GIAC
CERTIFICATIONS

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.

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

GISO – Basic Practical Assignment

Information Security Officer Training

Version 1.0 (October 30, 2001)

© SANS Institute 2000 - 2005, Author retains full rights.

Prepared by:

Kenneth Low
SANS Network Security 2001
San Diego, California

27 Dec 2001

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Assignment	No.	Contents	Page
1	1.0	**Describe GIAC Enterprises**	3
	1.1	Description of GIAC Enterprises	3
	1.2	IT Infrastructure	3
	1.2.1	Router	5
	1.2.2	Firewalls and VPNs	5
	1.2.3	Internal Private Network & Screen Subnets	5
	1.2.4	Intrusion Detection System	6
	1.2.5	Additional Security Measures	6
	1.3	Business Operations	6
	1.3.1	Client Access	6
	1.3.2	Partner and Supplier Access	7
2	2.0	**Define Security Policy**	8
	2.1	Areas of Risk	8
	2.1.1	Attacks on routers and firewalls	8
	2.1.2	Access control threats	9
	2.1.3	Threats to Reliability of Service	9
	2.1.4	Attacks on default installs of operating systems and applications	10
	2.1.5	Failure to log or detect attacks	11
	2.2	Security Policy	12
	2.2.1	Router & firewall policy	12
	2.2.2	Access control policy	14
	2.2.3	Reliability of service policy	16
3	3.0	**Define Security Procedures**	18
	3.1	Implementation of router & firewall policy	18
	3.2	Testing of routers & firewalls	20
	3.3	Incident response for an attack on routers and firewalls	21
	4.0	**References**	26

List of Illustrations

Assignment	Fig.	Contents	Page
1	1	Diagram of GIAC Enterprises' Network	4
	2	Customer Access	6

© SANS Institute 2000 - 2005 Author retains full rights.

1.0 Assignment 1 – Describe GIAC Enterprise

1.1 Description of GIAC Enterprises

GIAC Enterprises (GE) is a publishing company based in the Republic of Singapore with annual sales turnover of its publications of about S$100 million. Recently, the company acquired a print company in India, Paper Strip Limited, and is preparing to put their sales network online. As GE plans to conduct e-business activities, it needs to develop a sound security policy and procedure that will help govern how the company should do business securely over the Internet. This new e-business initiative will allow GE to sell its publications to its customers over the Internet as well as receive online supply chain support from its subsidiary, suppliers and business partners as well. Hence, GE must establish and enforce a sound security policy and procedure to allow them to do business with these external organizations. Each of these external organizations has their own business needs and will be allowed access into GE's computer network in different ways.

1.2 IT Infrastructure

Before the IT infrastructure of GE was designed, an important security consideration was made – to secure the IT infrastructure according to the Defense-In-Depth principle i.e. adopt a layered security approach and using multiple perimeter mechanisms.

The following illustration gives a high level view of the design. This design can be analyzed by viewing it as discrete components. There are:

1.2.1 Router
1.2.2 Firewalls and VPNs
1.2.3 Internal Private Network & Screen Subnets
1.2.4 Intrusion Detection System
1.2.5 Additional Security Measures

© SANS Institute 2000 - 2005, Author retains full rights.

