space. There will also be an egress filter to ensure that all packets leaving the GIAC network contain source addresses from GIAC's public address space. Comments

(italicized) have been included below to help document the purpose of the ACL statements.

Ingress filter

GIAC Public Address Space

```
access-list 101 deny   ip 111.1.1.0  0.0.0.255 any
access-list 101 deny   ip 111.2.2.0  0.0.0.15 any
```

RFC1918 Private Address Space

```
access-list 101 deny   ip 10.0.0.0  0.255.255.255 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
```

Loopback

```
access-list 101 deny   ip 127.0.0.0  0.255.255.255 any
```

Link Local Networks

```
access-list 101 deny   ip 169.254.0.0  0.0.255.255 any
```

Reserved/Unallocated

```
access-list 101 deny   ip 0.0.0.0  0.255.255.255 any
access-list 101 deny   ip 1.0.0.0  0.255.255.255 any
access-list 101 deny   ip 2.0.0.0  0.255.255.255 any
access-list 101 deny   ip 5.0.0.0  0.255.255.255 any
access-list 101 deny   ip 23.0.0.0  0.255.255.255 any
access-list 101 deny   ip 31.0.0.0  0.255.255.255 any
access-list 101 deny   ip 197.0.0.0  0.255.255.255 any
access-list 101 deny   ip 201.0.0.0  0.255.255.255 any
access-list 101 deny   ip 220.0.0.0  3.255.255.255 any
```

Class D (Multicast)

```
access-list 101 deny   ip 224.0.0.0  15.255.255.255 any
```

Class E (Experimental)

```
access-list 101 deny   ip 240.0.0.0  15.255.255.255 any
```

Accept any other source address

```
access-list 101 permit ip any any
```

Note: There is rather large range of unallocated/reserved address space (96.0.0.0 – 126.0.0.0) that could have been added to the above filter. However, since I used addresses from within this block for GIAC's "fictional" public address block, I've purposely left this out of the filter to avoid confusion.

Tips, Hints, Gotchas: If you decide to include reserved/unallocated address space in your ingress filter, remember that it is possible for some of those addresses to be utilized at some point in the future. In that event, those addresses will not have access to your Internet resources until you've modified your ingress filtering accordingly.

Egress Filter

Allow packets with GIAC public source address

```
access-list 105 permit   ip 111.1.1.0  0.0.0.255 any
access-list 105 permit   ip 111.2.2.0  0.0.0.15 any
```

Deny any other source address and log

```
access-list 105 deny     ip any any log
```

Other Router Configuration

There are a few other configurations to be done on the border router to tighten it down a bit.

Restrict administrative and SNMP access to GIAC's administrative network

```
access-list 90 permit 172.25.30.0 0.0.0.255
line vty 0 4
      access-class 90
      login local
snmp server community pamwl RO 90
snmp server community irmmyfp RW 90
```

Send syslog messages to internal syslog server

```
logging trap informational
logging 172.25.10.12
```

Disable unnecessary services

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no ip bootp server
no ip http server
```

Prevent router from giving out network info via ICMP

