Global Information Assurance Certification Paper

GIAC

Firewall Security Analyst

Practical Assignment

Version 1.5b

By Kenneth McVicker

Date: 4/2/2001

Abstract:

This paper is a security design for GIAC Enterprises. GIAC Enterprises is an internet startup which has just completed a merger. A security architecture will be presented and a security policy defined. The system will be audited and finally an attack on a similar system will be discussed.

Security Architecture

Introduction

GIAC Enterprises is a provider of fortune cookie sayings with sales of $200 million per year. As a fortune cookie saying provider, GIAC Enterprises must collect fortunes from partners and suppliers, store them and distribute to customers on demand. As the fortune cookie sayings are needed world wide, we must provide fortunes all hours of the day in a secure and reliable manner.

Overview

GIAC Enterprises has recently completed a merger. A large variety of operating systems and security devices are available from the two companies, which must be combined into one comprehensive system. One of the companies consisted of Solaris, HP-UX and AIX and the other used LINUX, Windows NT, and Windows 95/98. For network security we will standardize our systems to Solaris and Linux, as security personnel are most familiar with the operating systems and a the large number of software packages are available for the two operating systems. Current standards will be Solaris 7 and RedHat Linux 6.x. Desktops within the corporation will be migrated from Windows 95/98 to Windows NT to improve internal security slightly. Cisco routers will be used as both companies used them prior to the merger and security personnel the most familiar with these devices.

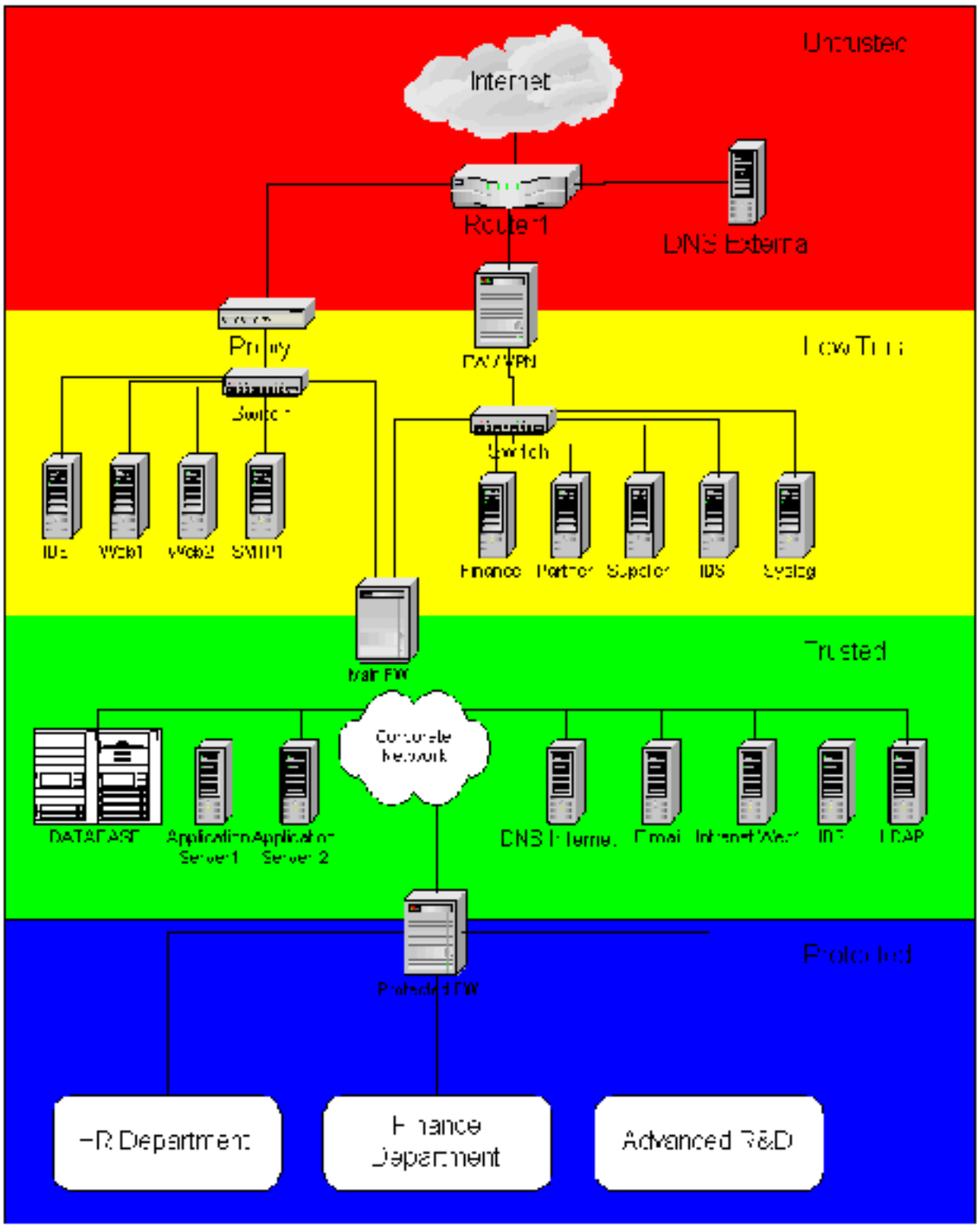
Security Areas

The security design consists of 4 security zones with varying degrees of trust and value of data. Servers are placed in each security Zone according to function, who needs access to it and the trustworthiness required for the data.

