

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Table of Contents 1
Edith_Twigg_GCFW.doc 2

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC Level Two:

Firewalls, Perimeter Protection,

And Virtual Private Networks

Practical Assignment for Capitol SANS
December 10 – 15, 2000

© SANS Institute 2000 - 2002, Author retains full rights.

Submitted By:

Edith V. Twigg

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

OBJECTIVE

The objective of this document is to layout a four-part Information Assurance strategy designed to address the security requirements of GIAC Enterprises. As a new Internet startup company that expects to earn $200 million per year in online sales of fortune cookie sayings, implementing the following recommendations of this document will benefit not only GIAC Enterprises, but help to make the Internet a safer place to conduct E-Commerce for everyone.

PART I

SECURITY ARCHITECTURE

In order to conduct E-Commerce on the Internet as a Visa E-Merchant, GIAC Enterprises must conform to the principles of the Visa Cardholder Information Security Program, "Top Ten" requirements. Visa will begin verifying compliance in May 2001. Further information can be obtained from: http://www.visabrc.com/doc.phtml?2,64,932,932a_cisp.html.

GIAC Enterprises will adhere to the Visa "Top Ten" requirements, while still providing the following access as securely as possible through the use of filtering routers, firewalls, Virtual Private Networks (VPNs) to partners, secure remote access, and internal firewalls.

- **Customers** - companies that purchase bulk online fortunes
- **Suppliers -** authors of fortune cookie sayings that connect to supply fortunes
- **Partners -** international partners that translate and resell fortunes

© SANS Institute 2000 - 2002, Author retains full rights.

PART II

SECURITY POLICY

The security policy for GIAC Enterprises will be based on the aforementioned Security Architecture. A Basic Information Assurance Security Policy will be defined for internal GIAC Enterprises employees, Customers, Suppliers, and Partners. The security policy will also include, but not be limited to defining the policies of the following four components in the Security Architecture:

- Border Router
- Primary Firewall
- Internal Firewall
- VPN – Secure Remote Access

PART III

SECURITY ARCHITECTURE AUDITING

Continual Security Architecture Auditing will be conducted as it relates to Parts I and II. As the risks of doing business over the Internet is ever changing, so must be GIAC Enterprises ability to adapt and adjust to those changes and risks. Auditing will be conducted, yet will not be limited to the following four components in the Security Architecture:

- Border Router
- Primary Firewall
- Internal Firewall
- VPN – Secure Remote Access

© SANS Institute 2000 - 2002, Author retains full rights.

PART IV

DESIGN UNDER FIRE – CONSIDER THE THREATS

In an attempt to stay one step ahead of the Internet attack threat, DESIGN UNDER FIRE is intended to be an exercise in analysis, as there is always room for improvement in any Security Architecture. A previously posted GCFW practical assignment will be subjected to analysis and subsequent attack to identify possible vulnerabilities in its design.

© SANS Institute 2000 - 2002, Author retains full rights.

PART I

SECURITY ARCHITECTURE

GIAC Enterprises is a new Internet startup company that expects to earn $200 million per year in online sales of fortune cookie sayings. GIAC Enterprises has recently completed a merger/acquisition. As GIAC Enterprises embarks onto the Internet as a Visa E-Merchant business their Security Architecture is critical. For GIAC Enterprises to do business as a Visa E-Merchant, they must meet specific requirements set forth by Visa. These are referred to as the Visa Cardholder Information Security Program "Top Ten" logical requirements for protecting Visa cardholder information. The Top Ten requirements and how GIAC Enterprises plans to meet them are as follows.

1) Install and maintain a working network firewall to protect data accessible via the Internet.
   a) Two load balanced firewalls will be implemented, sandwiched between two Alteon 184 Web Switches. Firewalls are application proxy firewalls. Vendor - Network Associates, Inc. Gauntlet Firewall version 5.5 running on Sun Solaris UNIX version 2.6.
   b) The firewalls will be implemented in such a way as to prevent packets from entering the internal networks from the untrusted Internet. Strictly controlled traffic from the Service and VPN Networks to the Internal Networks is allowed.
   c) The firewall software will be the only application running on the systems.
   d) The firewalls will contain the minimum hardware and software required to perform their function.
   e) All firewall remote administrative access will be encrypted utilizing SSH through the VPN concentrator.
   f) Personal Firewalls will be used by all VPN remote users.
   g) All trusts between trusted and untrusted networks will be explicitly defined.
2) Keep security patches up-to-date.
   a) All systems, firewall, DNS, SMTP, Syslog server, Web Content servers, etc., must have the latest vendor-supplied operating system and application security patches installed in a timely manner.
   b) A change-control procedure for all software modifications will be followed.

© SANS Institute 2000 - 2002, Author retains full rights.

c) Several different avenues of notification will be subscribed. Such as, CERT, SANS Security Digests, SecurityFocuses BugTraq, as well as specific vendor support mailing lists.

3) Encrypt stored data.
   a) Triple-DES encryption will be utilized on stored data.
   b) The cryptographic process must be isolated to ensure that no protected data will be disclosed.
   c) Keys will be the only approved devices to process encrypted material.
   d) Encryption keys will not be stored in a public place. Software or hardware systems may be used depending on the circumstances.
   e) Ensure all cryptographic systems conform to applicable international and national standards and all legal and regulatory controls.
4) Encrypt the transmission of cardholder information across open networks.
   a) Secure Sockets Layer (SSL) will be utilized when transmitting data that contains cardholder information across networks.
   b) E-mail that contains cardholder information will be encrypted using PGP.
   c) All communications between remote offices, business partners, road warriors, and home workers will be encrypted via hardware VPN solution – Cisco 3030 VPN Concentrator.
5) Use and regularly update anti-virus software.
   a) Enterprise wide dissemination of anti-virus software and update signature files will be accomplished through login scripts. This applies to local and remote users.
   b) Anti-virus software will be installed and maintained through Enterprise dissemination on all servers in the GIAC network.
   c) Subscribing to the selected anti-virus software vendors' alert mailing list is advised.
6) Restrict access to data by business "need to know".
   a) A formal process for approving all external network connections will be instituted.
   b) Firewall administration will be strictly limited to authorized IT Security Team only.
   c) Cardholder data will be crosscut shredded once it is no longer needed.
   d) Firewalls between internal corporate network departments will be deployed at a future date to compartmentalize access to data within the Private Corporate Network.
   e) Access to networks, servers, applications and data will be based upon the user's profile and his/her role(s) within the organization.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

7) Assign a unique ID to each person with computer access to data.
   a) Uniquely identify all users prior to allowing access to any data or system resources by way of user name and password, digital certificates, or external token devices.
   b) Ensure that a mechanism for logging is available and properly functioning.
8) Don't use vendor-supplied defaults for system passwords and other security parameters, as these passwords are commonly known to a wide range of people.
   a) Password crack programs will be run on a regular basis to ensure strong passwords are being created. Programs such as:
      John the Ripper - http://www.openwall.com/john/
      Crack - http://www.users.dircon.co.uk/~crypto/
      L0phtCrack - http://www.l0pht.com.
9) Track all user access to data by unique ID.
   a) The audit trail records of activity are a direct result of number 7 above functioning properly and will be critical to any data-related investigation.
   b) Retain audit trail history files for a period consistent with effective use and legal regulations. Three years of file retention is not unreasonable and strongly recommended.
   c) All audit trail history files will be stored in an encrypted format.
10) Regularly test security systems and processes.
   a) Run integrity checks daily on all servers utilizing Tripwire from http://www.tripwiresecurity.com
   b) Conduct daily port scans of all servers on the Service Network utilizing ISS from http://www.iss.net/. Bi-weekly port scans on the Private Production Network.
   c) Employ strategic placement of Intrusion Detection Systems (IDS) from http://www.iss.net/ and consistently monitor the logs for suspicious activity.
   d) Retain the services of an independent security-auditing firm to test security architecture each month.
   e) Ensure that a mechanism for alerting IT Security personnel if a compromise is suspected.

Basic Network Design

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GIAC Enterprises Security Architecture begins with a basic network infrastructure design as indicated in **Figure 1**. The Main Corporate Site is identified as five distinct parts. These are further described in the **Physical Network Architecture** section.

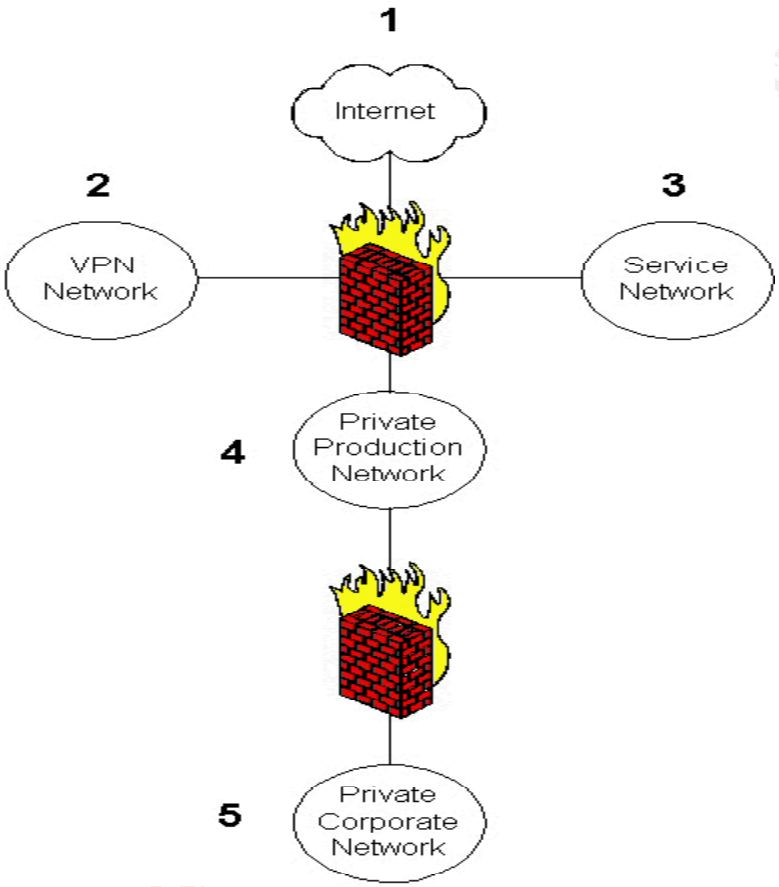


Figure 1

1. **The Untrusted Network (The Internet)**
2. **The Virtual Private Network (VPN)**
3. **The Service Network**
4. **The Private Production Network**
5. **The Private Corporate Network**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detailed Network Design

A more detailed Network Security Architecture design is shown in **Figure 2.** This design is further described in the following section entitled **Physical Network Architecture**.