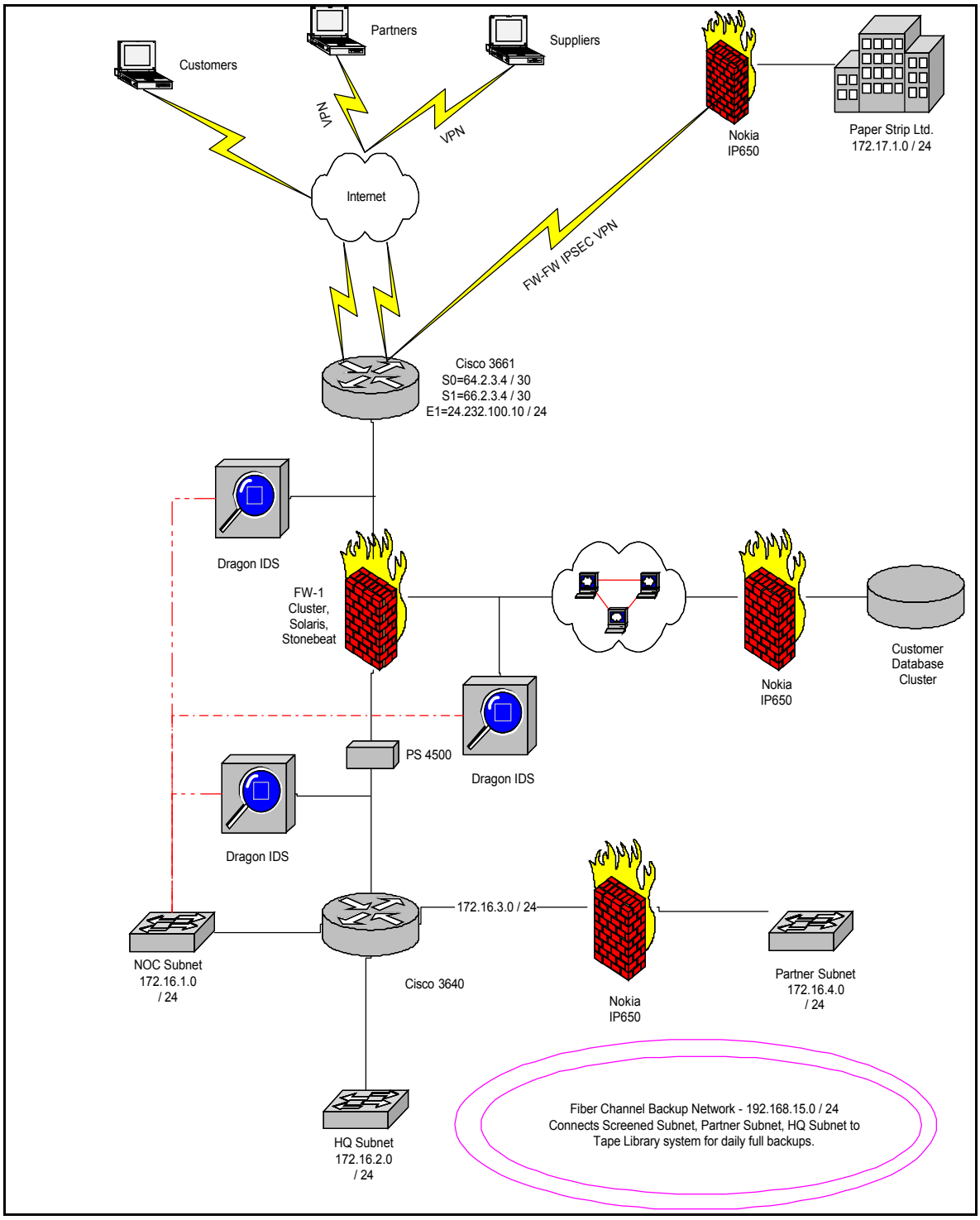


Figure 1: Diagram of GIAC Enterprises' Network

© SANS Institute 2000 - 2005 Author retains full rights.

1.2.1 Router

GE uses a Cisco 3661-AC as its router. To provide redundancy and defend the network against Distributed Denial Of Service (DDOS) attacks, GE is connected to two Internet Service Providers (ISP), each using a high-speed leased line. The router will also allow GE to filter out network attacks such as IP spoofing and DOS attacks. Furthermore, the router will be used to control the packets allowed to enter the demilitarized zone (DMZ).

1.2.2 Firewalls and VPNs

After the router, the second layer of defense is a firewall. In GE's network, a Firewall cluster is deployed using Sun's hardware, Check Point's Firewall-1/ VPN-1 firewall and VPN programs and StoneBeat's load balancing software. The VPN-1 software will provide VPN connections between GE and to GE's customers, suppliers, partners and its subsidiary. The Firewall-1 uses a lot of RAM as it maintains its state tables. We have also found that it the tape drive provides backup capability while keeping our firewalls off of the tape backup network. This helps to isolate the firewalls.

GE has also deployed Nokia IP 650 internet appliances running IPSO 3.3, at other locations on the network to provide access control. IPSO is a hardened version of FreeBSD that is managed from a Web based interface. The firewall software that will we on the Nokia IP650, is Checkpoint Firewall-1 / VPN –1, v4.1 SP3.

At the newly acquired subsidiary, Paper Strip Limited, GE has also installed a Nokia IP 650 with a similar configuration. An IPSec-compliant VPN connection between the Nokia and the Sun Cluster is configured so that all communications between GE and its subsidiary are protected.

1.2.3 Internal Private Network & Screen Subnets

A Cisco 3640 router is deployed to protect GE's HQ LAN. This router will perform packet filtering and route the traffic onto different subnets. The subnets that are created are the:

a. **Users Subnet** - houses a Windows 2000 domain. The Domain Controllers, Exchange Sever, DNS server, and other needed servers are located here.
b. **Network Operations Center (NOC) Subnet** - houses the machines that monitor the network and manage security devices. The management stations for the Check Point firewalls, the Check Point VPN, Cisco routers Entercept and Dragon intrusion detection systems are all located here.

c. **Partner Subnet -** contains Windows 200 servers running Oracle

© SANS Institute 2000 - 2005 Author retains full rights.

databases. The databases will house all of the information about GE's publications and control access to them. GE's partners and suppliers can access this information by establishing a VPN to this subnet and then authenticating to a RADIUS server through a firewall.

1.2.4 Intrusion Detection Systems (IDS)

The Dragon network-based IDS (NIDS) are deployed in GE's network at some strategic choke points to monitor the network. In addition to NIDS, GE also installs the Entercept 2.0 host-based IDS to monitor its web servers and database servers to detect server intrusions.

1.2.5 Additional Security Measures

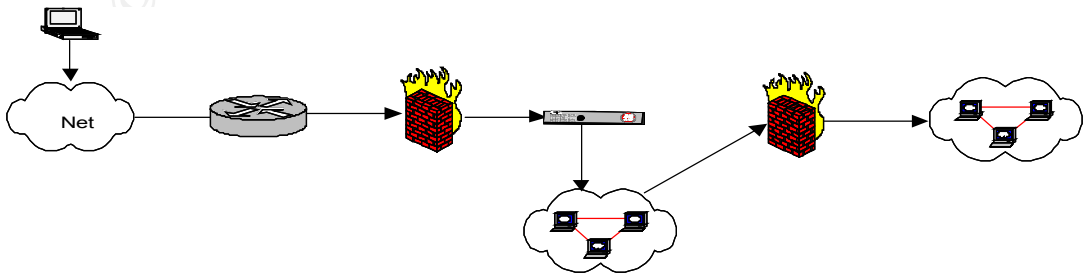
Besides providing digital security mechanisms, physical security and power backup measures are also taken to safeguard the premises of the network.