Security Zone	Description
Untrusted	A zone open to the Internet that is considered a hostile environment. In this environment system must be hardened.
Semi-trusted	A zone that is protected from the internet but accessible to outside parties for data transfer to and from them.
Trusted	Corporate network available to Employees and contractors which contains private company information
Protected	Data which is considered sensitive to personnel or the corporation, the loss of which could result in great financial loss.

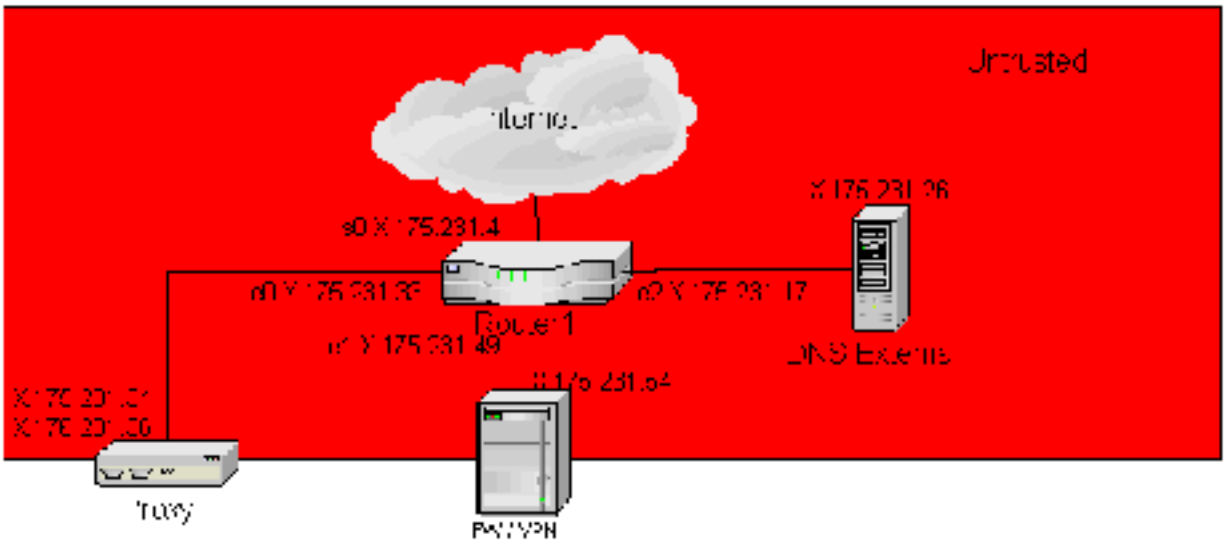
General Design

The following graphic is the overall system design showing equipment located in each zone. Each zone will be presented with the description of the equipment in that zone and the functions outlined. Since we have a site license with I-Planet whenever possible management has directed the use those components (web servers, application servers, directory servers, etc.)



Functions of Servers

Untrusted Security Zone



External DNS

The external DNS server will be a Intel Pentium PC running RedHat Linux 6.x. It will only have ports 22 and 53 open. The external DNS will only contain the DNS entries as follows. Zone transfers will be allowed as we have no internal information available in the DNS. SSH will be used to manage the server remotely. If the DNS server is compromised we have our ISP that will also supply DNS information. Updates and DNS security alerts will be monitored by security personnel and new patches applied as appropriate.

Name	IP
www.giac.com	X.175.231.34
Dns.giac.com	X.175.231.26
Mail.giac.com	X.175.231.36

Router1

Router 1 will be a Cisco 3660 running IOS 12.1 or later with a OC-3 connected to the internet and 3 Ethernet interfaces. ACL's will be used to limit access to the router. SSH will be used for remote management and only be available on the internal interface connected to the FW/VPN. ACL's will also be used to limit services to the Proxy, VPN Firewall and DNS servers. The router will be configured to log to the syslog server in the low trust security zone. The full policy will be presented in the Security Policy section.