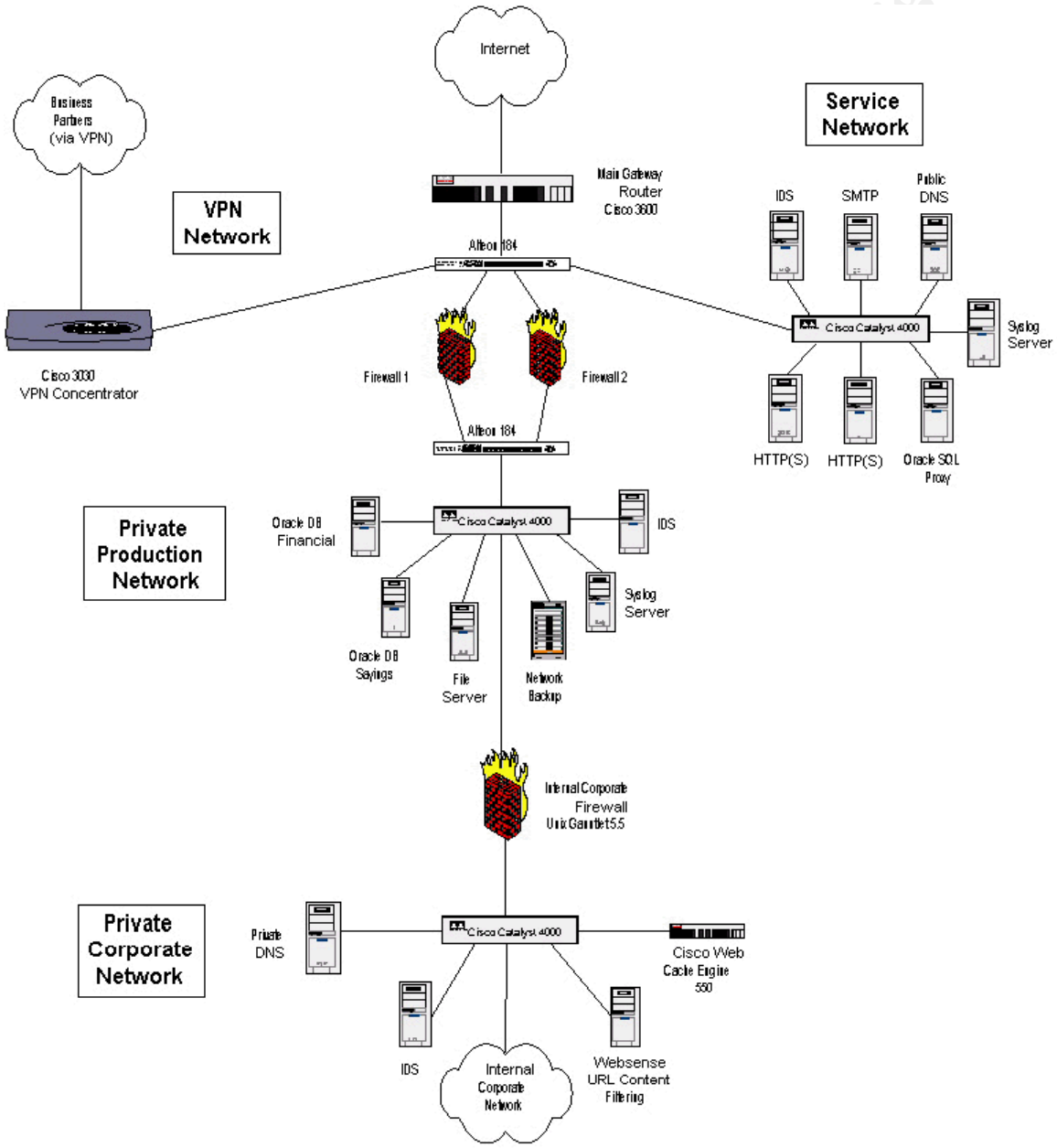


Figure 2

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Physical Network Architecture

1) **The Untrusted Network (The Internet)** – Consists of a T-3 to the public Internet. Connection from the public Internet is through the Main Gateway Router (GW1)– Cisco 3600 series to an Alteon 184 Web Switch. Traffic is redirected to the Service Network through the Alteon switch where filters are applied, thus protecting the Service Network. The Alteon switch basically acts as packet filtering firewall to the Service Network. The servers residing out on the Service a Network will be O/S and application hardened. HTTP and HTTPS services are load balanced through the Alteon switch to provide increased service reliability, server efficiency, and application scalability. Services provided to the Untrusted Network (Internet), Customers and everyone else – DNS, SMTP, and HTTP/HTTPS, and Oracle SQL Reverse Proxying.

2) **The Virtual Private Network (VPN)** – Consists of a Cisco 3030 VPN Concentrator coming from the public Internet and connected directly to the Alteon 184 Web Switch. The Alteon 184 directs the VPN traffic through the load balanced Gauntlet 5.5 Firewalls. This will provide secure VPN connectivity with business partners, road warriors, and home workers and System Administrators who connect through their ISP. Remote users connecting to the VPN Concentrator are required to be running the Enterprise Anti-Virus software and the Enterprise BlackIce Personal Firewall software. Connection will not be allowed without these prerequisites. Once connected the following services are provided to VPN customers:
   a) To the Service Network:
      i) Public DNS services.
      ii) SMTP services.
      iii) An Oracle SQL Reverse Proxy serving up pages from the Oracle Database servers from within the Private Production Network.
      iv) Corporate web servers.
      v) Secure Shell (SSH) connectivity for remote administration.
   b) To the Private Production Network:
      i) Oracle DB access to financial, customer, and Fortune Cookie Sayings databases.
      ii) File sharing capabilities.
      iii) Other critical business data.
      iv) Secure Shell (SSH) connectivity for remote administration.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

c) To the Private Corporate Network:
   i) Secure Shell (SSH) connectivity for remote administration.

3) **The Service Network** - The service network is protected from the public Internet by the Alteon 184 Web Switch through the use of filtering rules on the switch. All servers out on the Service Network will be hardened, both operating system and applications. No unnecessary services will be running on any of the Service Network servers. This network will provide the following services:
   a) To/From the public Internet:
      i) Public DNS services.
      ii) SMTP services.
      iii) An Oracle SQL Reverse Proxy serving up pages from the Oracle Database servers from within the Private Production Network..
      iv) Corporate web servers.

4) **The Private Production Network** – The Private Production Network is protected from the Untrusted, VPN, and Service Networks by the load balanced Gauntlet Firewalls. Access to the Private Production Network from the Untrusted Internet is completely blocked. Access allowed to the Private Production Network is outlined below.
   a) To/From the VPN Network for Business Partners, road warriors, and home workers and System Administrators:
      i) Oracle DB access to financial, customer and Fortune Cookie Sayings databases.
      ii) Other critical business data.
      iii) File sharing services.
      iv) Secure Shell (SSH) connectivity for administration.
   b) From the Private Corporate Network:
      i) Oracle DB access to financial, customer and Fortune Cookie Sayings databases.
      ii) Other critical business data.
      iii) File sharing services.
      iv) Secure Shell (SSH) connectivity for administration.
   c) To/From the Service Network:
      i) Oracle SQL data to/from the Oracle SQL Proxy.
      ii) Public DNS resolution.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5) **The Private Corporate Network** – The Private Corporate Network will be further protected by an Internal Corporate Gauntlet 5.5 Firewall. The outside interface of this Firewall will be connected to the Private Production Network Cisco Catalyst 4000 Router and the internal interface will be connected to the Private Corporate Network Cisco Catalyst 4000 Router. This network will have access to the following services on designated network components:
   a) To the Service Network:
      i) Public DNS services, forwarded from the Private DNS on the Private Corporate Network.
      ii) SMTP services.
      iii) Corporate web servers.
      iv) Secure Shell (SSH) connectivity for administration.
   b) To the Private Production Network:
      i) Oracle DB access to financial, customer and Fortune Cookie Sayings databases.
      ii) File sharing capabilities.
      iii) Other critical business data.
      iv) Secure Shell (SSH) connectivity for administration.
   c) Outbound only from the Private Corporate Network:
      i) HTTP and HTTPS services.
      ii) FTP services.

      The Private Corporate Networks' HTTP and HTTPS access will go through the Websense URL Content Filtering device and web content will subsequently be cached on a Cisco Web Cache Engine – Model 550, both described below.
      a. Websense will transparently monitor, report and manage traffic from the internal networks to the Internet. This will provide the following benefits:
         i. Conserve precious network bandwidth resources.
         ii. Reduce legal liability.
         iii. Boost employee productivity.
         iv. Filter objectionable material.
      b. The Cisco Web Cache Engine – Model 550 will provide the following benefits:
         i. Accelerate content delivery.
         ii. Optimize bandwidth usage.
         iii. Employ content access control when used with the

© SANS Institute 2000 - 2002, Author retains full rights.

Websense Enterprise Content Filtering software.

Network Addressing Scheme

Network Address Translation (NAT) will be used with a RFC 1918 compliant address space for the Private Corporate Network. See **Figure 3**.

The use of Real IP's (RIP) and Virtual IP's (VIP) is explained in the **Alteon 184 Web Switch** section of this document.

The Class C Network 192.168.0.0 is subnetted as a Class B with a subnet mask of 255.255.224.0. This provides 8 subnets for department compartmentalization in the following manner:

Departments	Network	Hosts	Broadcast Address
Network Management	192.168.0.0	192.168.0.1 to 192.168.31.254	192.168.31.255
Executive Software/Prod.	192.168.32.0	192.168.32.1 to 192.168.63.254	192.168.63.255
Web Developers	192.168.64.0	192.168.64.1 to 192.168.95.254	192.168.95.255
Database Analysts	192.168.96.0	192.168.96.1 to 192.168.127.254	192.168.127.255
Human Resources	192.168.128.0	192.168.128.1 to 192.168.159.254	192.168.159.255
Accounting	192.168.160.0	192.168.160.1 to 192.168.191.254	192.168.191.255
Sales/Marketing	192.168.192.0	192.168.192.1 to 192.168.223.254	192.168.223.255
Service	192.168.224.0	192.168.224.1 to 192.168.255.254	192.168.255.255

Figure 3

The public IP space used by the GIAC's Corporate Network will be a Class B subnet range as shown in **Figure 4**.

Network Segment	Network	Hosts	Broadcast Address
Private Corporate Network	xxx.210.130.0	xxx.210.130.1 to 147.210.130.254	xxx.210.130.255
Private Production Network	xxx.210.131.0	xxx.210.131.1 to 147.210.131.254	xxx.210.131.255
Service and VPN Network	xxx.210.132.0	xxx.210.132.1 to 147.210.132.254	xxx.210.132.255
Reserved for Future use	xxx.210.133.0	xxx.210.133.1 to 147.210.133.254	xxx.210.133.255

Figure 4

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Following are detailed network diagrams for each of the corporate network segments.

Private Corporate Network	**Figure 5**
Private Production Network	**Figure 6**
Service Network	**Figure 7**
VPN Network	**Figure 8**
Reserved for future growth	