1) Physical security – CCTVs, card and biometric ID systems are deployed at the building and the network's data center.
2) Power Backup - To safeguard against any possible business downtime, GE's network obtains power from two separate power stations and installs a backup generator that will provide at least 24 hours of electric power.
3) Storage of backup media and sensitive passwords are kept in a fire-resistant safe vault.

1.3 Business Operations

The Internet is central to GE's publishing business. They have customers who will read and purchase their publications and news from the GE's corporate website and frequent email dispatches. Suppliers and partners from around the world access GE's internal database over the VPN. GE also communicates and collaborates with its newly acquired subsidiary over the Internet via the secure VPN link it has established.

1.3.1 Client Access



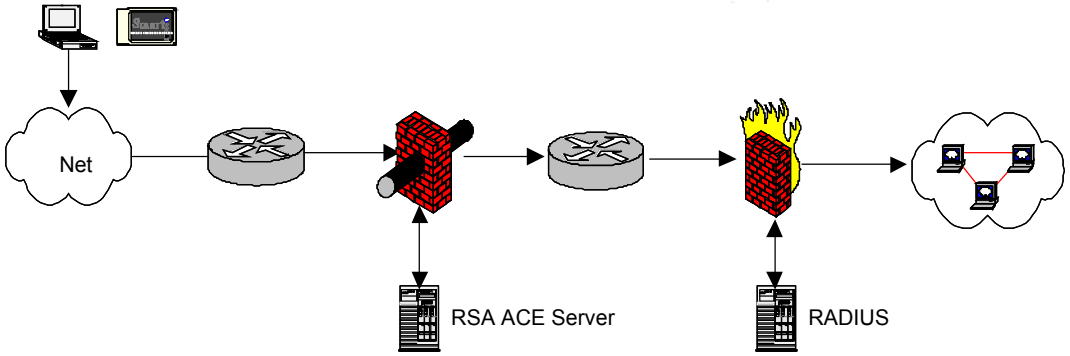
Customer Web Server Access

© SANS Institute 2000 - 2005 Author retains full rights.

Figure 2: Customer Access

Customers access GE's web servers via the Internet, the firewall and to a switch on a screened subnet. This switch has a virtual IP address that is the IP address of www.giac-enterprises.com. When connections are made to the GE's corporate website, the switch will provide load balancing to the web server farm. The customers will connect to the servers, which are running Apache v2.0, using the http and the https protocols. All of the web transactions between customers and GE are secured using 128-bit Secure Socket Layer (SSL) encryption. As customers place orders or inquiries, the web server will contact the Oracle customer order databases that are located behind a firewall on the screened subnet. This will keep customer and adversarial traffic contained to the screened subnet.

1.3.2 Partner & Supplier Access



Partner / Supplier Access

Figure 3: Partner & Supplier Access

GE's business partners and suppliers access GE's databases in a similar manner. All partners and suppliers will have Check Point's SecureClient installed on their workstations and they will be issued with a RSA SecurID tokens to provide 2-factor authentication along with a one-time password. VPN sessions are established to the Check Point firewall using SecurID authentication. In this way, GE's partners and suppliers gain access to the Oracle databases in the Partner subnet. They will be allowed through by authenticating to the Firewall, using the Steel Belted Radius, RADIUS server. All of their transactions with the database will be through a web interface using SSL encryption.

© SANS Institute 2000 - 2005 Author retains full rights.

2.0 Assignment 2 – Define Security Policy

2.1 Areas of Risk

As the security of GE's network is critical to the smooth running of its online business, five (5) areas of risk have been identified. They are

2.1.1 Attacks on routers and firewalls
2.1.2 Access control threats
2.1.3 Threats to Reliability of Service
2.1.4 Attacks on default installs of operating systems and applications
2.1.5 Failure to log or detect attacks

Each of these risk areas is discussed in greater detail here.

2.1.1 Attacks on routers and firewalls

Although GE has deployed routers and firewalls to secure its perimeter, two specific threats in the form of perimeter attacks are of concern to the company – (a) exploitation of unsecured ports and (b) IP spoofing attacks.

a. Exploiting unsecured ports

Unsecured and open ports can potentially allow both legitimate users and unauthorized attackers to connect to GE's network. The more ports that are unsecured and open, the more possible ways that an unauthorized attacker can connect to GE's network. The consequences of this type of intrusion are serious as attackers can disrupt business operations, steal information or change critical data.

To reduce the risk of an exploitation of unsecured ports, it is crucial to keep the least number of ports open on GE's network necessary for the business to function properly. All other ports must be closed. Once the ports that are required to be open are determined, the minimal subset of ports that must remain open for GE's system to function effectively must be identified. After which, all other ports are to be closed. To close a port, find the corresponding service and turn it off/remove it.

b. IP spoofing attacks

Attackers can possibly use spoofing of IP addresses commonly to hide their tracks when they attack GE's network. One possible consequence of a successful IP spoofing attack on GE happens when an attacker use a "smurf" attack which uses a feature of routers to send a stream of packets to thousands of machines. Each packet contains a spoofed source address of a victim. The

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

computers to which the spoofed packets are sent flood the victim's computer often shutting down the computer or the network.
To mitigate the risks of IP spoofing attacks, packet filtering must be performed on traffic coming into your network (ingress filtering) and going out (egress filtering) can help provide a high level of protection. A strong set of filtering rules must be established and enforced at all of GE's router and firewall configurations.