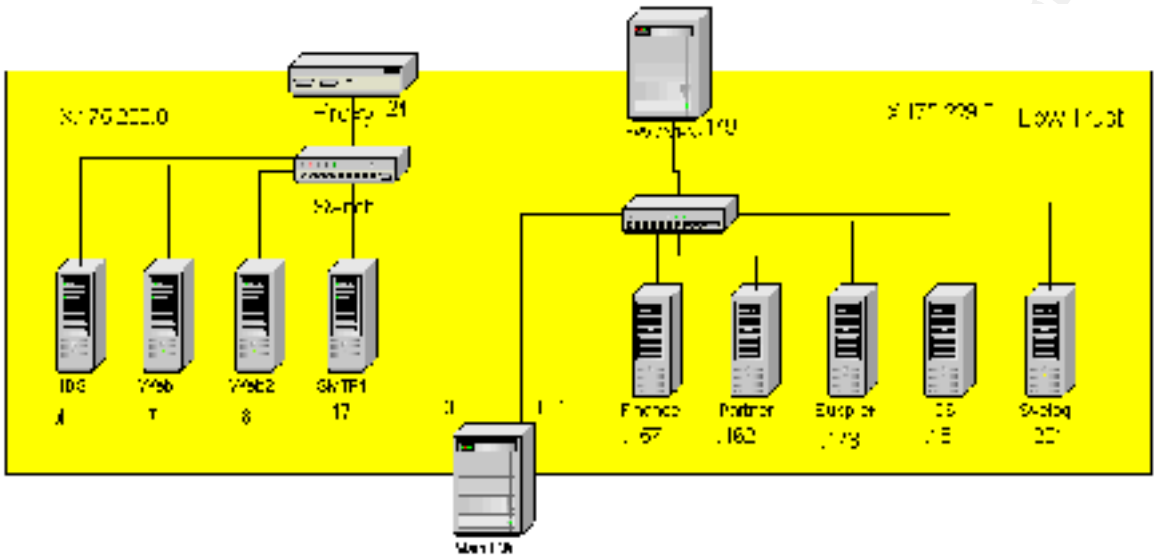
Firewall / VPN

The firewall will be a Sun E450 running Checkpoint Firewall-1 on Solaris 2.7. The server will have all non-essential services removed and be hardened according to a combination of various cookbooks available (www.sans.org, www.sun.com/security). Management will be via SSH using digital certificates authenticated against the LDAP server in the trusted zone. External users and employees will also be allowed VPN access and will authenticated through the use of digital certificates via the LDAP server. Employees will be allowed access through the Main Firewall the FW/VPN to Trusted security zone. Partners and Suppliers will be limited to the appropriate servers in the Low Trust Security Zone. All client access will be through the Proxy server via http and https to the web servers. The firewall will allow ssh connection out to the router and DNS server for management.

Proxy

The proxy will be a Sun E450 running I-Planet Proxy server 3.5 on Solaris 2.7. It will act as a reverse proxy and allow external entities access to SMTP and HTTP, and HTTPS traffic. It will also allow act as a proxy and allow internal users to access the Internet via http, https and allow mail to be sent out.

Low Trust Security Zone



Web

Web servers will be Sun E250s running Solaris 2.7 with Iplanet WebServer Enterprise Edition 4.X, as we have a site license for Iplanet. This server will connect to the Trusted LDAP for digital certificate authentication. All transaction to and from clients will be via SSL using 128 bit encryption. The administration server will be accessible only from the internal IP's and run on port 8876 (not a standard or default port). The administration server will only be accessed via SSL with digital certificate authentication of persons in the LDAP WebAdmin group. SSH access will also be allowed to IPs internal to the corporation that require admin access. The web server will be the gateway to application running on the application server inside the firewall. No CGI's or servlets will be run on the web server. They will strictly run static content and the web connector to connect to the Application servers in the Trusted Zone. CGIs and shell scripts will not be allowed on web servers.

SMTP

This server will be a Intel PC running Linux 6.x. It will also be running Trend-Micro's InterScan VirusWall to block viruses and malicous code in SMTP traffic. We will use InterScan VirusWall's SMTP server. The internal E-mail server will contact this SMTP server once a minute to download and upload new messages.

IDS

Both IDS's will be Intel Pentium PCs running Redhat Linux 6.x. The IDS software will be snort initially. This will be done to get something up and running quickly. We will evaluate both free and commercial products and make a future determination of the direction the company will go.

Finance

This server will be an Intel Pentium PC running Redhat Linux 6.x. It will be available to approved financial institutions with whom we do business. The host will be hardened and have all non-essential processes removed. All data on this server will be stored in encrypted format. All communication to and from will be via SSH or https. The server will have a web server available for displaying pages to external entities.

Partner

This server will be an Intel Pentium PC running Redhat Linux 6.x. It will be available to approved partners with whom we do business. The host will be hardened and have all non-essential processes removed. All data on this server will be stored in encrypted format. All communication to and from will be via SSH or https. The server will have a web server available for displaying pages to external entities.

Supplier

This server will be an Intel Pentium PC running Redhat Linux 6.x. It will be available to approved Suppliers with whom we do business. The host will be hardened and have all non-essential processes removed. All data on this server will be stored in encrypted format. All communication to and from will be via SSH or https. The server will have a web server available for displaying pages to external entities.