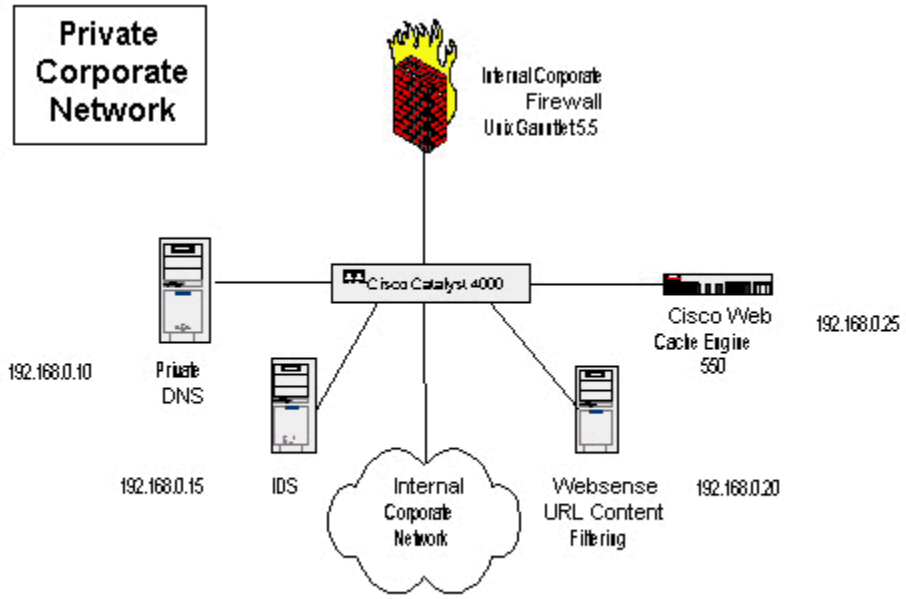


Figure 5

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

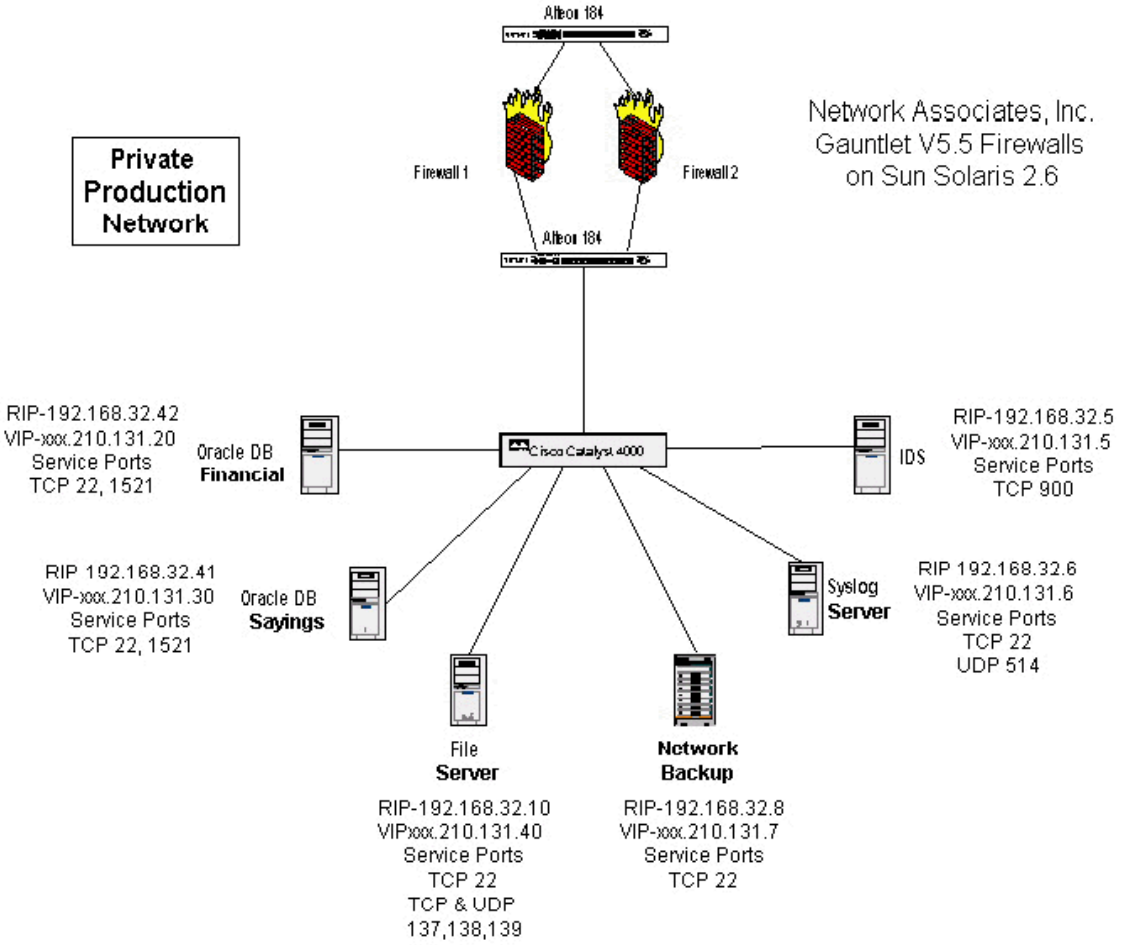


Figure 6

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

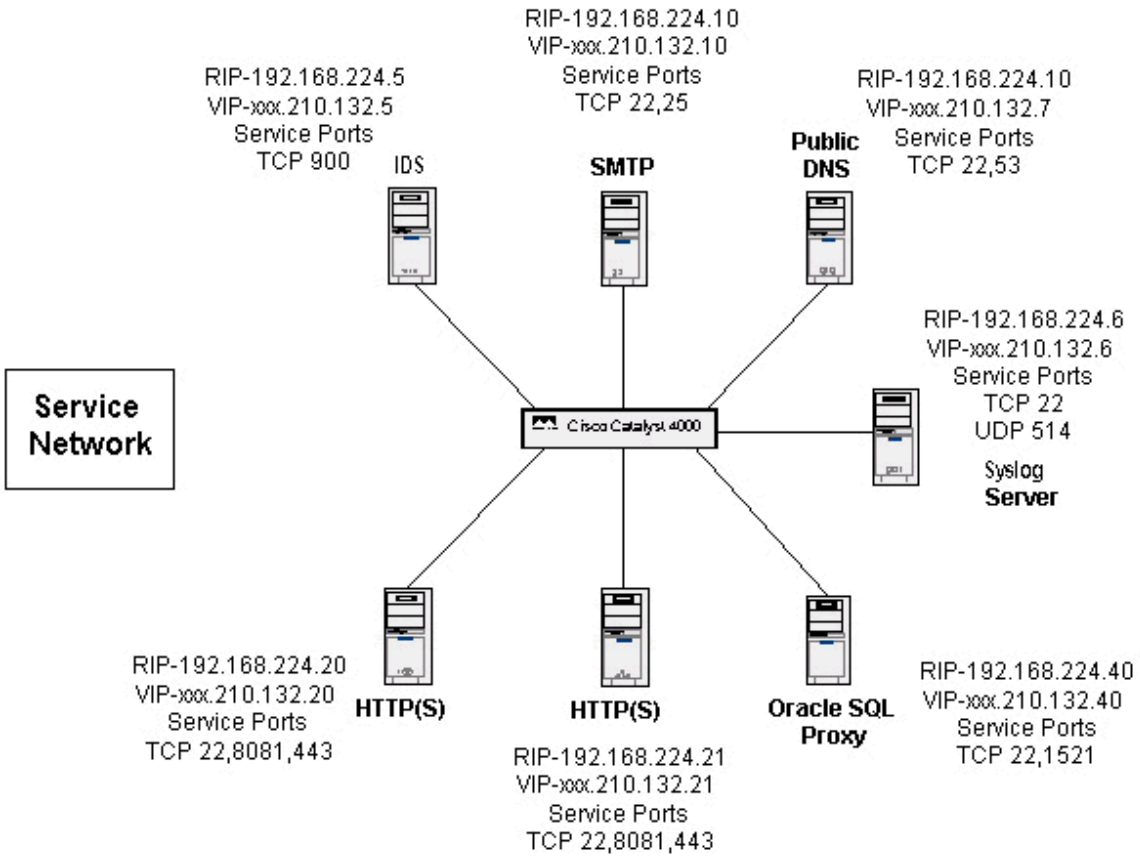


Figure 7

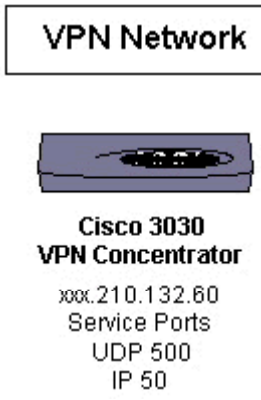


Figure 8

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

PART II

SECURITY POLICY

The GIAC Enterprises Security Policy follows a defense in depth concept as outlined below.

- Physical security for all GIAC Enterprises Security Architecture components, such as routers, switches, VPN Concentrators, Firewalls, and all Enterprise servers, will be maintained and controlled at all times. Installation of unauthorized hardware or modification of authorized hardware will be controlled by the Network Management Department, of which the IT Security Team is a member.
- The Main Gateway Router will provide basic traffic blocking as described in the Main Gateway Router Configuration and Rules.
- The Alteon 184 Web Switches will provide port/service redirection filtering for allowed services to allowed network components. The Alteon switches will also provide server load balancing for HTTP and HTTPS services on the Service Network and Firewall load balancing of the two Main Perimeter Firewalls. Configuration described in the Alteon 184 Web Switch section.
- The load balanced Main Perimeter Firewalls will further protect the Private Production Network through the use of application proxies on the firewalls. Configuration described in the Main Perimeter Load Balanced Firewalls section.
- The Internal Corporate Firewall will further protect the Private Corporate Network through the use of application proxies on the firewalls. Configuration described in the Internal Corporate Firewall section.
- Anti-virus software will be installed and signature files maintained through Enterprise dissemination on all servers in the GIAC network.
- Enterprise wide dissemination of anti-virus software and update signature files will be accomplished through login scripts for all users. This applies to local and remote users.
- Remote users connecting to the VPN Concentrator are required to be running the latest Enterprise Anti-Virus software and the Enterprise BlackIce Personal Firewall software. Connection will not be allowed without meeting these prerequisites. The VPN Concentrator is further

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

described in the Cisco 3030 VPN Concentrator section.

- All GIAC Enterprises and Business Partner employees will comply with the Information Assurance Security Policy as outlined in the Information Assurance Security Policy section.
- Modems are forbidden in user workstations on the Main Corporate Network, as they pose a serious security risk as a back-door into the network.

© SANS Institute 2000 - 2002, Author retains full rights.

Information Assurance Security Policy

Services allowed in and out of the GIAC Enterprises Network are outlined in the Security Architecture. All internal and remote users will adhere to the following Basic Information Assurance Security Policy. This is a living document and will be changed and updated as business needs change.

- The Information Assurance Security Policy must be enforceable to achieve its objectives. Management must be educated about security issues and the need for this policy. Management must be committed to supporting the development, promulgation, and enforcement of this policy.
- All users, both internal and remote VPN, will be trained in security policies and procedures. All users, both internal and remote VPN, will be required to sign an Acceptable Usage Agreement prior to receiving access to GIAC Enterprises resources.
- All users, both internal and remote VPN, will have a unique username and a strong password. All passwords will be changed on a monthly basis and will conform to security policy password standards.
- All users, both internal and remote VPN, will run the Enterprise anti-virus software that is distributed and updated through the users logon script.
- Remote users connecting to the VPN Concentrator are required to be running the latest Enterprise Anti-Virus software and the Enterprise BlackIce Personal Firewall software. Connection will not be allowed without these prerequisites.
- GIAC Enterprises employees and Business partners will conduct company business through a VPN connection to the GIAC IT resources.
- Public Internet access to the GIAC Enterprises Network will be limited to the Service Network only.
- Access to data in the GIAC Network from authorized users is restricted on a per user basis, thus complying with the Visa 'need to know' requirement.
- All data leaving the GIAC Network over the public Internet will be encrypted.
- Email traffic will be encrypted using PGP.
- Internal GIAC users are prohibited from using any category of software

© SANS Institute 2000 - 2002, Author retains full rights.

that has not been approved by IT Security. Such as, but not limited to the following:

- Messaging software – AOL – IM, MSN Chat, Yahoo Chat, any IRC software.
- Network Monitoring and Maintenance Software – SNMP, NTP, ICMP.
- File Sharing Software – Napster, WebNFS, NFS.

- For GIAC Enterprises to avoid the risks of possible litigation and liability, it is essential that users see a statement when they login informing them that they will use the workstation in accordance with the acceptable use policy and that their use will be monitored to ensure compliance.
- Failure on the part of any GIAC employee or Business Partner employee to comply with the aforementioned policy will find their access to GIAC IT resources suspended pending review by GIAC Enterprises Management.

© SANS Institute 2000 - 2002, Author retains full rights.

Main Gateway Router Configuration and Rules

Appropriate secure ACL's will be maintained on the Cisco 3600 Main Gateway Router (GW1). GW1 will provide basic blocking of traffic such as known malicious addresses and/or networks. Anti-spoofing rules will be implemented as well. Logging will be maintained and reviewed on a regular basis.