2.1.2 Access control threats

Possible access control threats to GE can come in the following forms:

- Password cracking: Access to password files, use of bad passwords (blank, default, easy-to-guess or rarely-changed passwords).
- External access to password files, and sniffing of the network
- Attack programs allowing internal access to systems (backdoors).
- Attack programs allowing external access to systems (backdoors visible to external networks).
- Unsecured maintenance modes, developer backdoors.
- Modems are easily connected, allowing uncontrollable extension of the internal network.
- Bugs in network software can open unknown/unexpected security holes. These holes can be exploited from external networks to gain access to the internal network. As software becomes increasingly complex, this threat grows.
- Unauthorized physical access to GE's data center.

The reality is that most systems and applications are configured to use passwords as the first, and only, line of defense. As user login names are fairly easy to obtain and dial-up access that bypasses the firewall is a common problem, Therefore, if an attacker can determine an account name and password of an GE employee, he or she can log on to the company's network. Also, there are other problems such as users defining weak passwords, using default passwords and even having no passwords at all (for convenience's sake). Hence, this is clearly an area of great concern to the security of GE's network.

In practice all accounts with weak passwords, default passwords, and no passwords should be removed from your system.

To mitigate the risk of access control threats, these steps are to be performed to prevent unauthorized access to GE's network resources:

© SANS Institute 2000 - 2005 Author retains full rights.

- All accounts with no password are given a password or are removed, and weak passwords are strengthened.
- To prevent users from using weak passwords, all user passwords should be validated. Computer programs are available to reject any password change that does not meet your security policy. These programs ensure that when passwords are modified, they will be of the length and composition required to make guessing and cracking difficult.
- For critical applications, such as VPN communications between GE and its external parties, password-generating tokens (e.g. RSA's SecurID) or biometrics (e.g. Digital Persona's U.are.U) shall be used.

2.1.3 Threats to Reliability of Service

As GE relies on the Internet for taking orders and receive support from its partners and suppliers, the IT operations cannot afford any unplanned downtime. The following list of key threats to the reliability of service have been identified:

- Denial of service attacks
    - Network abuse: misuse of routing protocols to confuse and mislead systems
    - Server overloading (processes, swap space, memory, "tmp" directories and overloading services)
    - Email bombing (message flooding)
    - Downloading or receipt (via email) of malicious Applets, ActiveX controls, macros, postscript files etc.
- Sabotage: Malicious (deliberate) damage or deletion of information or information processing functions.
- Theft of information and media
- Deliberate electrical overloads or shutting off electrical power.
- Virus, Trojans and/or worms
- Change process – loss of critical files during installation of upgrades, new versions, patches.

2.1.4 Attacks on default installs of operating systems and applications

G1.1 Description:

As most of operating systems and applications used by GE come with default installation programs, there are potentially many dangerous security

vulnerabilities inherent in these programs because users do not actively maintain and patch software components they don't use. These un-patched services provide paths for attackers to take over computers.

For operating systems, default installations nearly always include extraneous services and corresponding open ports. Attackers can break into GE's systems via these ports. For applications, default installations usually include unneeded sample programs or scripts. One of the most serious vulnerabilities with web servers is sample scripts; attackers can potentially use these scripts to compromise the GE's system or gain information about the company. In most cases, the system administrator whose system is compromised did not realize that the sample scripts were installed. Sample scripts are a problem because they usually do not go through the same quality control process as other software. In fact they are shockingly poorly written in many cases. Error checking is often forgotten and the sample scripts offer a fertile ground for buffer overflow attacks.

To mitigate the risk of attacks on default installs of operating systems and applications, GE needs to remove unnecessary software, turn off unneeded services, and close extraneous ports. This can be a tedious and time-consuming task. Standard installation guidelines for all operating systems and applications must be developed and used by the organization. These guidelines include installation of only the minimal features needed for the system to function effectively.

5. Failure to log or detect attacks

GE's network is vulnerable to attacks from within and without the network. As new vulnerabilities are discovered every week, it is nearly impossible to defend GE's network against an attacker using a new vulnerability. The failure to log or detect new attacks has serious consequences because there is little chance of discovering what the attackers did and no knowledge of whether the attacker is still in control of the system.

To mitigate this type of risk, logging must be done on a regular basis on all key systems, and logs should be archived and backed up because you never know when you might need them. All essential communications over the security devices (e.g. routers, firewalls, VPN gateways) are to be logged locally and sent to the central NOC subnet for reporting and analysis. This provides redundancy and an extra layer of security. Now the two logs can be compared against one another. Any differences could indicate suspicious activity on the system. Another way to mitigate this risk is to deploy Tripwire data integrity agents across critical servers and devices in the network to detect violations to file integrity. Wherever possible, send logs to a device that uses write-once media.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

2.2 Security Policy

A security policy is written to address the following areas of risk described in the previous section:

- Attacks on routers and firewalls
- Access control threats
- Threats to Reliability of Service

2.2.1 Router & Firewall Policy

a. Purpose / Background

This document describes a required minimal security configuration for all routers and firewalls connecting to a production network or used in a production capacity at or on behalf of GIAC Enterprises.

b. Scope

All routers and firewalls connected to GIAC Enterprises' production networks are affected. Routers and firewalls within internal, secured labs are not affected.

c. Policy Statement:

- Rules for user identification and authentication must be adhered
- The policy and configuration of the firewall must be accurately documented.
- Incoming user connections from the Internet shall use a strong authentication system: one-time passwords, challenge-response, etc..
- Administrator accounts shall also use either a one-time password mechanisms or encrypted login sessions.
- Router and firewall systems must be securely installed. All unnecessary services shall be stopped in the operating system.
- Detailed router and firewall logs must be kept on a dedicated server, with write-once media.
- Logs of all security audits must be kept.
- Logs are to be automatically analyzed and critical errors must trigger alarms.
- Statistics on usage must be available at all times.
- All Internet access from the corporate network must occur over proxies situated in a firewall.
- Default configuration: unless otherwise specified, services are forbidden.
- All users are allowed to exchange email with the Internet
- R&D department users are allowed to use WWW and ftp (over proxies). Other users require authorization.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

- Users may not provide services to the Internet.
- Research departments requiring full Internet access for experimental services should not install these services on the corporate network, but on a separate network outside the routers or firewalls.
- Users should not be able to logon directly onto routers or firewalls.
- Internet access to illicit material should be prevented where possible.
- All login sessions to routers and firewalls must use encrypted login or one-time passwords.
- Subversion and spoofing of network services such as routing, DNS and email must be prevented.
- Change management: Updates and configuration changes shall be logged and carried out according to Quality processes.
- Alerts should be raised if important services/processes crash.
- Important services (such as WWW proxy) should be configured for high availability.
- Regular backups shall be made where necessary (e.g. configuration files, changing data such as WWW).
- The router and firewall systems must be audited annually.
- Logs from the routers and firewalls must be archived for at least one year.
- Critical log entries must be examined weekly.
- The integrity of router and firewall files must be checked once a month.
- The routers and firewalls must be available 24h x 7d, maximum downtime 2 hours (during office hours), maximum frequency once per month. Maintenance slot: Friday after 1900 hours.
- Testing of the routers and firewalls system is performed in an environment isolated from your operational networks
- The routers and firewalls are to be retested after every configuration change and periodically using the regression test suite

d. Responsibility

The Chief Security Officer (CSO) can draft, review, approve or modify policy. The Information Security Officer (ISO) will carry out specific policy directives. The Information Security Engineer (ISE) shall ensure that the policy is properly enforced.

© SANS Institute 2000 - 2005 Author retains full rights.

2.2.2 Access control policy

a. Purpose / Background

The purpose of this policy is to protect GIAC Enterprises' electronic information from being inadvertently compromised by unauthorized personnel using legitimate user accounts to access the network resources of the company.

b. Scope

The scope of this policy includes all personnel who are authorized to access the systems that resides at any GIAC Enterprises' facility, has access to the GIAC Enterprises' network, or stores any non-public GIAC Enterprises' information.

c. Policy Statement

- Users are to be provided with the least privileges for the shortest time necessary to do their work.
- All users must be authorized.
- Users must be able to set the privileges of objects belonging to them in their environment.
- Users should be prevented from deleting others user's files in shared directories.
- Root login is only possible via the management console of the system.
- It must be possible to control user access to all objects on the system (files, printers, devices, databases, commands, applications etc.)
- Users must not be able to examine the Access Control granted to other users.
- Accounts must only exist for authorized persons.
- Each user must be identified by his / her username, employee ID number and group.
- Username and group name structure must be standardized enterprise-wide (number of characters, composition) if possible.
- User and groups must be managed by the administrator and not by the users themselves.
- Group accounts are to be avoided.
- Each user should have only one account on the system.
- If guest accounts are used, their working environment should be very restricted
- Guest accounts are not allowed.
- Usernames and passwords should not be distributed in the same communication.
- When a user is transferred or terminates employment, his account should be blocked or deleted immediately. Procedures should exist whereby the personnel administration automatically informs system

© SANS Institute 2000 - 2005 Author retains full rights.

administrators.

- A password-protected screensaver must be activated after 15 minutes of idle time with password protection.
- The current directory should not be included in the users search path.
- Users should be informed of actions that violate security. Likewise they must inform their security administrator if they suspect a security violation.
- If an account is subjected to continuous login failures in short period of time (e.g. 20 attempts in 1 hour), block the account and notify the user. Don't do this for administrative accounts (open a denial of service attack weakness)!
- When a user logs on the following should be displayed:
  1. *A legal notice informing the user of implications of system abuse.*
  2. *The time & device of last successful and unsuccessful login (user should check that they are correct).*
- Logons should only be enabled when necessary (e.g. between 06:00 and 22:00 from Mondays to Fridays.
- Avoid allowing direct super-user logon, especially where more than one person administers a system.
- On Dialup systems:
  1. Disconnect the phone line after (say) 3 unsuccessful login attempts.
  2. It should be possible to specify what ports are available at what time of day.
- If a user enters a bad login name or password, the error message should be the same for both cases. A possible attacker should not be informed if a user account is valid, rather that the combination of account and password is incorrect.
- If an incorrect username/password combination is entered, wait one second before presenting the login prompt again. If the combination is again incorrect, wait 2 seconds, the next time 3 seconds etc. This should slow (& frustrate) attackers and especially automated logon-attack-programs.
- Management must authorize members of the administrator groups.
- It should be possible to specify how many simultaneous sessions a user may have.
- It should be possible to set an expiration date for a user account.

d. Responsibility

The Chief Security Officer (CSO) can draft, review, approve or modify policy. The Information Security Officer (ISO) will carry out specific policy directives. The Information Security Engineer (ISE) shall ensure that the policy is properly enforced.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

2.2.3 Reliability of Service Policy

a. Purpose / Background

The purpose of this policy is to ensure that business information and services are available when needed and to provide the controls to ensure the reliability of services.

b. Scope

The scope of this policy includes all components in GIAC Enterprises' network that could potentially disrupt the availability of business information and services.

