



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 permitted without express written permission.

Table of Contents.....	1
Mihaela_Iftimi_Ilie_GCFW.doc.....	2

© SANS Institute 2005, Author retains full rights.

**Global Information Assurance Certification (GIAC)
GIAC Certified Firewall Analyst Practical
Assignment
(Version 4.1)**



Author: Mihaela Iftimi-Ilie

Submitted date: 31 January 2005

© SANS Institute 2005, Author retains full rights.

Table of Content

<u>Summary</u>	1
<u>1. Assignment 1- Future State of Security Technology</u>	1
<u>1.1 Introduction</u>	1
<u>1.2 The use of honeypots</u>	1
<u>1.3 Honeypots, technical issues</u>	2
<u>1.4 Honeypots, legal issues</u>	5
<u>1.5 Conclusion</u>	7
<u>2. Assignment2 - Security Architecture</u>	7
<u>2.1 Introduction</u>	7
<u>2.2 Understanding the Access Requirements</u>	8
<u>2.2.a Description of the company</u>	8
<u>2.2.b Customers</u>	8
<u>2.2.c Suppliers</u>	8
<u>2.2.d Partners</u>	8
<u>2.2.e Sales force</u>	8
<u>2.2.f General public</u>	9
<u>2.2.g GIAC employees on the internal network</u>	9
<u>2.2.h Networks</u>	9
<u>2.2.i Internet Service Provider</u>	9
<u>2.2.j Remote Management and monitoring</u>	10
<u>2.3 Information infrastructure</u>	10
<u>2.3.1 Uploading of the Fortunes</u>	10
<u>2.3.2 Marketing of the Fortunes to resellers</u>	11
<u>2.3.3 Administration (human resource, general and financial administration)</u>	11
<u>2.4 Access requirements</u>	12
<u>2.6 Security Architecture</u>	15
<u>2.6.1 Network Perimeter Devices</u>	19
<u>2.6.1.a Border Router (only for GIAC Main network)</u>	19
<u>2.6.1.b Firewalls and VPN</u>	19
<u>2.6.1.c Intrusion Detection and Prevention</u>	21
<u>2.6.1.d Internet DMZ</u>	22
<u>2.6.1.e Intranet DMZ</u>	25
<u>2.6.1.f Protected LAN</u>	26
<u>2.6.1.g Management LAN</u>	27

<u>2.6.1.h Workstations LAN</u>	28
<u>3. Assignment 3 – Router and Firewall Policies</u>	28
<u>3.1 Introduction</u>	28
<u>3.2 Border Router Policy</u>	28
<u>3.2.a Ingress ACL</u>	29
<u>3.2.b Egress ACL</u>	29
<u>3.3 Firewall Policy</u>	30
<u>3.3.a Firewall Policy (Main network Primary Firewall)</u>	31
<u>3.3.b Firewall Policy (Satellite Networks Primary Firewall)</u>	35
<u>4. References</u>	37
<u>4.1 Assignment 1</u>	37
<u>4.2 Assignment 2</u>	37
<u>4.3 Assignment 3</u>	38

Summary

This paper includes the following three assignments (a detailed overview for each assignment is included in the introduction of each topic):

- **Assignment 1 – Future State of the Security Technology:** It is short paper on deploying honeypots.
- **Assignment 2 - Security Architecture:** It is describing the security architecture of GIAC Enterprise.
- **Assignment 3- Router and Firewall Policies:** It is providing the security policies for the filtering router and the primary firewall that were mentioned in assignment 2.

1. Assignment1- Future State of Security Technology

Topic: Alert, enemy at the gate! - Deploying honeypots

1.1 Introduction

The techniques with which a hacker attacks your network are becoming more and more complex. It is very hard, even impossible, to prevent all types of attacks used by a hacker simply because you are not aware of all of them.

Prevention, Detection and Response is a well-known cycle used by security professionals. There is no end-to-end security equipment or solution that can cover all the concepts; instead comprehensive security solutions include a mixture of software and hardware components. Honeypots fall under two main categories, Detection and Response. Honeypots have as their primary goal to collect as much information as possible about attacks. The honeypot should operate in stealth mode so that the attacker is unaware of its presence. The information gathered would give the defenders a considerable advantage to be able to protect and prevent attacks on the production systems.

This paper is an attempt to describe the technical and legal implications of deploying honeypots.

1.2 The use of honeypots

There are different views about the use of honeypots. Some people say it is a way to catch a hacker, or to keep him/her busy from attacking your production server. These views probably apply to 'script kiddies', since they are part of the point-and-click generation and do not care what system they hack. A honeypot does not fool the real hackers that you really want to catch and keep from hacking your systems. On the contrary, these real hackers can sometimes use the honeypot as stepping-stone into the rest of your network.