To control inbound and outbound traffic through the gateway router ingress and egress filtering will be defined as in the following ACL:

```
no ip directed-broadcast                                    #smurf attack prevention
no ip source-route                                          #source route attack prevention
no ip proxy-arp                                             #Deny Proxy-Arp
no ip unreachables                                          #Deny ICMP unreachable on all if's.
no service tcp-small-servers                                #Disable echo, discard, chargen and
no service udp-small-servers                                #  daytime services
no ip bootp                                                 #Disable bootp
no ip http                                                  #Disable http
no service finger                                           #Disable finger service
service password encryption                                 #Encrypt password
ip access-group 110 in                                      #apply access list 110 to incoming traffic
ip access-group 120 out                                     #apply access list 120 to outgoing traffic

access-list 110 deny ip 10.0.0.0 0.255.255.255 any log      #RFC-1918 addresses, log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log     #RFC-1918 addresses, log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log     #RFC-1918 addresses, log
access-list 110 deny ip 127.0.0.0 0.255.255.255 any log     #Deny Localhost, log
access-list 110 deny ip 255.0.0.0 0.255.255.255 any log     #Deny Broadcast, log
access-list 110 deny ip 224.0.0.0 7.255.255.255 any log     #Deny Multicast, log
access-list 110 deny ip 0.0.0.0 any log                     #Deny no ip address, log
access-list 110 deny ip xxx.210.130.0 0.0.0.255 any log     #spoof prevention, log
access-list 110 deny ip xxx.210.131.0 0.0.0.255 any log     #spoof prevention, log
access-list 110 deny ip xxx.210.132.0 0.0.0.255 any log     #spoof prevention, log
access-list 110 deny ip xxx.210.133.0 0.0.0.255 any log     #spoof prevention, log
access-list 110 deny ip any any log                         #Deny everything else, log
access-list 110 permit tcp any host xxx.210.132.10 eq smtp  #Allow smtp traffic to mail servers only
access-list 110 permit tcp any host xxx.210.132.7 eq domain log     #DNS traffic to DNS server only
access-list 110 permit udp any host xxx.210.132.7 eq domain         #DNS traffic to DNS server only

access-list 120 deny icmp any any log                       #Deny outbound ICMP
access-list 120 permit ip xxx.210.130.0 0.0.0.255 any               #Allow only traffic from local net
out
access-list 120 permit ip xxx.210.131.0 0.0.0.255 any               #Allow only traffic from local net
out access-list 120 permit ip xxx.210.132.0 0.0.0.255 any           #Allow only traffic from local net
out access-list 120 permit ip xxx.210.133.0 0.0.0.255 any           #Allow only traffic from local net
out access-list 120 deny ip any any log                             #Deny everything else, log

logging xxx.210.133.6                                       #Log everything to Syslog
```

© SANS Institute 2000 - 2002, Author retains full rights.

Cisco 3030 VPN Concentrator

The Cisco VPN Concentrator is a remote-access Virtual Private Network (VPN) hardware device with client software that provides hardware encryption and authentication techniques, such as tunneling support for IPsec, PPTP and L2TP/IPsec connections. GIAC Enterprises will use the IPsec suite of services. The method of encryption/authentication is IPsec Encapsulating Security Payload (ESP) using DES/3DES (56/168-bit). The Concentrator also has packet-filtering capabilities, which will provide security for the GIAC Enterprises Corporate Network.

The Cisco VPN 3000 client is IPsec-compliant and will be pre-configured for mass deployments, thus requiring very little user intervention. Centrally configurable policy management, such as split tunneling policy, will be pushed down from VPN 3030 Concentrator, as the VPN access policies are created and stored in the Concentrator and pushed to the client when a connection is established. A split-tunneling configuration makes it so that the remote client can only transmit data to the VPN or their ISP but not both at the same time.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Alteon 184 Web Switch

The Alteon 184 Web Switch in the GIAC Enterprises Security Architecture serves several purposes. As it is the first route into the Main Corporate Network from the Gateway Router, and the connectivity point from the VPN Network, it will provide an additional level of filtering for incoming and outgoing traffic. Possibly even alleviating some of the burden of filtering for the Gateway Router and Firewalls. The Alteon Switch will also serve to load balance HTTP and HTTPS services on the Service Network, as well as load balance the two Gauntlet Firewalls that are sandwiched between them. The implementation of these switches will eliminate a single-point of failure at the Firewalls, as well as the Corporate Web Servers on the Service Network. The load balancing will help to improve performance, scalability, and efficiency of both the Web Servers and Firewalls.

Using IP Routing the Alteon switches isolates the private server network or Real IP's (RIP) from the routable public Virtual IP's (VIP). The world talks to the VIP's and the servers talk to the switch. This will ensure that no one can directly address the servers and visa-versa, because of the non-routable IP address.

FROM Untrusted Internet TO Service Network

Traffic from the Untrusted Internet is redirected to the Service Network through the first Alteon 184 switch where filters are applied, thus protecting the Service Network. The Alteon switch basically acts as packet filtering firewall to the Service Network. HTTP and HTTPS services are load balanced through the Alteon switch to provide increased service reliability, server efficiency, and application scalability, so the two HTTP(S) servers are identified with a virtual IP address on the switch. The two HTTP servers are running on port 8081.

© SANS Institute 2000 - 2002 Author retains full rights.

Alteon 184 Web Switch redirection to the Service Network is accomplished through the following steps:

1) Configure the interfaces on the Alteon switch.
2) Configure the real IP's (RIP) of the servers behind the switch.
3) Configure the virtual IP's (VIP) of the servers behind the switch.
4) Put the real IP's into groups.
   a) Group 1 - HTTP and HTTPS
   b) Group 2 - SMTP
   c) Group 3 - DNS
   d) Group 4 - Oracle SQL
5) Create filters to redirect the desired traffic to the Service Network.
   a) /cfg/slb/filter #/source IP any/destination VIP/protocol tcp/source port any/destination port 80/action redirect/redirect port 8081/group 1
   b) /cfg/slb/filter #/source IP any/destination VIP/protocol tcp/source port any/destination port 443/action redirect/redirect port 443/group 1
   c) /cfg/slb/filter #/source IP any/destination IP xxx.210.132.10/protocol tcp/source port any/destination port 25/action redirect/redirect port 25/group 2
   d) /cfg/slb/filter #/source IP any/destination IP xxx.210.132.7/protocol tcp/source port any/destination port 53/action redirect/redirect port 53/group 3
   e) /cfg/slb/filter #/source IP any/destination IP xxx.210.132.40/protocol tcp/source port any/destination port 1521/action redirect/redirect port 1521/group 4
6) Apply the above filters to the appropriate ports on the switch.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FROM VPN Network TO Service Network

Traffic from the VPN Network through the Alteon184 switch can access the Service or Private Production Networks depending upon destination IP address.

To get to the services provided out on the Service Network from the VPN Network, the following filters will be implemented. In addition to the rules above, access from the VPN Network to the Service Network is required for Secure Shell (SSH) connectivity for remote administration.

1) Configure the interfaces on the Alteon switch.
2) Configure the real IP's of the servers behind the switch.
3) Configure the virtual IP's (VIP) of the servers behind the switch.
4) Put the real IP's into groups.
   a) Group 1 - HTTP and HTTPS
   b) Group 2 - SMTP
   c) Group 3 - DNS
   a) Group 4 - Oracle SQL
   b) Group 5 - SSH
5) Create filters to redirect the desired traffic to the Service Network.
   a) /cfg/slb/filter #/source IP any/destination VIP/protocol tcp/source port any/destination port 80/action redirect/redirect port 8081/group 1
   b) /cfg/slb/filter #/source IP any/destination VIP/protocol tcp/source port any/destination port 443/action redirect/redirect port 443/group 1
   c) /cfg/slb/filter #/source IP any/destination IP xxx.210.132.10/protocol tcp/source port any/destination port 25/action redirect/redirect port 25/group 2
   d) /cfg/slb/filter #/source IP any/destination IP xxx.210.132.7/protocol tcp/source port any/destination port 53/action redirect/redirect port 53/group 3
   e) /cfg/slb/filter #/source IP any/destination IP xxx.210.132.40/protocol tcp/source port any/destination port 1521/action redirect/redirect port 1521/group 4
   f) /cfg/slb/filter #/source IP xxx.210.132.60/destination IP any/protocol tcp/source port any/destination port 22/action redirect/redirect port 22/group 5
6) Apply the above filters to the appropriate ports on the switch.

© SANS Institute 2000 - 2002, Author retains full rights.

FROM VPN Network TO Private Production Network

To get to the services provided on the Private Production Network from the VPN Network, the following filters will be implemented. This traffic will be intercepted, interrogated, and authenticated by the load balanced Gauntlet Firewalls sandwiched in between the two Alteon 184 Switches.

1) Configure the interfaces on the Alteon switch.
2) Configure the real IP's of the servers behind the switch.
3) Configure the virtual IP's (VIP) of the servers behind the switch.
4) Put the real IP's into groups.
   a) Group 1 – Oracle SQL
   b) Group 2 – File Sharing
   c) Group 3 – SSH
5) Create filters to redirect the desired traffic to the Private Production Network.
   a) /cfg/slb/filter #/source IP any/destination IP xxx.210.131.20/protocol tcp/source port any/destination port 1521/action redirect/redirect port 1521/group 1
   b) /cfg/slb/filter #/source IP any/destination IP xxx.210.131.30/protocol tcp/source port any/destination port 1521/action redirect/redirect port 1521/group 1
   c) /cfg/slb/filter #/source IP any/destination IP xxx.210.131.40/protocol tcp/source port any/destination port 137,138,139/action redirect/redirect port 137,138,139/group 2
   d) /cfg/slb/filter #/source IP any/destination IP any/protocol tcp/source port any/destination port 22/action redirect/redirect port 22/group 3
6) Apply the above filters to the appropriate ports on the switch.

© SANS Institute 2000 - 2002 Author retains full rights.

Main Perimeter Load Balanced Firewalls

The Main Perimeter load balanced Firewalls are both Network Associates, Inc. Gauntlet version 5.5 Firewalls running on Sun Solaris 2.6 platforms.
The Solaris platform will be hardened following the SANS' Solaris Security Step-By-Step Guide, available from:
http://www.sans.org/newlook/resources/hard_solaris.htm

The YASSP: Hardening Script for Solaris is a script that can be customized for the specific type of server being hardened: http://www.yassp.org
All operating system and application patches will be kept up to date, within 3 days of availability.

The log files for both Firewalls will be copied to the Syslog Server on the Private Production Network for manipulation by the WebTrends Firewall Software Suite in a real-time manner. Security alerts will serve to notify the IT Security Team of any potential compromises. Comprehensive management reporting of services will be accomplished through the use of this software as well.

Access to the Firewalls for administration will be limited to the consoles and SSH connections from the VPN Concentrator.

DNS services will not be running on the Gauntlet Firewalls. DNS will be set to NONE. To facilitate DNS traffic to pass from the Internal Corporate Network Private DNS first through the Internal Corporate Firewall and then through the load balanced Firewalls out to the Public DNS server on the Service Network, packet filter rules must be established on all three Firewalls.

1) Load Balanced Firewalls – To allow DNS resolution from the Private DNS on the Private Corporate Network out to the Public DNS on the Service Network.

Forward Packet Filter Rules:

Action	Interface	Protocol	Source Port Range	Source IP	Destination Port Range	Destination Address
Permit Forward	Internal	TCP	*	192.168.0.10	53-53	xxx.210.132.7
Permit Forward	External	TCP	53-53	xxx.210.132.7	*	192.168.0.10

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Local Packet Filter Rules:

Action	Interface	Protocol	Source Port Range	Source IP	Destination Port Range	Destination Address
Permit Forward	External	TCP	*	xxx.210.132.7	53-53	External VIP
Deny	External	*	*	0.0.0.0	53-53	External VIP

The basic underlying rule is to deny everything and then explicitly allow only specific services to and from specific sources.

Traffic that has been redirected by the Alteon 184 switch from the VPN Network destined for the Private Production Network will traverse two load balanced Gauntlet 5.5 Firewalls. The two firewalls rules and proxies will be configured the same.