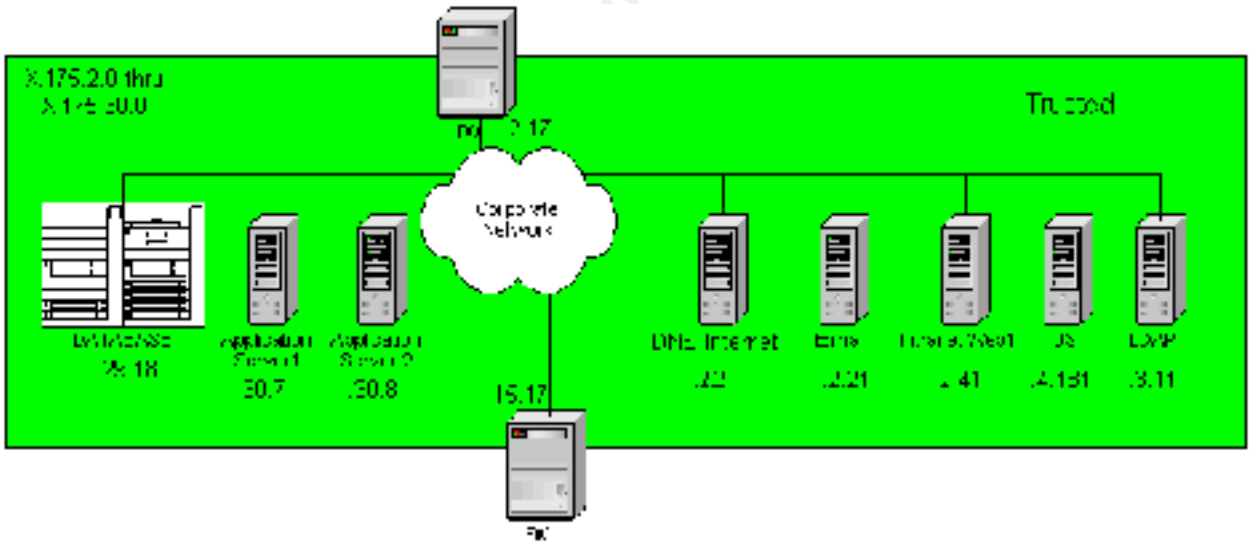
Syslog

This server will be an Intel Pentium PC running Redhat Linux 6.x. It will be configured with 60 GB HD space to allow logs to be kept online for a month. Older logs will be archived to tape for storage for 2 years. Only syslog and ssh will be available.

MAIN FW

The Main firewall will be a Sun E450 running Checkpoint Firewall-1 on Solaris 2.7. The server will have all non-essential services removed and be hardened according to a combination of various cookbooks available. This firewall will isolate the screened networks in the LowTrust Security Zone from the Trusted Zone.

Trusted Security Zone



Database

We will be using a clustered pair of Sun E3500's running Solaris 2.7 for the database running Orade 8i for the Database. Only computing resources in the Trusted Zone and the Protected zones may directly access the database. Password will be set so as to not be easily guessed or cracked. Default passwords will be changed immediately upon installation. SSH will be used by DBA for management so as to not give away their passwords. Telnet will be disabled.

Application Server 1 & 2

The application servers will be Solaris E-450's running Solaris 2.7 and running I-Planet Application Server currently 4.1 with the latest patches. As this is an application server, the version of Java must be watched carefully for security violations. This is one item the security team must track.

Internal DNS

The internet DNS server will be a Intel Pentium PC running RedHat Linux 6.x. It will only have ports 22 and 53 open. The internal DNS will contain the DNS entries for the entire internal corporation. Zone transfers will be allowed only to backup DNS servers within the corporation. SSH will be used to manage the server. This information will not be propagated outside the corporation. Updates and DNS security alerts will be monitored by security personnel and new patches applied as appropriate.

Intranet Web Server

Web servers will be Sun E250 Running Solaris 2.7 with I-Planet WebServer Enterprise Edition 4.X, as we have a site license for I-Planet. This server will connect to the Trusted LDAP for digital certificate authentication. Both http and https will be available to internal users. The administration server will be accessible only from specific internal IP's and run on port 7655 (not a standard or default port). The administration server will only be accessed via SSL with digital certificate authentication of persons in the LDAP WebAdmin group. SSH access will be permitted to personnel internal to the corporation that requiring admin access.

Email

The Email server will be Intel Pentium PC running RedHat Linux 6.x. It will be a pop mail server running Qpopper. It will contact the external SMTP servers 1 time a minute to transfer message to and from.

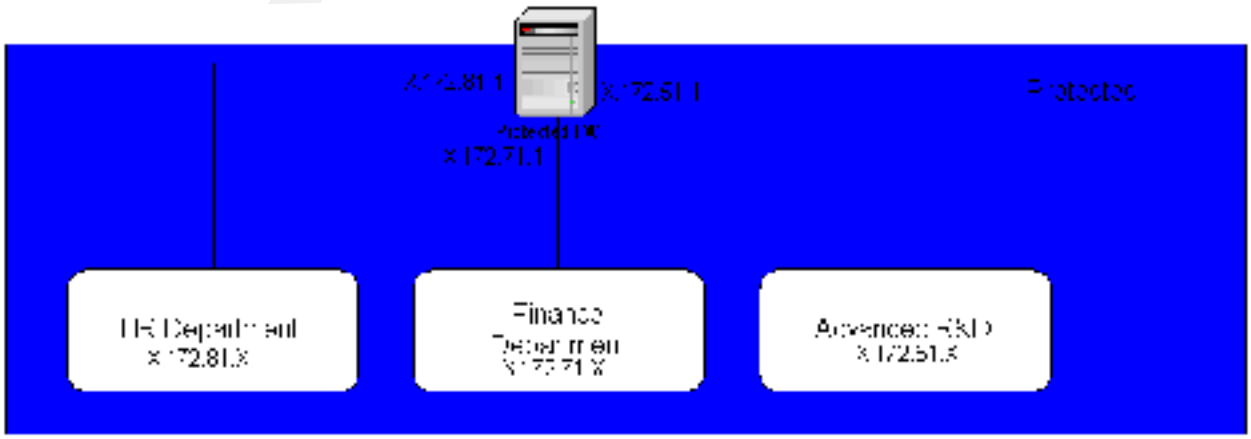
LDAP

The LDAP server will be a Sun E250 Running Solaris 2.7 with I-Planet Directory Server. It will contain the users and group information as well as their valid digital certificates information. It will contain digital certificate information for employees, contractors, partners, financial institutions, and suppliers. This server will be managed via SSH from valid administrators only. All other ports will be disabled.