Others say it is an advanced form of Intrusion Detection System where there is real intrusion to detect. If your network gets attacked, there are chances that your honeypots will also be included in the attack. Therefore, if your honeypots are triggered, you know you are under attack. Although, this is a valid use of the honeypots, they put a lot of stress on your company since it requires permanently monitoring the honeypots and taking appropriate action when they are triggered.

Taking in to consideration all the issues mentioned above, the most convenient use of the honeypots is an educational and research tool. They provide information about new exploits (in some cases even with the exploits themselves), rootkits and worms. Using this information you can take appropriate measures to protect your systems. Additionally, statistics reports about your honeypots (threats, port scans and break-in attempts on your network) can be created in order to justify additional security budget for the corporate network to the management board.

1.3 Honeypots, technical issues

Before deploying the honeypots, the purpose of implementing them must be analyzed. Is it to protect the environment by diverting hackers away from the production environment, or is it to strengthen the security of the IT infrastructure by studying the techniques, the kind of tools and exploits used by them? One thing must be very clearly understood – the honeypots cannot replace the firewall, anti-virus or intrusion detection systems. Furthermore, it is important to ensure that honeypots should not pose any risk to the rest of your network, your organization or to any organization within cyberspace. Some important technical issues related to deploying of honeypots are outlined below:

- Never use a honeypot in a production environment. It must be an isolated system that is used only as honeypot. It should be connected to the network you want to monitor (for example an Internet DMZ) and all the traffic to and from the honeypot must be considered malicious. The management of the honeypot system should be via a dedicated line (e.g.: a serial connection or a separate network interface – not the most secure way but the most convenient).
- One of the biggest problems, and probably will continue to be for the honeypot administrators, is how to 'bait' hackers to the honeypot. There is no exact way of doing this. There are some posted bugs or some hints in various documentations or IRC channels. Probably, the best way is to change the domain and IP address of the honeypots as often as possible. In this way, the honeypots appear to be different systems each time. However, this requires good contacts with a number of ISP's or the organization needs to be connected to a backbone.

- Since it is expected that a honeypot will be compromised it must not contain any real information (e.g.: genuine production accounts, passwords or data). It would be a disaster if an account on a honeypot had the same password as its counterpart in the production network and the hacker used this to break into the rest of your system. Therefore, using an old production database as honeypot to emulate a Web application is not recommended.
- Skilful hackers are very suspicious, so the system that acts as honeypot should appear innocuous. Probably, the best solution is that a honeypot should have a default installation of the operating system with some, but not all patches installed. This gives the appearance of a poorly managed system that someone has forgotten to upgrade or fix. This setup raises the level somewhat above the capabilities of most script kiddies. For educational purposes, a hardened honeypot can be deployed that has all the available patches for the operating system installed and all unnecessary services disabled. Using this setup, only hackers that use the latest exploit will break into your honeypot. Therefore, in this way you are provided with new exploits and methods, without all the other noise.
- Since all the traffic to and from the honeypots is considered malicious, it should be logged on a different system. These logs must be analyzed when a break-in has occurred in order to determine what happened.
- The honeypots should not be used to scan and hack other systems. Therefore, all incoming traffic must be allowed but the outgoing traffic must be restricted. However, http and ftp must be allowed so the hackers can download their tools.
- It is very important when building the honeypot that it can serve a number of different operating systems (to see which exploits are being used on different operating systems). A very good choice is to use a Linux platform with VMware (www.vmware.com) as a honeypot. VMware can support a number of operating systems as guest such as: any version of Linux, Windows (95,98,NT, 2000 and XP) and FreeBSD. The honeypot could also be installed with tools such as SPECTER, BackOfficer Friendly or Mantrap. Furthermore, by configuring the firewall to prevent outgoing traffic, the attackers will get trapped in the honeypot once they have managed to penetrate into the internal network
- It is essential that a honeypot can be restored once it has been compromised. When installing a guest OS under VMware, it creates a file on the host OS file system that will serve as disk for the guest OS. Therefore, restoring a compromised honeypot is as easy as restoring a copy of the VMware disk file.