Three Network Groups will be created in the Gauntlet Configuration. VPN, Trusted (the Private Production and Internal Corporate), and Service.

The VPN Network Group will be allowed the following services:

1) Oracle SQL Proxy
   a) Identify the port on which the Oracle SQL proxy should listen for traffic. In this case, port 1521.
   b) Identify Oracle Database SID's to the proxy.
2) A plug proxy will be created to pass the SSH traffic on port 22 to the Private Production Network.
3) Plug proxies for ports 137-139 will be created to pass the necessary traffic to accomplish file sharing to the Private Production Network.

The Service Network Group will be allowed the following service:

1) Oracle SQL Proxy
   a) Identify the port on which the Oracle SQL proxy should listen for traffic. In this case, port 1521.
   b) Identify Oracle Database SID's to the proxy.

© SANS Institute 2000 - 2002 Author retains full rights.

The Trusted Network Group will be allowed to pass the following services through the load balanced Firewalls:

1) Oracle SQL Proxy
   a) Identify the port on which the Oracle SQL proxy should listen for traffic. In this case, port 1521.
   b) Identify Oracle Database SID's to the proxy.
2) SMTP Proxy
   a) Identify the SMTP server that is out on the Service Network to the proxy.
   b) Enable Anti-Relaying on the SMTP proxy and on the SMTP server itself. This to prevent outsiders from using the GIAC SMTP server as a relay.
3) HTTP Proxy
   a) Configured so that only HTTP traffic will be allowed outbound from the Cisco Web Cache Engine.
4) SSL Proxy
   a) Configured so that only SSL traffic will be allowed outbound from the Cisco Web Cache Engine.
5) A plug proxy will be created to pass the SSH traffic on port 22.
6) Plug proxies for ports 137-139 will be created to pass the necessary traffic to accomplish file sharing to the Private Production Network.
7) FTP Proxy
   a) Configured for outbound FTP connections from the Trusted Network only.

© SANS Institute 2000 - 2002 Author retains full rights.

Internal Corporate Firewall

The Internal Corporate Firewall is a Network Associates, Inc. Gauntlet version 5.5 Firewall running on the Sun Solaris 2.6 platform. The Solaris platform will be hardened in the same manner as the two load balanced Firewalls. All operating system and application patches will be kept up to date, within 3 days of availability.

The log files for the Internal Corporate Firewall will be copied to the Syslog Server on the Private Production Network for manipulation by the WebTrends Firewall Software Suite in a real-time manner. Security alerts will serve to notify the IT Security Team of any potential compromises. Comprehensive management reporting of services will be accomplished through the use of this software as well.

Access to the Firewall for administration will be limited to the console and SSH connections from the VPN Concentrator through the Main Perimeter Firewalls.

DNS services will not be running on the Gauntlet Firewall. DNS will be set to NONE. To facilitate DNS traffic to pass from the Internal Corporate Network Private DNS first through the Internal Corporate Firewall and then through the load balanced Firewalls out to the Public DNS server on the Service Network for resolution, packet filter rules must be established on all three Firewalls.

Forward Packet Filter Rules:

Action	Interface	Protocol	Source Port Range	Source IP	Destination Port Range	Destination Address
Permit Forward	Internal	TCP	*	192.168.0.10	53-53	xxx.210.132.7
Permit Forward	External	TCP	53-53	xxx.210.132.7	*	192.168.0.10

© SANS Institute 2000 - 2002, Author retains full rights.

Local Packet Filter Rules:

Action	Interface	Protocol	Source Port Range	Source IP	Destination Port Range	Destination Address
Permit Forward	External	TCP	*	xxx.210.132.7	53-53	xxx.210.130.20
Deny	External	*	*	0.0.0.0	53-53	xxx.210.130.20

The basic underlying rule is to deny everything and then explicitly allow only specific services to and from specific sources.

The following Gauntlet proxies will be used to pass traffic between the Private Production and Private Corporate Networks:

1) Oracle SQL Proxy
   a) Identify the port on which the Oracle SQL proxy should listen for traffic. In this case, port 1521.
   b) Identify Oracle Database SID's to the proxy.
2) SMTP Proxy
   a) Identify the SMTP server that is out on the Service Network to the proxy.
   b) Enable Anti-Relaying on the SMTP proxy and on the SMTP server itself. This to prevent outsiders from using the GIAC SMTP server as a relay.
3) HTTP Proxy
   a) Configured so that only HTTP traffic will be allowed outbound from the Cisco Web Cache Engine.
4) SSL Proxy
   a) Configured so that only SSL traffic will be allowed outbound from the Cisco Web Cache Engine.
5) A plug proxy will be created to pass the SSH traffic on port 22.
6) Plug proxies for ports 137-139 will be created to pass the necessary traffic to accomplish file sharing to the Private Production Network.
7) FTP Proxy
   a) Configured for outbound FTP connections from the Trusted Network only.

© SANS Institute 2000 - 2002, Author retains full rights.

PART III

SECURITY ARCHITECTURE AUDITING

Based on the Security Architecture defined in Parts I and II, the Security Architecture Auditing section will provide a comprehensive information systems security audit for GIAC Enterprises. The methodology is broken up into three distinct parts.

1) **The Assessment Plan** – The Assessment Plan will describe the technical approach taken to assess the security perimeter defenses, and when the assessment will take place. Specific risks and considerations will be identified.
2) **Implementation of the Assessment Plan** – Implementing the Assessment plan will serve to validate the perimeter security design is implementing the security policy outlined in Part II – Security Policy. Or it will identify vulnerabilities that will need to be addressed.
3) **Conduct a perimeter analysis** – Based on the aforementioned Assessment Plan, the security perimeter will be subjected to an analysis of the perimeter defenses. Recommendations for improvements or alternate architectures will be described as they are identified.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Assessment Plan

Prior to beginning the Assessment, strategy meetings will be held with the following individuals or groups:

1) IT Manager/CIO – The IT Manager will serve as liaison to GIAC Management. Management must be briefed about the impending Security Assessment, as some of the tests may pose risks to the systems being assessed. It should be stressed to Management that risks imposed by the assessment are minimal compared to the risk of not conducting the assessment at all.
2) Systems Administrators, Network Administrators, and Security Team – These individuals would know their specific areas the best, as a review of the GIAC Enterprises Security Policy will be the baseline for assessment. These individuals should be available during the assessment in case any problems arise with systems that they are responsible for.
3) IT Manager/CIO and the aforementioned Administrators from the Business Partners should be briefed about the impending Security Assessment, as it may affect access to GIAC Enterprises resources.

The following meeting agenda will serve to better design the Assessment Plan.

1) Discuss the current Security Policy in detail. This will help to define any risks or vulnerabilities in the Security Architecture as a result of the Security Policy. Once the Assessment has been completed and the results are being analyzed, a determination will be made as to whether the risks or vulnerabilities can be better mitigated or if they are acceptable to doing business on the Internet.

2) Recommend that backups be done on all servers in the enterprise, prior to the assessment tests. Users workstation data should be backed up as well.

3) Obtain a contact list with phone numbers of all relevant individuals to the assessment and determine the procedure that will be followed if any of the systems are adversely affected during the assessment. Points of contacts would include Systems Administrators, Network Administrators, and the IT Security Team members.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4) Determine the best time for conducting the assessment. Conducting the assessments during non-peak hours is recommended, as this is an E-Commerce business and any downtime as a result of the assessment could be very costly. Management may be more supportive of the Security Assessment if the risks of downtime are minimized.

© SANS Institute 2000 - 2002, Author retains full rights.

Several tools will be utilized in an effort to comprehensively assess the Security Architecture. The tools and their function are described below.

1) Footprinting - During this phase, information about the design and architecture of the network is collected. This phase assesses the target's exposure to hostile reconnaissance by using tools such as FINGER, WHOIS and NSLOOKUP, and DIG for acquiring network and management information from authoritative sources.
    a. DNS is one of the biggest story-tellers about an organization. GIAC Enterprises is running a split DNS configuration, so even if the external DNS server is compromised, an intruder cannot learn the internal network mapping. DIG, for instance can be used to get as much information about the DNS server as possible, such as the specific version of BIND or if a zone transfer were possible, the names and IP addresses of each host on the Public DNS and in the case of GIAC Enterprises, of each host on the Service Network.

2) Network Reconnaissance - This phase compares the target network architecture as designed, with the results of 'mapping' the real world network. NetRecon from Symantec Corp. will be used to identify all machines on the target network, and by subnet. This will be used by the Network Management Department to verify that the systems that are connected to the GIAC network should be connected.

    Traceroute will be used to gather information about the various hops a packet takes from the source to the destination. It could be used to identify intervening routers and firewalls, thus creating a logical map of the network. The GIAC Network should block this type of activity.

3) Network Service/Port Scan - The purpose of this phase is to assess intrusion susceptibility of the network at the machine level using automated scanning tools designed to search for known exploits and configuration-based vulnerabilities. Internet Scanner by Internet Security Systems will be used for all port scans. Port scans will be targeted on all servers, to include firewalls, and workstations on all network segments.
4) Authentication Scan – Password crack programs such as, John the Ripper, Crack, and L0phtCrack will be used to identify weak or even

© SANS Institute 2000 - 2002, Author retains full rights.

worse, non-existent passwords on servers and workstations.

5) War Dialers – War Dialers will be used to find if any phone lines are hooked into modems. Fax machines will be identified in advance of the War Dialer scan as they are allowed on the network.

Implementation of Assessment Plan

Utilizing the tools described above in the Assessment Plan, all servers, including firewalls, were subjected to extensive port scanning and probing. Port scanning was conducted from the DMZ and targeted at the Service, VPN, and Main Corporate Networks. Port scanning was attempted through the load-balanced firewalls through to the Private Networks. Port scans were also conducted internally, in an effort to assess the internal machines security. The results of the port scans in conjunction with firewall logs will determine if the security perimeter is protecting as it was designed in the router and switch ACL's and firewall access rules. While the port scanning was being conducted on the internal network, the scanner was directed to attempt outbound legitimate and illegitimate traffic.

Each discovered vulnerability should be evaluated for risk. Each reported machine should then be logged onto using local administrative privileges so that non-acceptable vulnerabilities can be checked and examined to validate its existence.

Any and all verified and non-acceptable vulnerabilities should then be appropriately fixed, patched, or protected from compromise. Documentation of employed countermeasures and good hardware and software configuration management will help prevent vulnerability recurrence.

© SAN Institute 2000 - 2002 Author retains full rights.

PERIMETER ANALYSIS

Based on the information gathered in the Assessment Plan and Assessment Implementation, an analysis of the security perimeter can be correlated to the Information Assurance Security Policy in PART II of this document.

FOOTPRINTING PHASE – DIG identified the following servers on the Service Network: SMTP, Oracle SQL Proxy, and the Corporate Web Servers. No unnecessary information was divulged regarding the Service Network servers and no internal server information was exposed as a result of this phase.

NETWORK RECONNAISSANCE PHASE – NetRecon was first used to map the VPN and Service Networks outside the load balanced firewalls from GW1 and then from the Private Production and Corporate Networks inside the load balanced firewalls. A decision was made to not allow access through the load balanced firewalls for the network reconnaissance to take place. To do so would have opened up a significant hole in the security perimeter, even if only for a short time. Access for the reconnaissance was allowed through the Internal Corporate Firewall so that the Private Corporate Network could be mapped, however. The output from NetRecon is intended to give the Network Management Department a map of the devices on their network. This will give them the ability to verify what is connected to the network should in fact be connected. As this is a process that the Network Management Department conducts on a regular basis, no unauthorized devices were found. If unauthorized devices were to be found, they would be identified and disconnected immediately and upon further investigation the party or parties responsible for connecting the device or devices would receive a written reminder of the Security Policy and possible reprimand.

Traceroute was attempted from outside GW1. The GW1 ACL blocks this type of activity, so was stopped at the Main Gateway Router.