```
no ip unreachables
```

Prevent against being a smurf amplifier

```
no ip direct-broadcast
```

Tips, Hints, Gotchas: You may want to look into replacing telnet on a Cisco router with secure shell (SSH). Note that only later versions of IOS with IPSec support SSH and only SSH version-1 at that. But even with its known issues, SSH version-1 is probably a better choice than telnet.

Primary Firewall

In this section is written firewall policy based on the access requirements defined previously. This policy also includes statements addressing security concerns not directly stated or implied by the access requirements. Following the firewall policy is a step-by-step guide to implementing this policy using Firewall-1.

Firewall Policy

1. All firewall management and administration will be done locally on the firewall itself, from the firewall management console, or other devices on the administrator's network. No other access to the firewall appliance is permitted.
2. Inbound DNS queries may only be made to the external DNS server on the service network.
3. Only the DNS secondary server, hosted by GIAC's ISP, is permitted to get zone data from the GIAC external primary DNS server.
4. All SMTP traffic will enter and leave the GIAC network via the email gateways on the service network.
5. All inbound web traffic must be addressed to the service network. All actual content and other business data must reside on servers and storage on the internal network.
6. Syslog traffic from the DMZ and service networks may pass through the firewall to the internal syslog server.
7. Snmp traps generated from the DMZ and service network devices may pass through the firewall to the internal *SNMP* server.
8. No netbios, Windows 2000 file sharing, or NFS connections will be allowed to pass through the firewall.
9. X11 connections from the GIAC network to the Internet will be denied.
10. No inbound ICMP traffic will be allowed to enter the GIAC network. Exceptions can be made to allow the administrative staff to perform network testing and diagnostics.
11. All outbound connections from the internal network, not explicitly denied via the previous statements, will be allowed.
12. All other traffic not explicitly allowed via the previous statements will be dropped.

Implement the Policy

Set Policy Properties

Firewall-1 has policy properties settings that can affect the behavior of the policy. Therefore it is important to decide which settings to use and set them prior to creating the firewall policy. Figure 4 shows the Security Policy tab of the Policy Properties screen. The important settings for GIAC's implementation are:

Apply Gateway Rules to Interface Direction: Set to inbound. The default is to apply rules on traffic both inbound to and outbound from the firewall. However, inspecting traffic passing into the firewall should be adequate for our purposes and result in slightly better firewall performance.

Implied Rules: The firewall policy will use explicit rules to handle Firewall-1 control connections, DNS, and ICMP. Therefore all these checkboxes should be left unchecked. The firewall will not run RIP, so that checkbox should be left unchecked too. However, since we are applying our policy rules on inbound connections only, we need to check the "Accept Outgoing Packets Originating From Gateway (Last) box.

> **Tips, Hints, Gotchas:** If you want to use Firewall-1's ICMP stateful inspection feature, you must check the ICMP box. I've had mixed results in using this feature and therefore prefer to filter ICMP in a "non-stateful" manner.

Log Implied Rules: Check this item so any matches on implied rules will be logged.

Install Security Policy only if it can be successfully installed on ALL selected targets: There is only one firewall in this configuration, so this can be left unchecked.

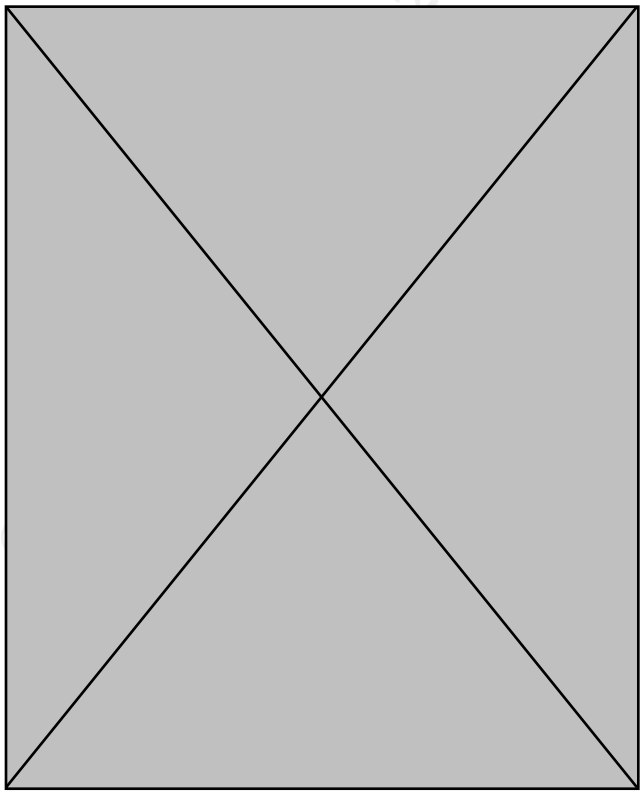

Figure 4