- There is a risk when building a honeypot using a hardened Linux platform with VMware, that a hacker can break the honeypot from the VMware 'prison' due to some buffer-overflow or unknown feature. This would make the honeypot useless, or at least less unreliable. To prevent this scenario the Linux on the honeypot should be patched with security patches such as: grsecurity (www.grsecurity.net) or LIDS (Linux Intrusion Detection System – www.lids.org) or LSM (Linux Security Module – lsm.immunix.org). The honeypot can be additionally hardened using the Bastille Linux hardening scripts (www.bastille-linux.org).
- More and more rootkits and other hacker tools use SSH as a backdoor connection. Since the traffic is encrypted, it is impossible to see the actual traffic that is hidden by SSH. This can be solved using a kernel based on keystroke-logger (<http://keystroke-loggers.staticusers.net/unix.shtml>) for Linux or Unix honeypots. For Windows honeypots, this issue is a quite problematic since most of keystroke-loggers work on the console but not on netcat based network enabled cmd sessions. They could use a NT rootkit that provides some keylogging functionality. In both cases some additional software must be installed on the honeypots, which in itself is an additional risk of being detected. It is important to hide both the software program and the data it generates.

A typical diagram of a honeypot deployment is shown in figure 1.3.

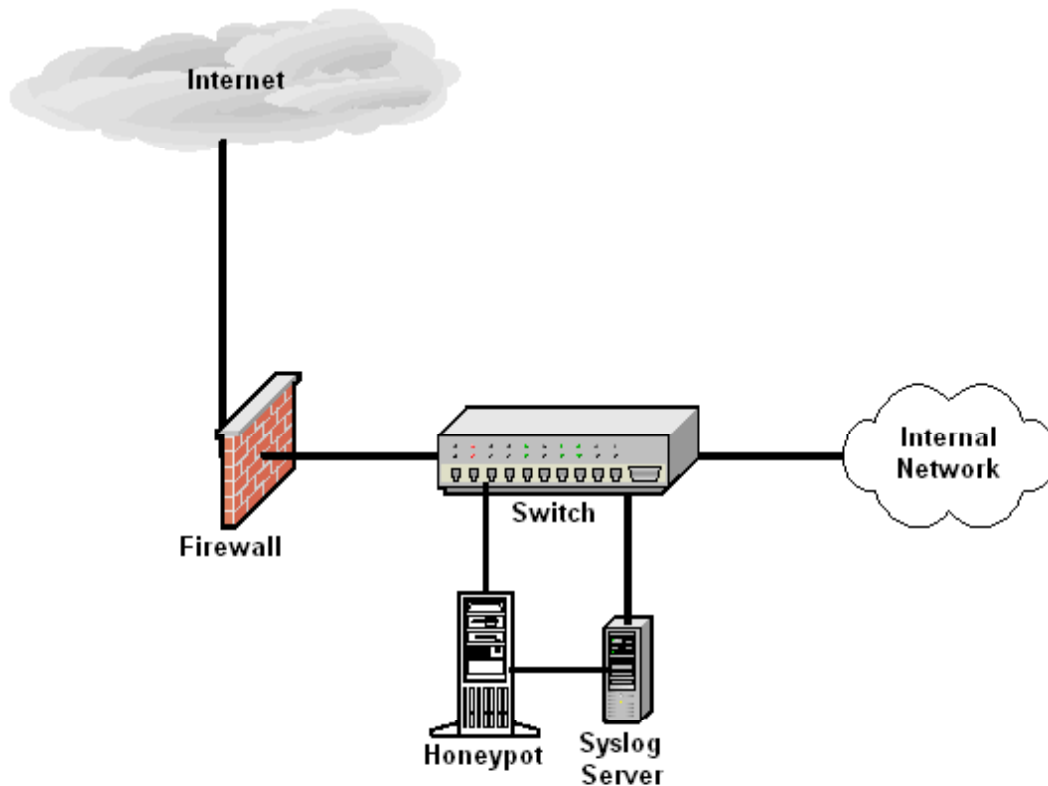


Figure 1.3

The firewall limits both incoming and outgoing traffic. The honeypot captures all the traffic. The Syslog server gathers the logs from the honeypot via a dedicated interface connected to the honeypot. It also provides for management of the honeypot. Analysis of the logs is performed on the Syslog server. The honeypot would be installed with VMware (with any OS – Windows, Linux or FreeBSD) and hardened Red Hat Linux as host OS. The honeypot would have installed software such as BackOfficer Friendly, Mantrap or Specter to gather all necessary information about the hackers' motives. This typical network diagram of a honeypot will be very useful if deployed in an enterprise environment.