NETWORK SERVICE/PORT SCAN PHASE – Internet Scanner by Internet Security Systems was used during this phase of the Security Assessment. The Internet Scanner targeted the GIAC Enterprises Network in much the same manner as was the Network Reconnaissance Phase. The following diagram depicts what services the Internet Scanner should find running on specific machines on specific network segments. As stated in the section Implementation of Assessment Plan, any discovered vulnerabilities will

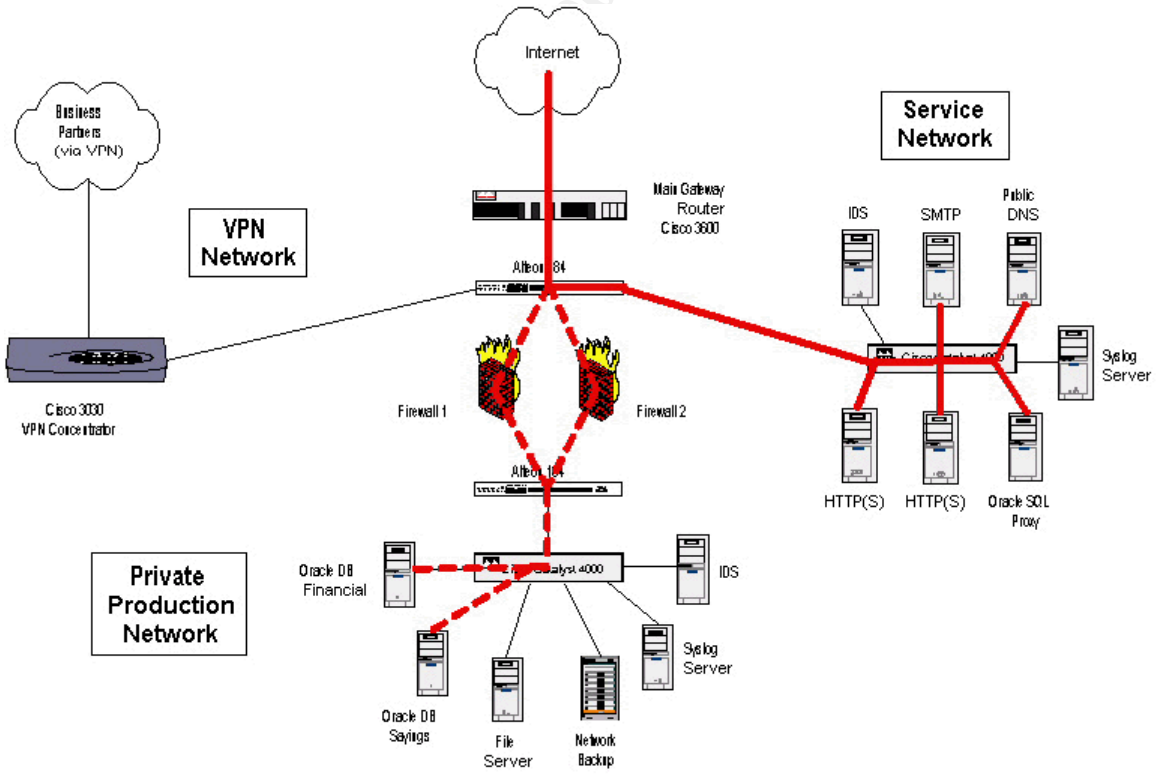
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

be verified, evaluated for its risk, and immediately fixed, patched, or protected from compromise.

Traffic pattern for specific services and ports are depicted in the following descriptions and diagrams.

Inbound services from the public Internet for customers to the Service Network are indicated by a solid red line. Oracle SQL Service from the Service Network to the Private Production Network is indicated by the broken red line.

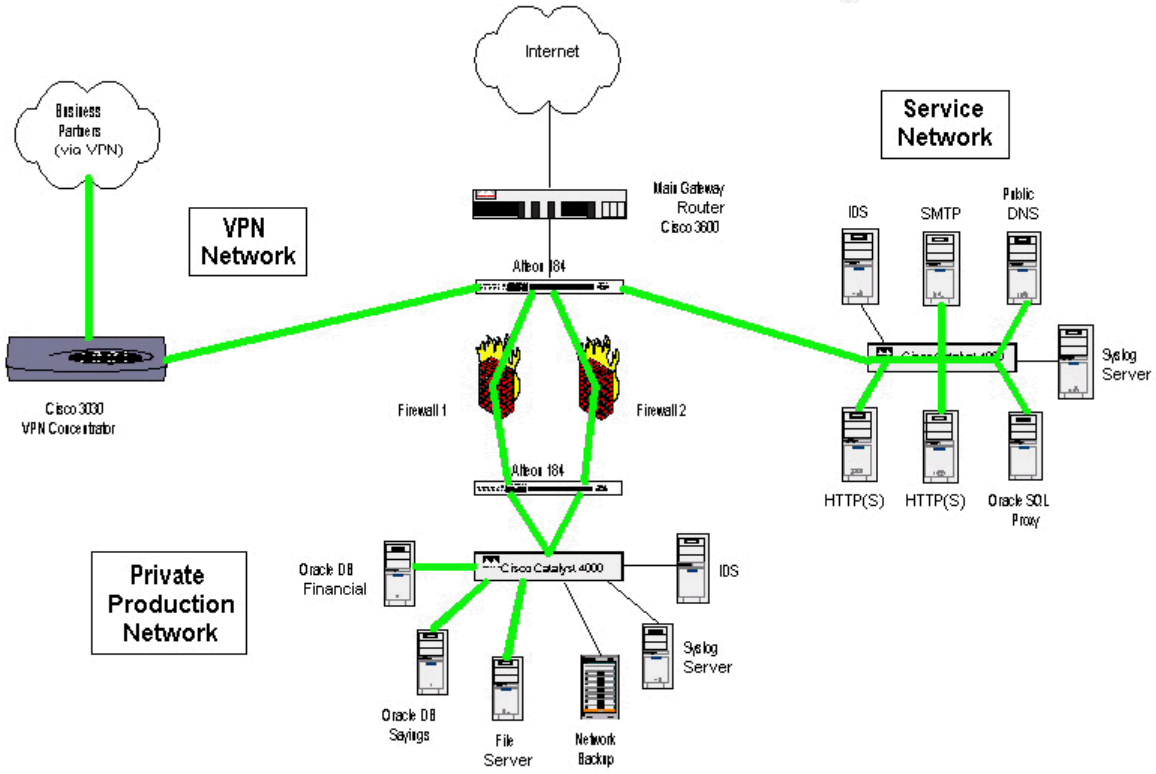
- SMTP 25
- Public DNS 53
- HTTP redirected to port 8081
- HTTPS 443
- Oracle SQL Reverse Proxy 1521



Inbound services from the VPN Network to the Service and Private Production Networks are indicated by a solid green line. These services are accessible to Business Partners, road warriors, and administrators.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

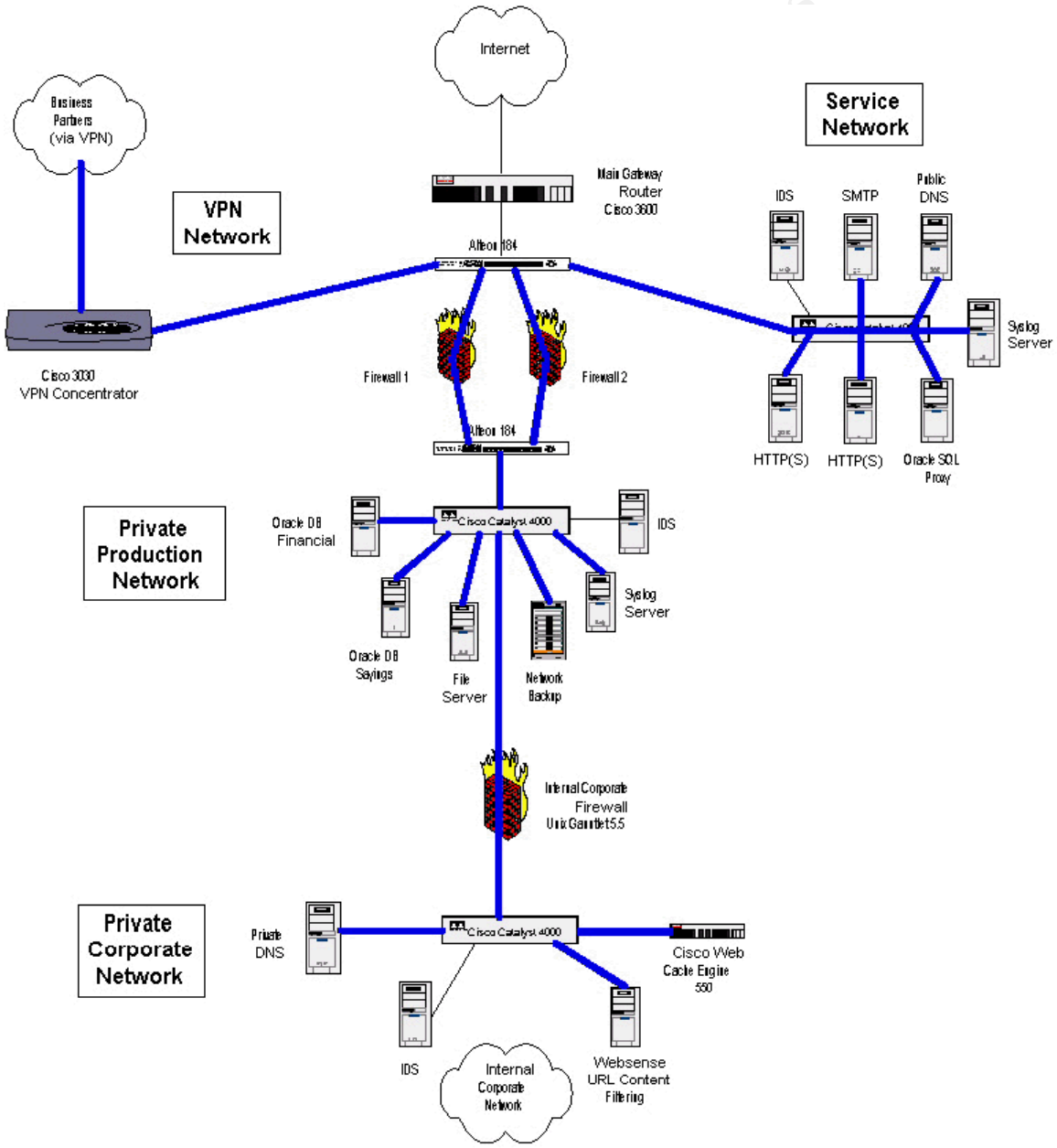
- SMTP 25
- Public DNS 53
- HTTP redirected to port 8081
- HTTPS 443
- Oracle SQL Reverse Proxy 1521
- File Sharing 137-139



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Inbound services from the VPN Network to the Service, Production, and Corporate Networks are indicated by a solid blue line. The SSH service is strictly controlled and only granted to administrators.