Protected Firewall

The Main firewall will be a Sun E450 running Checkpoint Firewall-1 on Solaris 2.7. The server will have all non-essential services removed and be hardened according to a combination of various cookbooks available. The protected firewall will screen the normal corporate network from those areas considered sensitive or great value to the corporation.

Protected Security Zone



Not all network segments require separation from other areas. Portions containing personal information, or information where the loss would cause harm to individuals or the corporation will be segmented in to their own security zone. Each area behind a protected Zone will reside in a key card coded area of the building and will have access to the normal corporate network. All connection to the Trusted Zone must be initiated from inside the Protected Zone. The following three protected areas have been identified.

HR Department – contains sensitive personal information about Employees.
Finance Department – Contains financial information about the corporation, bank records and accounts as well as status that could be used for insider trading.
Advance R&D – Contains our latest fortune generation and other corporate research about trends and competitors.

Security Policy

Corporate Security Policy

The policy of Giac Enterprises is to divide networks into security zones with varying levels of trust and value of data on the networks. Employees and contractors may access appropriate data in the Trusted Security Zone. They must take all reasonable efforts to protect and secure all data. Data may be shared with other employees in this zone to allow the normal flow of business. Employees and contractors may access data in the Low Trust Security Zone as necessary. Employees will be issued digital certificates for Remote VPN access, signing of E-mail, and LDAP authentication to web resources. As possible, all connection from a more restricted zone to a less restrictive zone will normally be initiated from the more secure zone (web application servers excepted.)
Clients and general public shall only have access to web servers, SMTP servers and the External DNS server. Employees may access network resources via VPN connections across the public Internet. Partners, suppliers and financial institutions shall access the Low trust Zone thru VPN's. File transfers to and from them will be via SSH, HTTP and HTTPS. Access will only be granted to the servers that are specifically required by the business. VPN access for Partners, Supplies and Financial institutions will be through digital certificates.

Router Configuration

Router 1 will be a Cisco 3660 running IOS 12.1 or later with a OC-3 connected to the internet and 3 Ethernet interfaces. ACL's will be used to limit access to the router. SSH will be used for remote management and only be available on the internal interface connected to the FW/VPN. ACL's will also be used to limit services to the Proxy, VPN Firewall and DNS servers. The router will be configured to log to the syslog server in the Low Trust Security Zone. The full policy will be presented in the Security Policy Section

The entire router configuration will not be presented, such as routing, only those areas involving security.

Global Configuration commands

Command	Reason or Description
no cdp running	Keep this router from trying to detect or receive CDP information from any interface
no ip directed-broadcast	Not allow directed broadcasts
no ip source-route	Not allow source routing
no ntp enable	Disable NTP service
no service finger	Not allow finger to find information about logged in users.
no tcp small-servers	Disallow echo, chargen, and discard
no udp small-servers	Disallow echo, chargen, and discard
no ip http	Disable http server on router
no ip bootp	diable bootp on router
enable secret xxxxxxxx	Encrypt the enable password.
service password-encryption	Encrypt other passwords – this is weak encryption and can be easily cracked

	therefore password should be treated as if in the clear.
crypto key generate rsa	Generate a key pair for use with SSH. Once this is done SSH is automatically enabled.
ip ssh timeout 2	Set the SSH timeout to 2 minutes.
No ip unreachables	Disallow the router from resopnding to servers that do not exist.

Line Console 0

Command	Reason or Description
Login	Require a login at the console.
Password 7 xxxxxxx	set the password.
exec timeout 2	Timeout after 2 minutes if not used.
Transport input none	Not allow connection to console with any protocol.

Line VTY 0-4

Command	Reason or Description
Login	Require a login at the console.
Password 7 xxxxxxx	set the password.
exec timeout 2	Timeout after 2 minutes if not used.
Transport input ssh	Only allow connection to VTY's with SSH.
access-class 15 in	Use the access list named vty-cntrl for controlling access to the vty.