There are several honeypot deployment technologies that provide administrators with a lot of flexibility in honeypot type, placement and positioning with the organization. Below are some of the most important categories and deployment strategies of honeypots (a detailed discussion for each of these issues is out of scope of this paper):

- **Production** [Ref1.1]– In this deployment, honeypots are used to mitigate the risks in an organization. They are often used as reconnaissance or deterrence tools
- **Research** [Ref 1.1] – The purpose of this deployment is to gain information on the blackhat community.
- **Low-interaction** – A honeypot that captures limited data regarding an attack such as IP header information
- **High-interaction** – An advanced honeypot that is capable of gathering all the information regarding an attack (including IRC chats and third

- party communication to and from the honeypot)
- **Sacrificial Lamb** [Ref 1.2]– This is a honeypot deployment strategy in which an isolated system has no entry point to any production systems.
- **Deception Ports on Production Systems** [Ref 2] - A honeypot that emulates well-known services (HTTP, SMTP/POP, DNS, FTP)
- **Proximity Decoys** [Ref 1.2]- A high interaction honeypot decoys in close proximity to production hosts (same logical subnet)
- **Redirection Shield** [Ref 1.2] - An upstream router or firewall using port redirection to redirect suspicious traffic to a honeypot that appears as production server.
- **Minefield** [Ref 1.2]- Honeypots (in quantity) placed in the forefront of a system to serve as first attack targets to any scans.
- **Hacker Zoo** [Ref 1.2] - An entire subnet of honeypots with varied platforms, services, vulnerabilities, and configurations; called a zoo because attackers are in “cages” resembling their natural habitat.

1.4 Honeypots, legal issues

There are three main legal issues regarding deploying the honeypots: *Entrapment, Privacy and Liability* (Lance Spitzner, “*Honeypots Tracking Hackers*”, 2003, Pearson Education, Inc). The honeypots might break these legal issues, depending on the purpose and objectives of it. Different countries have different laws regarding honeypot technology. More seriously, some countries may have laws that limit certain honeypot implementations. The following topics raise the most complicated legal issues:

- Is your honeypot really deployed to catch the hackers of your network or you are trying to collect certain information about hackers’ terrorist group and sell this information to a third party? It may look like a non-sense assumption, but it may have an impact on bilateral relations between countries.
- If your honeypot is used by a hacker to launch attacks against another organizations, who is guilty? Your organization or the hacker? Or is there a ‘real’ hacker and not an internal user who launched the attacks? Therefore, each organization should have its own regulations that clearly state the use and implementation of a honeypot.
- Does your organization have the right to capture users’ communication, including that of the outsiders entering in your network? This legal issue may cost an organization a lot of money during a civil lawsuit. Therefore, before organizations implement and deploy a honeypot in their organization, they should seek professional legal advice from their lawyers on the matter to prevent any unnecessary future legal claims

As mentioned above there are three main legal issues regarding deploying of

a honeypot: *Entrapment, Privacy and Liability*.

Entrapment

The legal definition of entrapment is:

“A person is “entrapped” when he is induced or persuaded by law enforcement officers or their agents to commit a crime that he had no previous intent to commit” (Black, Henry Campbell – Black’s Law Dictionary, West Group, 1999)

This is not an issue, since a honeypot is used to neither induce nor persuade attackers. Instead, the attackers target and attack the honeypot on their own initiative.

Privacy

Regarding privacy, it needs to be very clear if the use of the honeypot invades users’ privacy including that of the attackers that hacked the honeypot. And, if this is the case, how much information can or cannot be captured? It depends on the interaction level of a honeypot, they record different amount of activities. A low-interaction honeypot mainly captures small amount of information such as source and type of attack whereas a high-interaction honeypot captures attacker’s communications such as chat programs or emails. Therefore, it becomes a question on how much information can be captured without breaking any laws?

Liability

Will the organization that deploys honeypots be held liable if the honeypots were used to conduct attacks on other organizations, or storing and distributing illegal material? Even if a real hacker performed the attack and not an internal user from the organization, it would not have been successful if the honeypot had been more secure. The risk of the honeypot being compromised can be reduced if the administrator ensures that the honeypot is secure and make it as difficult as possible for an attacker to use it in order to harm other systems. This will include system patching, updating of anti-virus signatures, etc. It also includes deploying updated versions of a honeypot with up-to-date patches. Effective access and data control mechanisms are some of the security measures that can be put in place when implementing and deploying honeypots.

The honeypot administrators have to permanently monitor the logs and content of the honeypot to ensure that the hackers do not store and distribute contraband using the honeypot that may result in legal implications for the organization.

1.5 Conclusion

A honeypot is not a security solution, but a tool. It has the disadvantages and

advantages of a security tool. The biggest disadvantages are the legal issues surrounding this technology (explained in section 1.4). Only by understanding these legal issues can organizations better prepare to face problems that may arise from deploying a honeypot in their organization. Additionally, they are useless if no one attacks them. If the attacker does not send a packet to the honeypot, it cannot detect any unauthorized traffic. However, honeypots can provide valuable information on an attacker's tools, techniques and motives. Using this information, an organization can improve its techniques regarding attack prevention, detection, and reaction.