- Secure Shell (SSH) 22

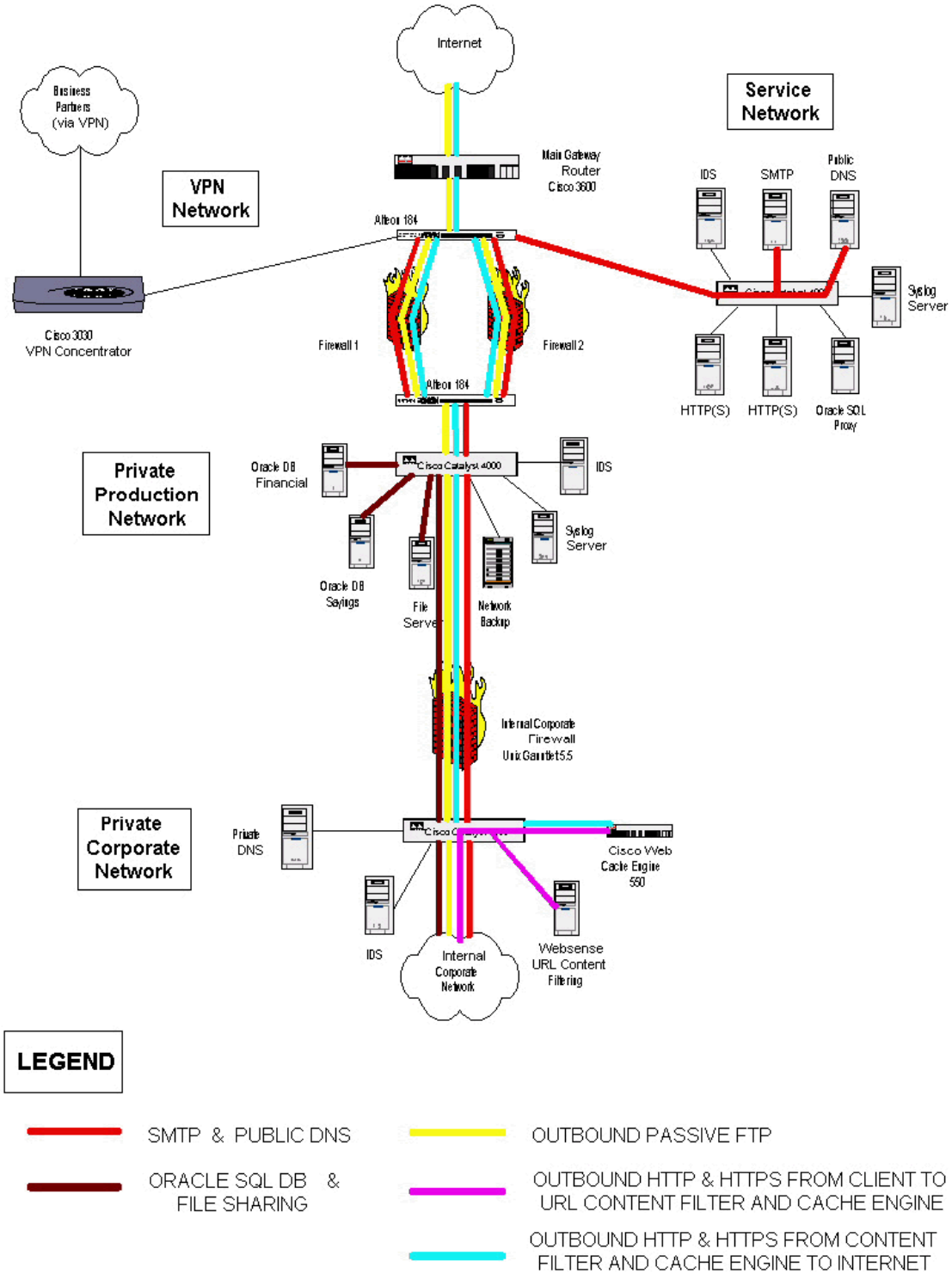


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Outbound services for internal GIAC employees to the Private Production, Service Networks, and the public Internet are depicted in the following diagram.

- SMTP 25
- Public DNS 53
- HTTP 80
- HTTPS 443
- FTP 21
- Oracle SQL 1521
- File Sharing 137-139

© SANS Institute 2000 - 2002, Author retains full rights.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security Assessment Conclusions

It is widely recognized in the Security profession that it is impossible to totally secure a network from any and all vulnerabilities. Even a network that is not connected to the public Internet still has inherent vulnerabilities, such as viruses, malicious conduct by internal users, servers not properly secured and thus vulnerable to compromise by internal users. The list goes on. The intention of this paper is to document best practices and methods for mitigating the risks of doing business on the Internet today as it applies to GIAC Enterprises, and E-Commerce Merchant.

The Security Architecture, along with the Security Policy defined in this document has laid a strong foundation for a secure and highly available network. However, after analyzing the results of the Security Assessment, it was discovered that there are aspects of the Security Architecture that can be strengthened and improved upon. Recommendations for improvement are submitted for consideration.

1) Firewalls between departments on the Private Corporate Network would further solidify one the Visa Top 10 Requirements – Need To Know. By implementing departmental firewalls, cardholder data would be less likely to be compromised. Although this was already mentioned earlier on in this document, it warrants repeating.

2) GIAC Enterprises depends on the Internet for its' very existence and their primary mode of doing business is through their Web Servers. Web Servers are inherently vulnerable, as new vulnerabilities are being discovered everyday. Moving the Web Servers to their own Service Network would be a prudent course of action. Segregate these vulnerable services from less vulnerable services to contain potential intrusions.

3) Recommend eliminating the one most significant single point of failure from the Security Architecture. That would be the T3, the single route to the Internet. If that route were to go down, for whatever reason, or if that single route were to become unavailable as a result of a Distributed Denial of Service (DDoS) attack, GIAC Enterprises would certainly suffer both financial and possibly even consumer confidence or even loss

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

as a result. By purchasing a backup link for services to continue in the unlikely event that the primary were to become disabled should be considered a small price to pay for the benefits of doing business on the Internet. For that matter, the second link may become necessary as business and presence grows. The 'backup' link may actually become a necessity.

© SANS Institute 2000 - 2002, Author retains full rights.

PART IV

DESIGN UNDER FIRE – CONSIDER THE THREATS

In an attempt to stay one step ahead of the Internet attack threat, DESIGN UNDER FIRE is intended to be an exercise in analysis, as there is always room for improvement in any Security Architecture. A previously posted GCFW practical assignment will be subjected to analysis and subsequent attack to identify possible vulnerabilities in its design.

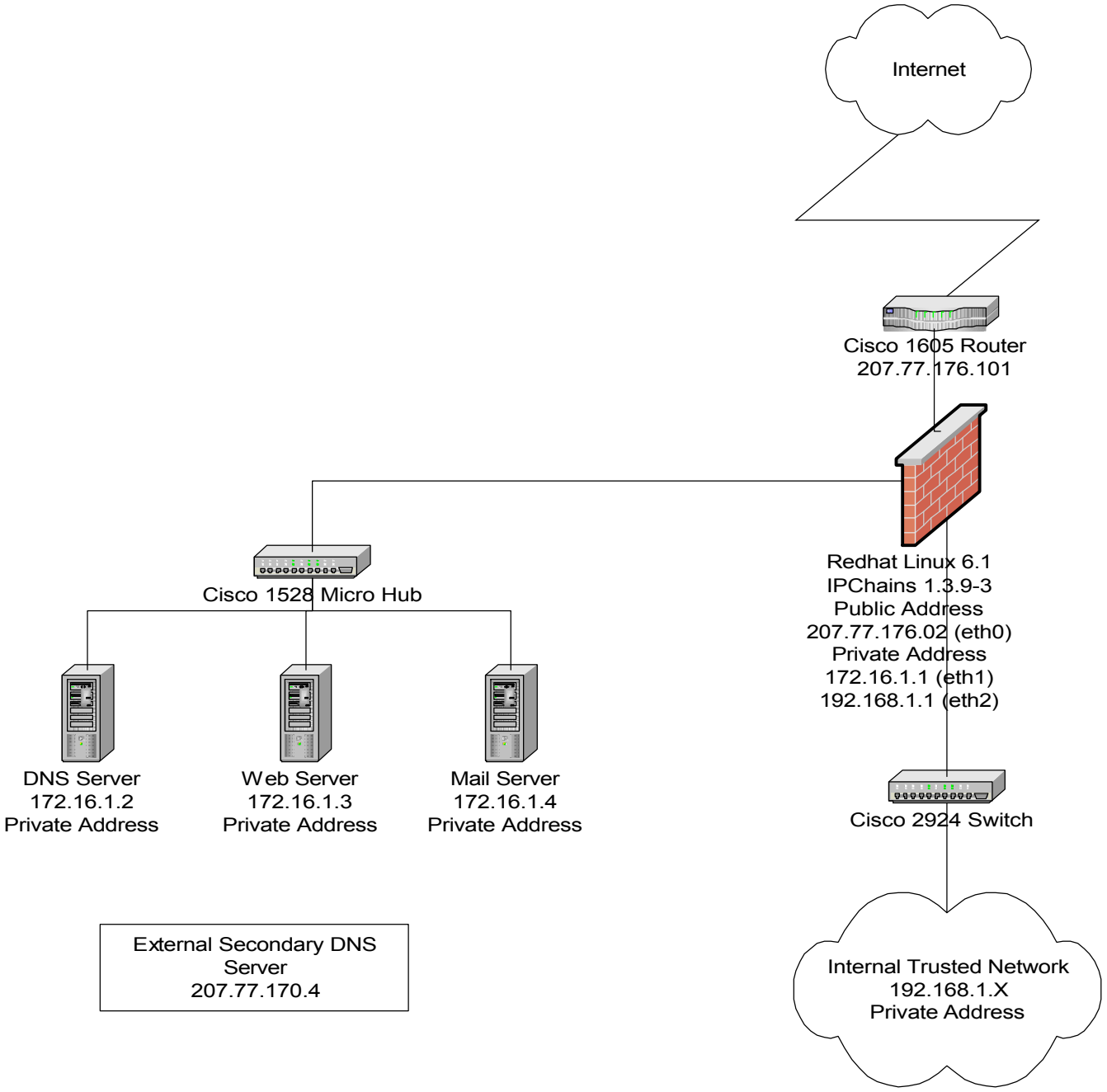
The selected network design for this DESIGN UNDER FIRE exercise is John M. Millican's assignment from SANS DC 2000. Mr. Millican's practical submission can be found on the SANS web site at the following URL: http://www.sans.org/y2k/practical/John_Millican_gcfw.doc

The following three attacks will be performed against Mr. Millican's architecture.

1) An attack against the firewall itself. Vulnerabilities will have been researched for the type of firewall in this design. An attack against the firewall will be chosen and the results of the attack explained.
2) A denial of service attack. A theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods will be employed. A description of the countermeasures that could be put into place to mitigate the attack will be included.
3) An attack plan to compromise an internal system through the perimeter system. A target will be selected and the attack process described.

Mr. Millican's network design is depicted below.

© SANS Institute 2000 - 2002, Author retains full rights.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

An attack against the firewall itself -

Vulnerabilities will have been researched for the type of firewall in this design. An attack against the firewall will be chosen and the results of the attack explained. In this case, the attack could be directed at the firewall running BIND, creating a denial of service or at the internal DNS server, creating a denial of service.

One thing can be said about the world of open source. Albeit on the surface it may come across that the products are poorly designed and written. Quite the contrary is true. Many excellent products are freely distributable on the Internet today. The reason for so many reported vulnerabilities may be that people have access to the code and can really exercise the code, thus exposing vulnerabilities. It's an interesting cycle when one really thinks about the game that is being played out day in and day out, and hopefully if we are notified of a new vulnerability BEFORE our systems are compromised, who really is the benefactor. US. This is actually a good thing. It may require more effort on the part of the administrators to keep up with their selected open source product, but in the long run it may be a more secure product having been beaten on by, let's face it, very talented individuals. So, we should not despair when yet another vulnerability is discovered in an open source product, rather we should applaud the people that are spending so much time beating on the products so that we can be made aware of the vulnerabilities and fix them.

Mr. Millican's IPChains firewall script is, very tight. Though I don't think it very realistic to believe that a companys' road warriors can do without access to company email while out of the office, but I don't know a whole lot about the company from his description.