c. Policy Statement

- The network is required 24 hours, 7 days a week. Maintenance window Friday 18:00-22:00. Maximum down time during office hours shall be 1 hour, maximum frequency once every two months.
- The network shall be monitored for errors and performance problems. Preventative action should be taken before serious network disruptions occur, where possible.
- Change management: Updates and configuration changes shall be logged and carried out according to Quality processes.
- A label containing the following information shall be stuck on all nodes during installation: Hostname, Machine manufacturer/model, IP address, MAC address, cabling node id (if network topology allows), end of guarantee date and security/helpdesk telephone number.
- Backups should be made regularly and some backup media should be stored regularly off-site.
- Class backups should be stored in a locked safe. All media must be accounted for. Old tapes must be destroyed, not thrown away.
- A backup policy must be documented for each system or group of systems, containing:
  - When and how are (full or incremental) backups made, where are media stored, for how long?
  - How often are backups made, who is responsible for checking their correct operation?
  - How long are indices kept? Where are they stored? How can they be recovered from archive media?
- A restore policy must also exist, containing:
  - Who is responsible for checking correct operation?
  - A detailed description of what utilities are used how to restore data for all applications. (e.g. OS, mechanisms that can restore databases).

© SANS Institute 2000 - 2005 Author retains full rights.

  - In particular a detailed description of how to restore the Operating System after serious disk or other hardware failures is required.
  - The expected restore time for various disaster scenarios should be documented.
- Test the restore policy quarterly.
- Only system administrators should install or update software on servers. Users may not install software on class workstations.
- Systems should be cleanly installed according to vendor instructions.
- A change log, detailing all changes to a system should be kept on EVERY server. It is suggested that as a minimum, a simple text file be created containing the date, sys-admin name, files changed and reason/comment.
- OS installations should include installation of all recommended patches.
- A label containing the following information should be stuck on all machines during installation: Hostname, Machine manufacturer/model, IP address, MAC address, cabling node id (if network topology allows), end of guarantee date and security/help line telephone number.
- Servers should also have: the server name on all peripherals, disk type/guarantee date/super-blocks/configuration, console commands for stopping/rebooting (e.g. special key sequences)

Only patches from the original software vendor should be applied. Patches downloaded from public networks (e.g. Internet) should be checked for integrity using a strong hashing mechanism (e.g. MD5). Patches should be pre-tested in a test environment (for at least a few weeks if possible) before being applied to production systems.

d. Responsibility

The Chief Security Officer (CSO) can draft, review, approve or modify policy. The Information Security Officer (ISO) will carry out specific policy directives. The Information Security Engineer (ISE) shall ensure that the policy is properly enforced.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

3.0 Assignment 3 – Define Security Procedures

This procedural document describes the following aspects of the router and firewall policy:

- Implementation of the router & firewall policy
- Testing of the routers & firewalls
- Incident response for an attack on routers and firewalls

3.1 Implementation of Router & Firewall Policy

The implementation of the router and firewall policy is distributed among the three groups of key personnel of GIAC Enterprises – the users, the ISO and the ISE.

Users

1. All users who require access to Internet services must do so by using software and Internet gateways approved by the CSO.
2. A firewall has been placed between our private networks and the Internet to protect our systems. Employees must not circumvent the firewall by using modems or network tunneling software to connect to the Internet.
3. Some protocols have been blocked or redirected. If you have a business need for a particular protocol, you must raise the issue with your manager and the Internet security officer.
4. One-time passwords (validated by the ISO) and hardware tokens are required for all remote access to internal systems through the firewall.
5. All non-business use of the Internet from GIAC Enterprises' systems is forbidden. All access to Internet services is logged. Employees who violate this policy are subject to disciplinary action.
6. Your browser has been configured with a list of forbidden sites. Any attempts to access those sites will be reported to your manager.

Information Security Officer (ISO)

1. A firewall shall be placed between the company's network and the Internet to prevent untrusted networks from accessing GIAC Enterprises' network. The firewall will be selected by and maintained by the CSO.
2. All other forms of Internet access (such as via dial-out modems) are prohibited.
3. All users who require access to Internet services must do so by using

software and Internet gateways approved by the CSO.

4. The network security policy shall be reviewed every quarterly by the ISE and the CSO. Where requirements for network connections and services have changed, the security policy shall be updated and approved. If a change is to be made, the ISE shall ensure that the change is implemented and the policy modified.

5. The details of the GIAC Enterprises' internal private network must not be visible from outside the firewall.

6. All non-business use of the Internet from GIAC Enterprises' systems is forbidden. All access to Internet services is logged. Employees who violate this policy are subject to disciplinary action.

Information Security Engineers (ISEs)

1. All firewalls should fail to a configuration that denies all services, and require the ISE to re-enable services after a failure.
2. Source routing shall be disabled on all firewalls and external routers.
3. The firewall shall not accept traffic on its external interfaces that appear to be coming from internal network addresses.
4. The firewall shall provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.
5. Secure media shall be used to store log reports such that access to this media is restricted to only authorized personnel.
6. Firewalls shall be tested off-line and the proper configuration verified.
7. The firewall shall be configured to implement transparency for all outbound services. Unless approved by the ISO, all in-bound services shall be intercepted and processed by the firewall.
8. Appropriate firewall documentation will be maintained on off-line storage at all times. Such information shall include but not be limited to the network diagram, including all IP addresses of all network devices, the IP addresses of relevant hosts of the Internet Service Provider (ISP) such as external news server, router, DNS server, etc. and all other configuration parameters such as packet filter rules, etc. Such documentation shall be updated any time the firewall configuration is changed.
9. The firewall will be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse.
10. The firewall shall notify the system administrator in near-real-time of any item that may need immediate attention such as a break-in into the network, little disk space available, or other related messages so that an immediate action could be taken.
11. The firewall software will run on a dedicated computer - all non-firewall related software, such as compilers, editors, communications software, etc., will be deleted or disabled.