Further readings: some documents regarding honeypots technology are mentioned in the reference pages.

2. Assignment2- Security Architecture

2.1 Introduction

This section describes the security architecture for GIAC Enterprises, a small company that markets fortune cookie sayings to customers worldwide. The following aspects of security design are discussed:

- The company's strategies as they are related to the development and distribution of fortune cookie
- The network protocols, ports and applications interaction with the company's internal users, remote users, customers, suppliers, partners and the general public
- The security infrastructure including security functions, technical and budgetary factors for each component chosen

2.2 Understanding the Access Requirements

2.2.a Description of the company

GIAC Enterprises is a small company, which markets fortune cookie saying to customers worldwide. GIAC employs fifty people with the majority located in or near its head office, the remainder located in or near the four regional satellite offices geographically distributed around the world.

GIAC is headquartered in Brussels-Belgium and has four satellite offices in: Amsterdam-The Netherlands, Utrecht-The Netherlands, Milan-Italy and Paris-France.

The company's main business strategy is to develop and market fortune cookies in the most profitable way. Therefore, the IT infrastructure must be easy to manage and to expand. In fact, the main requirement of this company, regarding its network, is that the design of its network should be as simple as possible and as secure as possible.

2.2.b Customers

When a customer requests information about purchasing Fortunes cookies from GIAC public Web site, they are requested to enter their geographic location via a web form. Based on the information filled in this web form, they are redirected to the public Web Server of their local reseller.

No purchasing is done via the GIAC public Web Server.

2.2.c Suppliers

GIAC has four suppliers firms that are located in Europe and the US.

- The role of the suppliers is to obtain Fortunes written in English from individual writers. The Suppliers consolidate the Fortunes in text files, which are offered to GIAC. This will be detailed later in this paper.

2.2.d Partners

GIAC has only one type of partner: resellers. The resellers are firms that sell bulk Fortunes to fortune cookie manufacturers. GIAC has ten reseller firms. “Resellers” don’t have access to the GIAC network. The remote users (“sales force”) support the resellers.

2.2.e Sales force

GIAC has six mobile users (“sales force”) with the following location:

- Four in Europe
- One in US
- One in Asia

As mentioned before, the “sales force” supports the “resellers” in getting the Fortunes.

2.2.f General public

The general public information regarding the GIAC business operations is offered to the general public via the GIAC public Web server.

2.2.g GIAC employees on the internal network

GIAC employs 44 office people (“internal users”) and six remote users (“sales force”). The “internal users” are located in the following locations:

- 36 in Brussels (head office)
- 2 in Utrecht
- 2 in Paris
- 2 in Milan
- 2 in Amsterdam

The “internal users” are divided in the following departments:

- Finance – employees who take care of all the financial issues of the GIAC Enterprise. These employees are located in Brussels.
- Administrator/Firewall specialist (Sysadmin) – two employees who

maintain GIAC network. They are located in Brussels.

- Legal reviewers – employees who review the Fortunes for legal copyrights. They are located in Brussels.
- Translation– employees, with the majority located in Brussels, who translates the Fortunes in Spanish, Chinese, Japanese, Italian, Dutch, Portuguese, French.
- Operational – employees who maintain/operate the Fortune database. They are located in Brussels
- Staff – one for each office (Brussels, Utrecht, Milan, Paris, Amsterdam).

2.2.h Networks

The following networks are considered:

- GIAC main network (“Main Network”) – is located in Brussels (since the majority of GIAC employees are located in Brussels). This network is the core of the GIAC network. The GIAC main servers and databases are included in this network. From now on it will be referred to as “Main Network”.
- GIAC satellite offices (“Satellite Networks”) networks – are located in Utrecht, Amsterdam, Milan, and Paris. These are very small networks (only two computers) since each of these offices has only two employees. From now on it will be referred to as “Satellite Networks”.

2.2.i Internet Service Provider

Each GIAC office has its own Internet Service Provider that provides and maintains the border router (a CISCO router), except the GIAC Main network, which provides and maintains its own border router. The ISPs of the Satellite Networks offer daily reports (traffic and log analysis of the border router) to the Sysadmin personnel of the GIAC Main network through an agreement signed with the ISPs.

2.2.j Remote Management and monitoring

Having a business that you can rely upon requires having a robust network. Therefore, the GIAC servers and network devices need to be up 24 by 7. As such, the GIAC system administrators (“Sysadmin”) are allowed to remotely manage and monitor the systems and network devices via SSH (version 2) or VPN connections (for the Satellite Networks).