Interface Serial 0

Command	Reason or Description
Access-class internetin in	Apply names access list internetin to the inbound traffic
Access-class internetout out	Apply names access list internetout to the outbound traffic

Interface Ethernet 0

No additional configuration

Interface Ethernet 1

No additional configuration

Interface Ethernet 2

Command	Reason or Description
Access-class e2in in	Apply names access list e2in to the inbound traffic
Access-class e2out out	Apply names access list e2out to the outbound traffic

ip access-list 15

Command	Reason or Description
ip access-list permit tcp X.175.231.54 0.0.0.0	Only allow vty access to the router from the firewall.

ip access-list extended internetin

Command	Reason or Description
Deny icmp any any	Deny all icmp messages.
Deny x.175.0.0	Deny all our internal IP coming in from the internet
Permit tcp any x.175.231.32 0.0.0.15 eq 80	Allow port 80 (http) to any IP in hosts x.175.231.33-47
Permit tcp any x.175.231.32 0.0.0.15 eq 80	Allow port 443 (https) to any IP in hosts x.175.231.33-47
Permit tcp any x.175.231.32 0.0.0.15 eq 25	Allow port 25 (smtp) to any IP in hosts x.175.231.33-47
Permit tcp any x.175.231.26 0.0.0.0 eq 53	Allow tcp dns requests to get to the dns server.
Permit udp any x.175.231.26 0.0.0.0 eq 53	Allow udp dns requests to get to the dns server.

ip access-list extended internetout

Command	Reason or Description
Permit tcp X.175.231.54 0.0.0.0 X.175.231.26 eq 22	Allow SSH traffic for menagement of the DNS External server.
Permit tcp any any eq 53	Allow any tcp requests.
Permit udp any any eq 53	Allow UDP requests to DNS

ip access-list extended e2in

Command	Reason or Description
Permit tcp X.175.0.0 0.0.255.255 any	Allow tcp traffic originating within our network
Permit udp X.175.0.0. 0.0.255.255 any	Allow UDP traffic origination within our network.

ip access-list extended e2out

Command	Reason or Description
Permit tcp x.175.231.26 0.0.0.0 established	Allow established TCP connections return packets
Permit udp any any gt 1023	Allow UDP DNS responses.

Main FW Configuration

The Main firewall will be a Sun E450 running Checkpoint Firewall-1 running at least Service Pack 2 on Solaris 2.7. The server will have all non-essential services removed and be hardened according to a combination of various cookbooks available. This firewall will isolate the screened networks in the LowTrust Security Zone from the Trusted Zone. Management will be via SSH.

The following is the rule set from the Main Firewall it is a screen shot from the CheckPoint-FW1 Policy Editor.

VPN/FW Configuration

The firewall will be a Sun E450 running Checkpoint Firewall-1 4.1 running at least Service Pack 2 or later on Solaris 2.7 and VPN-1. The server will have all non-essential services removed and be hardened according to a combination of various cookbooks available (www.sans.org, www.sun.com/security). Management will be via SSH using digital certificates authenticated against the LDAP server in the trusted zone. External users and employees will also be allowed VPN access and will authenticated through the use of digital certificates via the LDAP server. Employees will be allowed access through the Main Firewall the FW/VPN to Trusted security zone. Partners and Suppliers will be limited to the appropriate servers in the Low Trust Security Zone. All client access will be through the Proxy server via http and https to the web servers. The firewall will allow ssh connection out to the router and DNS server for management.

Employees and Contractors will be required to secure all computing resources used to remotely access GIAC computing resources with the use of a personal firewall device or software. GIAC Enterprises will supply BlackIce Defender to those who are in need of a firewall. Also, Norton Antivirus will be available and should be run monthly by employees to scan for viruses on system accessing GIAC Enterprises resources.

Partners, suppliers, and financial institutions are required to secure their own recourses so as to not provide a platform to attack our systems.

IPSEC will be used for VPN's with the ISAKMP key exchange. We will be using ESP and allowing 3DES. As new encryption algorithms are required, they will be evaluated by the security team through research on the Internet and a determination made as to their possible use. The following is the policy that will be used on the firewall / gateway.

Audit

Audit Plan

Giac Enterprises will audit the system at a minimum of 2 times a year. At least one of the two audits will be performed by an external entity. The others may be performed by internal security personnel. Audits may be conducted more frequently as the environment changes and to verify the fixes to vulnerabilities have be effectively mitigated. The security Audit will consist of five parts. The audit will be planned, perimeter analysis conducted and penetration attempted, a physical and system audit conducted, a report of finding prepared and reviewed, and the top vulnerabilities addresses.

The plan will be to perform the audit at a specific time with a specific window of opportunity. This will be scheduled and the plan signed off by the security manager. Security personnel may not change the configuration of the system during the security audit.

The perimeter analysis scan will be attempted by accessing the public Internet. The scan will be conducted in off-hours times on the weekend. At first, the information that will be used will be that available publicly about the company. Then second the architecture of the system with IP and system types will be allowed to be used. To start with, SAM Spade will be used to gather info on the corporation and it's personnel. DIG will be used to gather information about the GIAC.COM domain. The version of bind will attempt to be discovered. Any known vulnerabilities for the specific version will be attempted. NMAP will then be used to scan the hosts discovered in the DNS zone transfer. Ping and traceroute will also be attempted.

The physical and system audit will check the OS version and patched applied to systems. The auditor will determine if physical access to equipment is sufficient restricted. Versions of software will be recoreded and searched done for vulnerabilities on CERT, SerurityFocus and SANS. Vulnerabilities will be crossed checked with the current patch levels and software version.

A report of findings will be generated by the personnel that performed the audit. They will give an overall rating of the system, point out specific vulnerabilities and list them in critical priority.

The last step is to plan for corrective action for the findings. The most critical will be worked first and corrected. A secondary smaller audit of just the affected systems may be conducted to verify the fixes are in place and working.