© SANS Institute 2000 - 2005 Author retains full rights.

12. The firewall will be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse.
13. All access to Internet services is logged.

3.2 Testing the routers and firewalls

The purpose of the test activity is to verify that the router and firewall devices deployed in GE's network work as intended as defined by the router and firewall policy. Testing the routers and firewalls in GE's system and verifying that it operates properly increase the confidence that these security devices will perform as designed. The security team (CSO, ISO and ISEs) must understand the types of failures that are possible for each system component and recovery techniques for each type of failure. This will allow the security team to exercise the appropriate response and recovery processes when and if these failures occur once the firewall system becomes part of your operational infrastructure. The most common cause of firewall security breaches is due to mis-configurations of firewall system. Hence, GE must undertake to perform thorough configuration testing of the firewall system.

Steps to be taken

1. **Create a test plan** - test both the implementation of the router/firewall system and the policy being implemented by the system.
2. **Acquire testing tools** - network traffic generators (such as SPAK (Send PAcKets), ipsend, or Ballista), network monitors (such as tcpdump and Network Monitor), port scanners (such as strobe and nmap), vulnerability detection tools (there are a range of commercial tools available from various vendors) and intrusion detection systems such as Dragon and Entercept.

3. **Test the firewall functions in your test environment** – test functions such as packet filtering, scan for open and blocked ports, examine firewall logs and verify alert options.

4. **Test the firewall functions in your production environment** – connect the router or firewall system to the multiple-layered firewall architecture and the public and private networks, and test functions such as packet filtering, scan for open and blocked ports, examine firewall logs and verify alert options.

5. **Select and test features related to log files** – determine how the firewall system should respond when the log files are full, select and exercise the appropriate settings for the archival of log files.

6. **Scan for vulnerabilities** - use vulnerability detection tools to scan your firewall system to determine the presence of known vulnerabilities. If patches exist for vulnerabilities that a tool detects, install these on your firewall system and re-execute the tool. This ensures that the vulnerability has been

© SANS Institute 2000 - 2005 Author retains full rights.

eliminated.

7. **Design initial regression testing suite** - select a subset of test cases to be used for regression testing purposes during normal operations. These should include cases that verify that all incoming and outgoing packets are being routed, filtered, and logged as expected as well as service-specific cases that verify that packets requesting specific services (WWW, email, FTP, etc.) are being routed, filtered, and logged as expected.

8. **Prepare system for production use** - create and record cryptographic checksums or other integrity-checking baseline information of your firewall system once you have completed testing. Make a backup of your operational configuration once you have completed testing.

9. **Prepare to perform ongoing monitoring** - given the complex nature of networks, their traffic, and firewall systems, ongoing monitoring is the only way to ensure that you have specified the correct security policy and that the policy is being implemented properly. Ensure that you have the necessary policies, procedures, tools, and staff resources in place to monitor your networks and systems including your firewall system.

© SANS Institute 2000 - 2005, Author retains full rights.

3.3 Incident response for an attack on routers and firewalls

This procedure should detail which actions should be taken in case of a security incident on any routers or firewalls in GE's network. The router/firewall is designed to protect the corporate network from unauthorized Internet access. These security devices have to be regularly monitored for security breaches. When a breach is detected, the security team must know how to react and this the aim of this procedure. The prompt and proper response to an attack on GE's routers or firewalls will enable the speedy protection and restoration of the normal operating condition of GE's network services.

3.3.1 Incident Response Team

Although a security policy for the routers and firewalls is established, it is important to have an Incident Response Team on standby before a security attack on these security devices happens. GE hade made the following considerations in the formation of its Incident Response Team:

- Who are the members of this Incident Response Team?
- How should this team respond to a serious security breach?
- If internal team members are not adequately skilled, should this incident response procedure be outsourced to a managed security provider?
- Who is in charge in the event of a security incident? What is the chain of command?

The key members of the Incident Response Team are the Incident Manager, the Incident Engineer and the Incident Spokesperson. If any primary member of the Incident Response Team is not available, the backup person will be activated.

a. Incident Manager

Primary contact: Information Security Officer
- Telephone numbers
- Email address

Backup contact: Chief Security Officer
- Telephone numbers
- Email address

Responsibilities:
- Ensures that this incident response procedure is enforced.
- Identify the major threats to business continuity.
- Organizes incident response activities and makes key decisions during an incident.

© SANS Institute 2000 - 2005 Author retains full rights.

b. Incident Engineer

Primary contact: Information Security Engineer 1 (primary administrator in charge of routers and firewalls)

- Telephone numbers
- Email address

Backup contact. Information Security Engineer 2 (backup administrator)

- Telephone numbers
- Email address

Responsibilities:

- Administers the routers and firewalls that have been attacked.
- Detect incidents and take appropriate measures to contain damage done to the systems.

c. Incident Spokesperson

Primary contact: Manager, Public Relations

- Telephone numbers
- Email address

Backup contact: Director, Public Relations

- Telephone numbers
- Email address

Responsibilities:

- Provide official information to the media which protects the reputation of GE and the interests of GE's customers and partners.
- Make public statements and issue press releases
- Coordinate various forms of corporate communications.