In order to provide continued assurance of the security of the GIAC infrastructure, the following issues must be taken in consideration:

- Daily review of all security device logs for unusual or suspicious activity that are logged on the central Syslog server (detailed later). This is automated as much as possible on the Syslog server via scripts.
- Monitoring of all relevant newsgroups, mailing lists and web sites to keep abreast of latest developments in vulnerabilities, exploits and patches. A good site with links to many of security related material is www.infosyssec.net.

- Properly defined and tested incident handling and escalation procedures.
- Proper training for the Sysadmin staff is essential.

2.3 Information infrastructure

The main GIAC information infrastructure consists of three business processes:

- Uploading of the Fortunes
- Marketing of the Fortunes to resellers
- Administration (human resource, general and financial administration)

The data concerning each business process mentioned above is stored in a set of databases. These databases are MySQL (www.mysql.com) and use Fedora Core 2 Linux (www.redhat.com/fedora) as underlying operating system. The security of these databases is very important since they contain sensitive information such as information about GIAC business (customers, prices), personal files of GIAC employees, financial information.

The access to each application (in portal or application server), which is connected directly to a database, is controlled by a username and password. To each GIAC employee is assigned a unique username and password. Once they are logged in, access to functions of the application is restricted based on the group they belong to (legal reviewers, translators, financial, staff, operational). Each application has restricted access to tables within a database.

2.3.1 Uploading of the Fortunes

The uploading of the Fortunes from Suppliers to GIAC network consists of following:

- Using a username and password, provided by the GIAC Sysadmin, the Suppliers connect to the GIAC Main network via an Apache web portal (www.apache.org) ("Uploading Portal") in order to upload their text file with Fortunes. The portal is configured to support information transfer to client browsers via 128-bit encrypted HTTPS connection and Fedora Core 2 Linux as operating system. A strong policy was issued by the GIAC Sysadmin personnel for Supplier authentication, having in consideration the importance of verifying the identity of Suppliers:
 - Minimum password length: 8 characters
 - Maximum failed logins before the account is locked: 4
 - Password expiry time interval: 90 days
 - Password must consists of a mix of upper and lower-case letters (placing capital letters in random locations)

The Fortunes are collected from the Uploading Portal by the system that has the Fortune Database installed using a script via SSH.

2.3.2 Marketing of the Fortunes to resellers

This is the description of the business process for marketing the Fortunes to

the resellers. It consists of the following:

- The Legal reviewers connect to the Fortune Database (table “Temporary” – contains all the Fortunes from the suppliers) in order to review the Fortunes for legal copyrights. The Fortunes that pass their review are inserted into the Fortune Database (table called “Reviewed”). The Translators translate the Fortunes from the table “Reviewed”. After the Fortunes are translated, they are inserted in the Fortune Database in different tables separated by language.
- As mentioned in section 2.2.c, the resellers don’t have direct access to the GIAC network. The Sales Force supports them. The Operational connect to the Fortune Database and generate tables for each reseller, based on the Service Level Agreement (SLA) with each reseller. These tables are named after each reseller and are inserted into the Fortune Database in order to be offered to the resellers by the Sales Force.
- All the above operations are intermediated by the JBoss (www.jboss.com) Application Server. The GIAC employees, mentioned in this section, connect to the Application Server with a Web server through a 128-bit encrypted HTTPS connection. The Application Server connects to the appropriate database to provide business information.

2.3.3 Administration (human resource, general and financial administration)

The core of this process is the Administration database. This database contains the most sensitive information such as: administration (human resource, general administration), financial information, documentation and documents regarding GIAC business. Finance department and Staff personnel connect to the JBoss Application Server with a Web browser through a 128-bit encrypted HTTPS connection. In turn, the Application Server will connect to the Administration database via SQL to provide business information.

2.4 Access requirements

The access requirements are summarized the following table, including source, ports, protocols and a description of the purpose of the access:

Source	Destination	Port	Protocol
Sysadmin Staff	Primary Firewalls (Main Network and Satellite Networks) Intranet DMZ Internet DMZ	22/TCP (SSH)	Sysadmin staff SSH access to the primary firewalls and GIAC internal servers (Intranet DMZ) and public servers (Internet DMZ) for management purposes.