Perimeter Analysis and Penetration

As there is no system to audit. This will discuss how to carryout the implementation of the Audit.

To start with, SAM Spade will be used to gather info on the corporation and it's personnel. DIG will be used to gather information about the GIAC.COM domain. The version of bind will attempt to be discovered. Any known vulnerabilities will be attempted. NMAP and ISS's Safesuite will then be used to scan the hosts discovered in the DNS zone transfer. Ping and traceroute will also be attempted to the systems.

Second, the system will attempt to be penetrated with information from and about the system. IP's unknown to the outside(not in the DNS) will be attempted to be mapped with NMAP and SATAN and ISS's Safesuite Internet Scanner as we have worked with the product before.

Third, it will be assumed that the DNS server is compromised and is to be used a platform to attack the rest of the systems. Scan's will be done by placing a laptop with SATAN and NMAP in the position of the External DNS server. Scans will be attempted of the VPN-FW, proxy servers, and Router-1. We will also ISS Safesuite System Scanner to scan all systems. The system will attempt to be used as a denial-of-service platform to attack another site as well as our own site.

Fourth, it will be assumed that one of our web servers has been compromised and we will try from that location to attach the rest of the system again using NMAP and SATAN. We will scan the other servers in this segment as well as the Main-FW and the proxy server. The system will attempt to be used as a denial-of-service platform to attack another site as well as our servers. The same test will take place to show the results as if the SMTP host was compromised. During this attempt we will verify that our IDS detect the attack and reports it properly.

Fifth, it will be assumed that a partner, supplier or financial institution with whom we do business has been compromised and it trying to attack our systems. Again, NMAP and SATAN will be used to attempt to compromise other servers in the segment. During this attempt we will verify that our IDS detect the attack and reports it properly.

Physical and System Audit

The physical and system audit will verify the physical security of computing and network resources. Auditors will verify that access controls are in place and followed. Next the auditors will be given access to see the operational configuration on routers, firewalls, servers, and workstations. Software version and patches will be recorded. These version will be researched and vulnerabilities recorded in the report. This list will be checked once a month by security administrators. They will also subscribe to lists that publish vulnerabilities such as SANS and CERT. System and database passwords cracks will be attempted with l0phtcrack.

Security Administrator's Integrated Network Tool (SAINT) will be used to check for common vulnerabilities. Data in the databases and on servers that is supposed to be encrypted will be checked. We will also use ISS Safesuite System scanner to scan systems to identify additional system security vulnerabilities. We also will use ISS Safesuite Database scanner to scan out database server to determine its security status.

The router configuration will be reviewed including ACL's and VTY access. Firewall rules will be checked and verified for completeness and any backdoor created.

Report

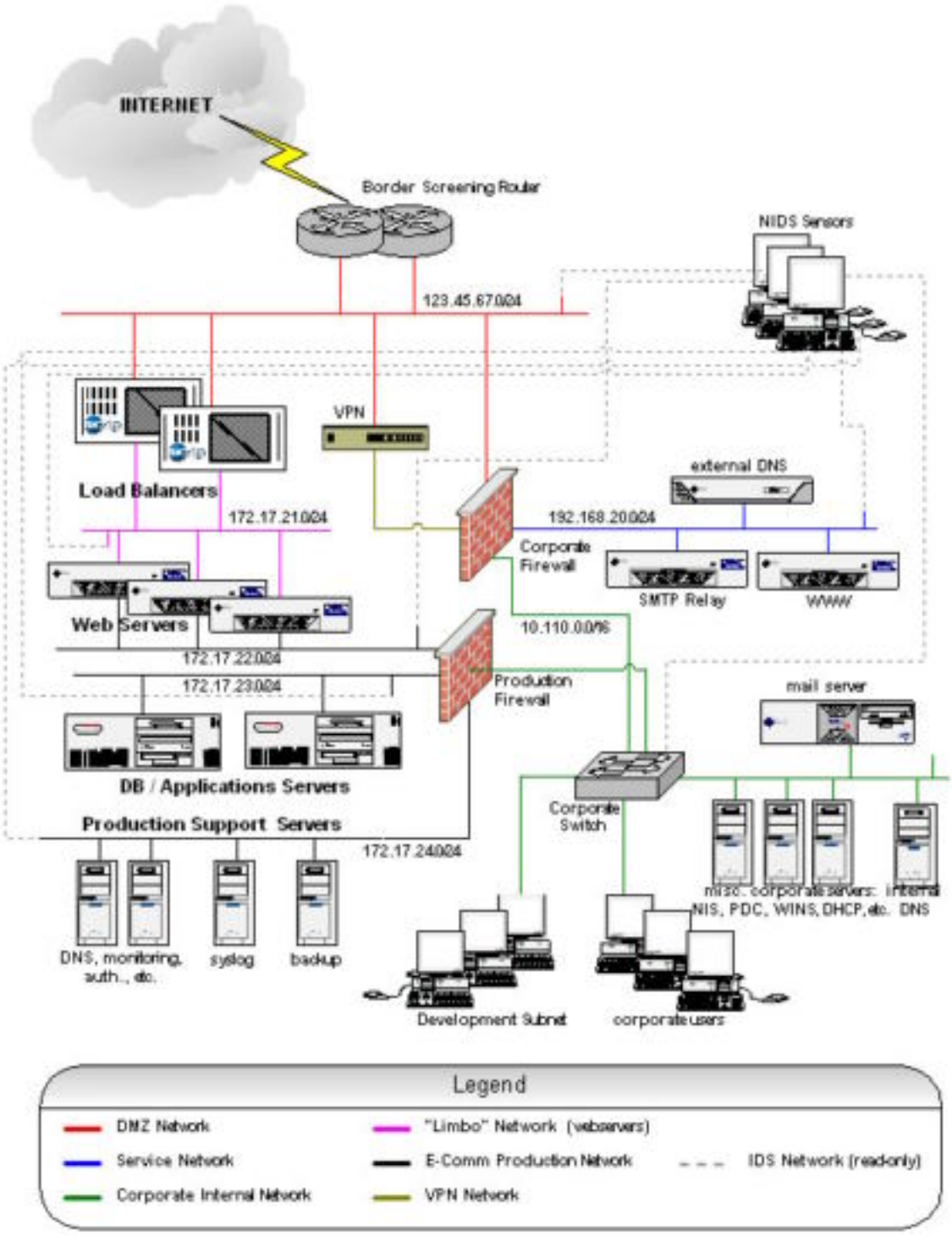
A report of findings will be generated by the personnel that performed the audit. They will give an overall rating of the system, point out specific vulnerabilities and list them in critical priority. The overall rating will be subjective and based on the number of critical findings. Specific vulnerabilities will be listed along with the vulnerable system's name, how they are vulnerable and the degree of vulnerability. These will be listed with the most critical first. Recommendations for fixing the vulnerability will also be included.