3.3.2 Incident Response Procedure

In case of an emergency, each of the following points should be considered and acted upon. The principal steps involved are:

a. Preparation: The security team should have read this procedure and be aware of the implications.
b. Incident detection: quick assessment
c. Immediate action: limit damage
d. Public Relations / Communications
e. Detailed situation analysis
f. Recovery: restore data/services/systems
g. Follow-up

© SANS Institute 2000 - 2005 Author retains full rights.

b. Incident detection: quick assessment

What has happened? :

- Source of threat: e.g. Accidental administrator damage/mistakes, accidental disclosure of internal or confidential documents, attack from the Internet, attack from the telephone network, attack from inside the corporate network or a hoax.
- Result of threat: Integrity, confidentiality or availability of systems / services / data may have been affected.

If an attack has occurred:

- Has the attacker successfully penetrated the systems. Can he re-enter at will? Where have intruders been detected? What is the extent of the damage? What is the principal danger posed? e.g. availability, information privacy, information integrity, adverse publicity.
- Note that "obvious" attacks from one source may, in fact, hide a much more subtle attack from a different source.
- Keep contact names, telephone numbers, email addresses off-line. Do not assume that your on-line address book will be available in an emergency.
- If the intruder seems very clever and difficult to stop, then it is worthwhile calling in experts to help.

c. Immediate action: limit damage:

If a serious attack or disaster occurs, the Incident Manager and Incident Engineer must decide on the immediate action to be taken to eliminate the threat or limit damage (depending on the gravity of the situation and user's needs).

- Start an event log: Document every single action taken, events, evidence found (with time & date).

Possible immediate actions are:

- Restore the availability of information and services that have been affected by the attack.
- Affected machines are to be isolated from the network or shutdown.
- The internal private network to be disconnected from the Internet,
- Remove the necessary VPN and remote access servers (if any) from the network, switched off or shutdown,
- Make a copy of all router and firewall logs onto a portable and secure media.

d. Public Relations / Communications

© SANS Institute 2000 - 2005 Author retains full rights.

- **IMPORTANT:** Only the Incident Spokesperson should contact or make statements to the press.
- If details of an attack need to be discussed with anyone via email, use encrypted email with signatures (e.g. via PGP).
- If necessary and authorized by the Incident Spokesperson, report the incident to an incidents site so that other companies can take precautionary actions to safeguard their networks against this type of attack.
- If the action taken to nullify the attack will affect services to users, inform helpdesk on what message to pass on to users. Seek to minimize the disruption to users.

e. Detailed situation analysis

- Prioritize key actions to be taken.
- Determine the extent of damage. e.g. what files have changed? What programs/accounts were added or modified? If modifications are found, check for these modifications on similar systems.
- Quickly establish the facts about what the attacker has done.
- Notify administrators, management and law enforcement authorities as required.

f. Recovery: restore data/services/systems

Depending on the nature of the incident, the following actions may be necessary:

- Clean systems and restore data/programs/services.
- Fix weaknesses found in the system.
- Do not trust programs on compromised systems, compare with safe copies (e.g. OS on CDROM).

g. Follow-up

- Have all of GE's network services been restored?
- Has the weakness used by the attacker been addressed? Has the cause been dealt with?
- Do insurance or legal claims/procedures have to be filed?
- Are changes to this Incident Response Procedure required?
- Are changes to the router/firewall configuration necessary?
- This incident response procedure should be tested, possibly yearly.

© SANS Institute 2000 - 2005 Author retains full rights.

4.0 References

1. Ryan, John. “Secure Network Perimeter Using Checkpoint 4.1”. 8 July 2001.

2. Carpenter, Jeffrey J.. “CERT/CC Overview Incident and Vulnerability Trends”. 17 Aug 2001.

3. Cross, Stephen E.. “Cyber Threats and the US Economy”. 23 February 2000.

4. CERT Coordination Center. “Establish a policy and procedures that prepare your organization to detect signs of intrusion”. 1 December 2001.

5. SANS Institute & Federal Bureau of Investigation. “The Twenty Most Critical Internet Security Vulnerabilities”. Version 2.501. 15 November 2001.

6. SANS Institute. “How To Eliminate The Ten Most Critical Internet Security Threats”. Version 1.33. 25 June 2001.

7. SANS Institute. “A Consensus Of the High Impact, Low Cost, Core Actions for a Program of System and Network Security”. 1999.

8. SANS Institute. “The 7 Top Management Errors that Lead to Computer Security Vulnerabilities”. 14 May 1999.

9. Guel, Michele D.. “The SANS Security Policy Project”. 2001.

10. Guttman, Barbara & Bagwill, Rober, National Institute of Technology & Standards. “Internet Security Policy: A Technical Guide”. 21 July 1997.

11. Fraser, Barbara Y.. “Site Security Handbook”. September 1997.

12. Boran, Sean. “IT Security Cookbook”. 1996 - 2001.

13. Markowski, Roman. “Computer Crimes: Examples of Network Security Attacks”. March 1999.

14. Vono, Vincent. “A General Overview of Attack Methods”. 25 June 2001.

15. Mackey, Richard & Gossels, Jonathan, Information Security Magazine. “A continuing series on the fundamentals of information systems security –

© SANS Institute 2000 - 2005 Author retains full rights.

Mastering Fundamentals, Part 3". March 2000.

© SANS Institute 2000 - 2005, Author retains full rights.