GIAC Certified Firewall Analyst (GCFW) Practical v4.1

Sales Force	Primary Firewall (Main Network)	500/UDP (IKE) IPSEC	Permits establishment of VPN client-to-site connection between sales force and Main network Primary Firewall. Where IPSEC includes: AH – IPSEC Authentication Header Protocol port 51. ESP – IPSEC Encapsulating Security Payload Protocol port 50. SKIP – IPSEC Simple Key management for Internet Protocols port 57
Primary Firewall (Main Network) Primary Firewall (Satellite Networks)	Primary Firewall (Satellite Networks) Primary Firewall (Main Network)	500/UDP (IKE) IPSEC	Permits establishment of VPN site-to-site connections between Primary Firewall (Main Network) and Primary Firewall (Satellite Networks).
Suppliers	Uploading Server	443/TCP (HTTPS)	Suppliers HTTPS access to Uploading Server to upload the fortunes text files.
Sales Force	Application Server	443/TCP (HTTPS)	Permits sales force to upload the fortunes database for the suppliers
Internal employees (Main Network) Web Cache (Satellite Networks)	Proxy Server	6120/TCP (Squid)	Allows internal employees (Main network) to access the GIAC Proxy Server in order access the Internet resources via HTTP, HTTPS and FTP. It also allows access the Web Cache (located on each Satellite Network) to Proxy Server. The Web Cache answers to HTTP, HTTPS and FTP request coming from internal employees located on the Satellite Networks. See section: 2.6.1.d –Proxy Server

GIAC Certified Firewall Analyst (GCFW) Practical v4.1

Proxy Server	Internet	80/TCP (HTTP) 443/TCP (HTTPS) 21/TCP (FTP)	Allows the Proxy Server to access the Internet in order answer to HTTP, HTTPS and FTP requests coming for internal users.
Internal employees (Satellite networks)	Web Cache (Satellite Networks)	6120/TCP (Squid) 53/UDP (DNS) 123/UDP (NTP)	Allow internal employees (Satellite network) to access the Internet resources via Squid. It also allows these users to perform internal DNS requests and NTP synchronization from Web Cache
General public	GIAC Web Server	80/TCP (HTTP)	General public access to GIAC public information.
Internet	Mail Relay	25/TCP (SMTP)	Allows inbound emails to enter in GIAC network.
Mail Relay	Internet	25/TCP (SMTP)	Allows outbound emails to be forwarded to the Internet.
Main Relay Email Server	Email Server Main Relay	25/TCP (SMTP)	Allows inbound emails to be forwarded to Email Server and outbound emails to be forwarded to Email Server.
Internal employees (Main Network)	Email Server	25/TCP (SMTP) 220/TCP (IMAP3)	Permits internal employees (Main network) to send and receive emails.
Internal employees (Satellite Networks) Sales force	Email Server	25/TCP (SMTP) 110/TCP (POP3)	Permits internal employees (Satellite Networks) and sales force to send and receive emails.
Internal employees	Internal Web Server (Main Network)	80/TCP (HTTP) 443/TCP (HTTPS)	Permits to all GIAC internal employees access to internal information posted on the Internal Web Server.
IPS DNS Server	External DNS Server	53/UDP (DNS) 53/TCP (DNS)	Permits DNS (requests and zone transfers) from IPS DNS server. Reason – see section 2.6.1.d – External DNS server
Internal DNS Web Cache (Satellite Networks)	External DNS	53/UDP (DNS)	Permits Internal DNS server of the Main network and Satellite networks (Web Cache) to resolve external DNS lookups.

GIAC Certified Firewall Analyst (GCFW) Practical v4.1

Internal Employees (Main network)	Internal DNS	53/TCP (DNS)	Allow internal employees (Main Network) to perform internal DNS lookups.
External NTP Server	ISP NTP Server	123/UDP (NTP)	Allow external NTP synchronized from ISP NTP server.
Internal NTP Server (Main Network) Web Cache (Satellite Networks)	External NTP Server	123/UDP (NTP)	Allow internal NTP synchronization.
Internal employees (Main Network)	Internal NTP Server	123/UDP (NTP)	Allow the internal workstations NTP synchronization.
Internal Employees	Application Servers	443/HTTPS	Allow GIAC internal employees access to GIAC databases (Fortunes and Administration) via Application Server.
Application Server	Fortunes Database Administration Database	3306/TCP (MySQL)	Allow performing SQL commands (update, queries, insert) or download of database tables by GIAC internal employees or sales force via Application Server.
Application Server	Radius Server	1812/UDP (RADIUS)	Authenticates the users who access the Application Server via Radius Server. Some old applications still use the old RADIUS port (1645/UDP), but the GIAC Radius Server uses port 1812.
Linux Servers (located in Internet and Intranet DMZ) Application Server Databases (Fortunes and Administration)	Syslog Server	514/UDP (Syslog)	Permits central management of the logs via a central Syslog server.