In the "CONFIGURING THE FILEWALL" section of Mr. Millican's practical, he states the following, "*the firewall should be hardened by applying all appropriate patches, uninstalling all unnecessary software, eliminating all services that are not needed, and securing any remaining ports*". As not to take anything for granted regarding what services may or may not be running on Mr. Millican's firewall, the attack I have chosen will attempt to exploit an identified vulnerability in BIND.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CERT Advisory, CA-2000-20 was reported on 11/13/00 affecting Red Hat Linux – version 6.1 (among others), the version of Linux that this firewall is running on. Specifically, they involve systems running Internet Software Consortium (ISC) BIND version 8.2.2-P6 and systems running name servers derived from BIND version 8.2 through 8.2.2-P2.

The vulnerability is the ZXFR bug and affects ISC BIND version 8.2.2, patch levels 1 through 6. The Red Hat advisory RHSA-2000:107-04, issued on 11/11/2000 states that BIND versions prior to 8.2.2_P7 are susceptible to remote DoS (denial of service) attacks. If named is open to zone transfers and recursive resolving, it will crash after a ZXFR for the authoritative zone and a query of a remote hostname. It apparently has been reported that not allowing recursive queries may help mitigate against the ZXFR vulnerability, ISC has indicated that this is not the case.

According to the Internet Software Consortium (ISC), a partial workaround can be implemented by disallowing zone transfers except from trusted hosts. Noting that if the trusted hosts are compromised, name servers with this bug will be vulnerable to denial of service attacks. Further, ISC has indicated that this attack can be implemented using utilities provided with the BIND package (named-xfer and dig).

The vulnerability is further described in the following advisories and descriptions:

http://www.isc.org/products/BIND/bind-security.html

http://www.redhat.com/support/errata/RHSA-2000-107.html

http://www.cert.org/advisories/CA-2000-20.html

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0888

© SANS Institute 2000 - 2002 Author retains full rights.

Following is an excerpt from the Bugzilla Bug #20546
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=20546
describing how the vulnerability works:

the recursive queried data must NOT be in cache or in a zone that bind is authoritative for. These queries are answered and DON'T kill bind.

My now 100% reproducable testcase:
- machine is called "foo.whatever.de".
- local bind 8.2.2-P5, being authoritative for "whatever.de"
- named being open to zone transfers and doing recursive resolving by himself
- start named (==> empty caches)
- try ZXFR for "whatever.de"
- dig @localhost www.someelseoutthere.de A

=> crash
For a trace, hook up on named via strace -p `cat /var/run/named.pid` before the recursive query.

A Denial of Service Attack (DDoS) –

Distributed Denial of Service (DdoS) attacks have been highly publicized in the media over the last couple of years. Last year for instance, several major web sites were the target of such costly attacks. These attacks served as a wake up call to the Information Assurance community and have been the subject of many long debates on how to best control, prevent, and report such activity.

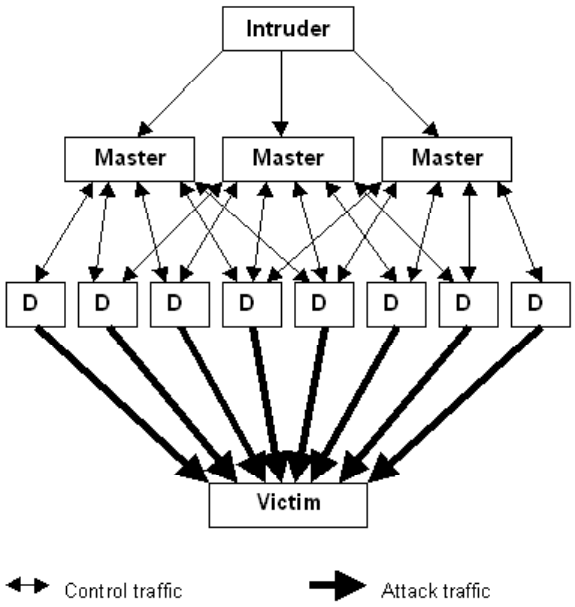
The DDoS attack can be summarily defined as a coordinated attack from many unknowing participants, simultaneously and ultimately targeted against one or more sites. With the proliferation of cable modem/DSL systems in homes throughout the world, in the hands of inexperienced and unprotected home users, DDoS attacks could potentially be coordinated with little difficulty.

A DDoS starts with an Intruder compromising many unsuspecting systems out on the Internet, by exploiting any number of vulnerabilities on those systems.

© SANS Institute 2000 - 2002, Author retains full rights.

The first victim and unwitting participant. The compromised system or systems are then loaded with hacking and/or cracking tools and DDoS programs. These systems can be referred to as the Masters. The Masters, through the use of the tools that were installed by the Intruder then seek out potentially hundreds or thousands of other vulnerable systems that they can deploy the DDoS Daemon onto. The actual attack is when the Intruder runs a program on the Master or Masters systems that in turn communicate with the DDoS Daemons. The unwitting systems that contain the DDoS Daemon then conduct the attack.

The following graphic, from the CERT article titled "**Results of the Distributed-Systems Intruder Tools Workshop**" at **http://www.cert.org/reports/dsit_workshop-final.html**, depicts the structure of systems used in a DDoS attack



There are many different types of DDoS attacks in the wild today. September 2000, a new DDoS tool called Trinity v3 was reported. Trinity is capable of launching several types of flood attacks on the target victims site, such as the following:

- tudp: udpflood
- tfrag: fragmentflood
- tsyn: synflood
- trst: rstflood
- trnd: randomflagsfloo

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- tack: ackflood
- testab: establishflood
- tnull: nullflood

Other commands available to Trinity v3:

- ping: Ping each client. The client will respond with "(trinity) someone needs a miracle..."
- size : Set the packet size for the flood, 0 for random.
- port : Set which port to hit, 0 for random.
- ver?: Get the agent's version.

As IRC and AOL's ICQ is so widely used by home cable modem/DSL users, this will be the exploited vulnerability. The DDoS attack is the Trinity v3 Attack. This exploit is controlled via IRC or ICQ. When a system has been compromised and the Trinity v3 tool installed, each compromised machine joins a specified IRC channel and waits for commands from the Intruder. The Intruder uses these Internet-connected systems to launch a packet flooding denial of service attack against one or more targets. Trinity appears to use primarily port 6667 and also has a backdoor program that listens on TCP port 33270.

There are many tools available to detect and remove the Trinity v3 program from the compromised systems. System administrators should ensure that their TCP port scanners are configured to scan for port 33270. Machines found to be listening on this port may have Trinity installed. It is important to note that if Trinity v3 is found on a system, root level access may have been compromised.

However, the news is not so good for the ultimately targeted site or sites. Although an organization may be able to harden its own systems to prevent the Trinity daemon from being installed, there is essentially little a site can do with currently available technology to prevent becoming a victim of a coordinated network flood. The impact on the target site or sites is really dependent upon the security, or rather the lack of security, of other sites.

As described in the Cisco document entitled "Improving Security on Cisco Routers", located at http://www.ieng.com/warp/public/707/21.html#flood , "careful router configuration can reduce the impact of such floods". By filtering

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

out the flood attack on the router at the source end of the line should be effective, but filtering at the destination end will have little or no effect. Employing filtering protections that place an even heavier burden on the router may make matters worse.

The following resources were used referenced while writing this section:

http://www.cert.org/reports/dsit_workshop-final.html
http://www.cert.org/incident_notes/IN-99-07.html
http://www.cert.org/incident_notes/IN-2000-10.html
http://www.sans.org/infosecFAQ/threats/DDoS.htm
http://xforce.iss.net/alerts/advise59.php
http://www.nipc.gov/warnings/alerts/1999/trinoo.htm
http://www.nipc.gov/warnings/advisories/2000/00-055.htm
http://www.fbi.gov/pressrm/pressrel/pressrel99/prtrinoo.htm
http://www.ieng.com/warp/public/707/21.html#flood

An attack plan to compromise an internal system through the perimeter system –

There are several ways to discover vulnerabilities in servers, many of which were described earlier in this document in the Security Assessment section. Much could be learned about the DNS, Web, and Mail servers out on the screened network in Mr. Millican's design.

© SANS Institute 2000 - 2002, Author retains full rights.

DNS servers are often susceptible to BIND vulnerabilities, one of which is described in the first attack attempt above.

Web server vulnerabilities are almost too numerous to mention. For that reason, web servers are often an easy mark for malicious intruders. Firewalls, in many cases will not protect a web server from many of the exploits being used today. The number and types of tools available to perpetrate attacks on web servers include, but are certainly not limited to script attacks, tools that take advantage of poorly configured HTTP or SSL services, and tools that exploit improperly set permissions, just to name a few.

One example of a script attack is found in the following CERT advisory: CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests
http://www.cert.org/advisories/CA-2000-02.html

Otherwise known as a Cross Site Scripting Vulnerability by Apache, the following link further describes this vulnerability, as Apache describes "is not an attack against any specific bug in a specific piece of software".
http://www.apache.org/info/css-security/

Basically this vulnerability describes, from the web site developers perspective, how a web server that does not adequately ensure that generated pages are properly encoded to prevent unintended execution of scripts, could inadvertently present malicious HTML to the requesting user.

As this is from the web site developers' perspective, developers of web pages should recode dynamically generated pages to validate output. Web site administrators should also obtain and apply any patches from their web server vendor.

The mail server, if not set up properly, could potentially allow SMTP relay. This is one quick way to get your site black listed and it's so easy to lock down.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Design Under Fire Conclusion –

While Mr. Millican's network design and security implementations are sound, as stated at the beginning of this exercise, no network is completely invulnerable to attack. The attack could conceivably come from anywhere and when you least expect it. The important thing to remember and it's something that makes this field so exciting and envigorating is that, you can never "know it all"! You can read everything you can get your hands on, play with things to see how you can break them and then fix them, but IT Security is and always will be the race that never ends, except for maybe in a CRASH!

© SANS Institute 2000 - 2002, Author retains full rights.

REFERENCES AND RECOMMENDED READING

Books:

SANS Institute	"Solaris Security Step-By-Step"
W. Richard Stevens,	"TCP/IP Illustrated, Volume 1."
Garfinkel & Spafford,	"Practical UNIX and Internet Security"
Chapman & Zwicky,	"Building Internet Firewalls"
Cheskwick & Bellovin	"Firewalls and Internet Security – Repelling the Wiley Hacker"
Northcutt & Novak	"Network Intrusion Detection An Analyst's Handbook (2nd Edition)
Brenton, Chris	"Mastering Network Security"
Austin & Hauman	"PKI Essentials:Planning and Implementing Digital Certificat Systems"
Ford & Baum	"Secure Electronic Commerce (2nd Edition)"

WWW:

SANS Institute Online	http://www.sans.org
SecurityFocus	http://www.securityfocus.com/
CERT - Security Improvement	http://www.cert.org/security-improvement/
Frank Keeney – Cisco ACL's	http://pasadena.net/cisco/secure.html
Insecure.org	http://www.insecure.org
Lance Spitzner's Security Papers	http://www.enteract.com/~lspitz/papers.html
The HoneyNet Project	http://project.honeynet.org/
COAST Homepage	http://www.cerias.purdue.edu/coast/coast-library.html
Packetstorm	http://packetstorm.securify.com

Products Mentioned in this paper – Listed Alphabetically

Alteon WebSystems (Part of Nortel Networks)	http://www.alteonwebsystems.com/
Cisco Systems, Inc.	http://www.cisco.com
Internet Security Systems, Inc.	http://www.iss.net
Network Associates, Inc.	http://www.nai.com
Network ICE Corporation	http://www.netice.com
Sun Microsystems, Inc.	http://www.sun.com
Symantec Corporation (Axent)	http://www.axent.com
Tripwire, Inc.	http://www.tripwire.com
Visa U.S.A., Inc. – Merchant Resource Center	http://www.visabrc.com/doc.phtml?2,64,932,932a_cisp.html
Websense, Inc.	http://www.websense.com

© SANS Institute 2000 - 2002, Author retains full rights.

WebTrends Corporation http://www.webtrends.com

© SANS Institute 2000 - 2002, Author retains full rights.