Corrective Action

The above steps are futile if corrective action is not taken on critical steps. Each finding will be reviewed and decided as to what action will be taken. A time will be set for each action to be completed. The actions reviewed weekly by security personnel until they are fixed or deemed unnecessary or outdate. An addendum to the above report will be included verifying to the fix.

Design Under Fire

For the design under fire, I have chosen http://www.sans.org/y2k/practical/Alexander_Usenko_GCFW.doc by Alexander Usenko.



Firewall Attack

For the firewall attack, he did not specify any patches and from www.cert.org, I found a vulnerability in Checkpoint 4.1 for IP Fragmentation Denial of service (http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html). This

vulnerability is fixed as of Service Pack 2. We will assume that this Service Pack has not been applied. This vulnerability can be exploited by sending a stream of large IP fragments to the firewall. As the fragments arrive, the mechanism used to log IP fragmentation anomalies can monopolize the CPU on the host machine and prevent further traffic from passing through the firewall. This then denies all others from accessing the firewall.

Denial of Service

For the Denial of service attack assuming that a denial of service can be instituted from 50 compromised cable/DSL modem systems. Since the web servers are not behind a firewall, we can flood them with TCP SYN, UDP or ICMP packets with spoofed IP's. Some load balancing system provide SYN defense like the Cisco LocalDirector. By only allowing a certain rate of SYNs or a certain number of connections that are half opened, it closes them after a certain number or rate has been reached. The Local Director also allows you to turn off the ability to ping the through it and can block UDP packets. Another way to protect the web server would be to put it in a DMZ that way a firewall could do the basic protection of the system. We could also use these web servers to do a ping-of-death attack on another unsuspecting system.

Attack to Compromise Internal Systems

For the Attack to compromise the inside systems, we will first concentrate on the web server as it is the most directly accessible. Assuming it is Apache web server, we will first try the Apache CGI example vulnerability (http://www.cert.org/advisories/CA-96.06.cgi_example_code.html). This allows a remote user may retrieve any world readable files, execute arbitrary commands and create files on the server with the privileges of the httpd process which answers HTTP requests. The example code contains a library function escape_shell_cmd() (in cgi-src/util.c). This function, which attempts to prevent exploitation of shell-based library calls, such as system() and popen(), contains a vulnerability. If running as root, we then have root access.
At minimum we have an account to now begin attacking the web server and possible to go thought the Production Firewall to the application/DB server or to the corporate network.

If web user accounts are used on the system, you could also attempt to monitor transactions to and from the web server to get the admin password. Also this same password could be used to try to access the router or other devices.

References:

Brenton, Chris, VPNs and Remote Access, SANS Security 2001, New Orleans LA

Spitzner, Lance, Advanced Perimeter Protection and Defense In-Depth, SANS Security 2001, New Orleans LA

, Increasing Secuirty on IP Networks, Cisco, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003/html

, Improving Security on Cisco Routers, CISCO, http://www.403-security.org/Advisories/cisco/ci9903.html

, Secure Shell Version 1 Support, CISCO,
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/sshv1.htm

Odom, Wendell, Cisco CCNA Exam #640-507 Certification Guide, Indianapolis IN

www.cert.org

www.sans.org

www.securityfocus.org

http://docs.iplanet.com

http://docs.iplanet.com/docs/manuals/proxy.html

http://docs.iplanet.com/docs/manuals/ias.html

http://docs.iplanet.com/docs/manuals/enterprise.html

http://www.iss.net/securing_e-business/security_products/security_assessment/index.php

http://www.trend.com/products/isvw/