Fortunes Database	Uploading Server	22/TCP (SSH)	Permits collecting of the fortunes from Uploading Server where are uploaded by the suppliers. It is done via a script (installed as cron entry on Fortunes Database) that connected to Uploading Server via SSH.
Internal users (Main Network)	Windows Domain Controller	135/UDP (RPC) 135/TCP (RPC) 137/UDP (NETBIOS) 138/UDP (NETBIOS) 139/TCP (NETBIOS)	Permits a common windows domain controller and a central windows update server for each GIAC network (Main network)

2.6 Security Architecture

In keeping with recognized best practices in network security, the design for GIAC Enterprises security architecture applies security in layers. Since all the GIAC business is concentrated in two databases (Fortune Database and Administration Database), the security architecture consists of concentric systems that help to provide “defense-in-depth” *Ref [2.1]* for those databases. In figure 2.6.1 is shown the security architecture of the GIAC Main network including the IP addressing scheme. Where: X.Y.Z.0/28 are public IP addresses.

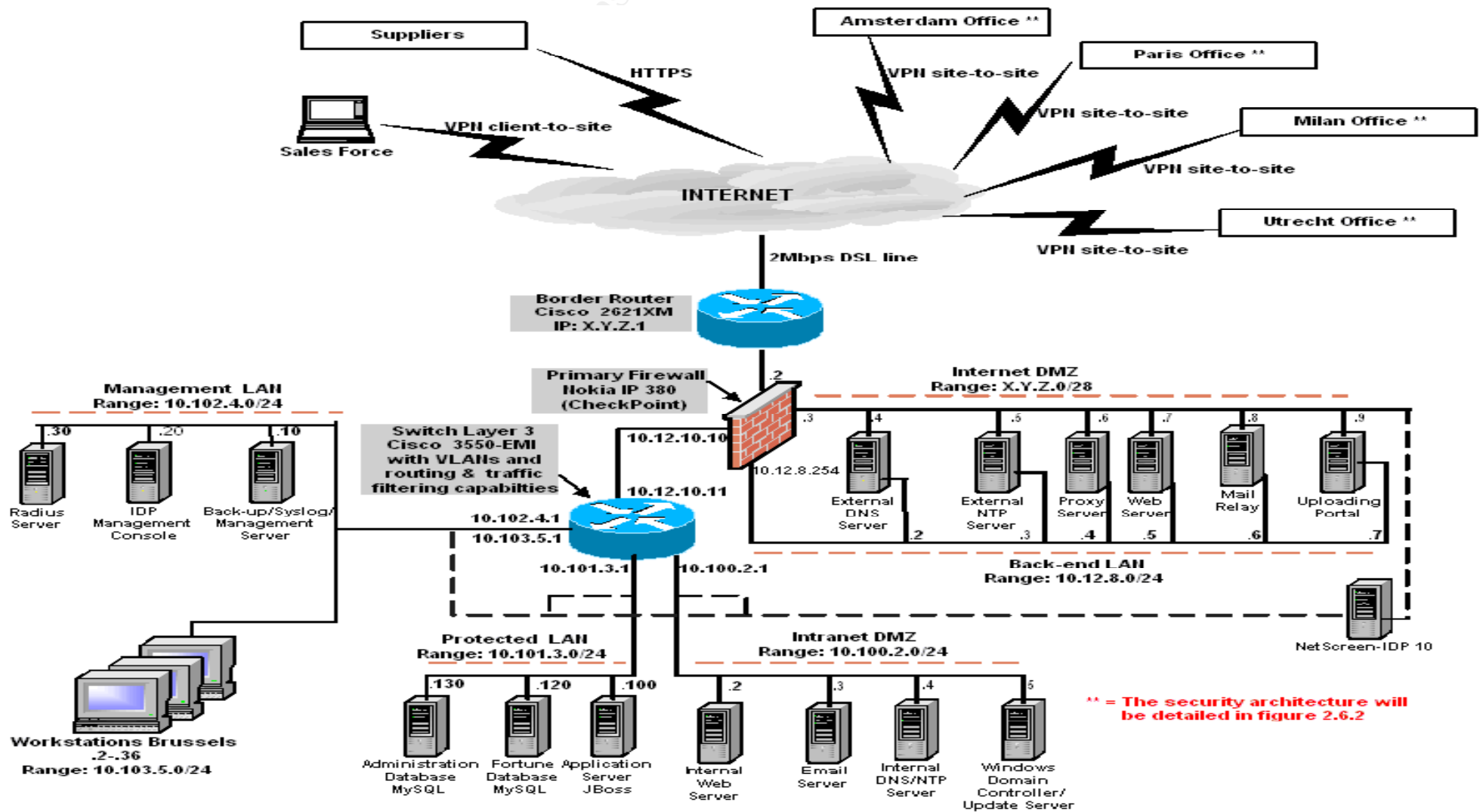
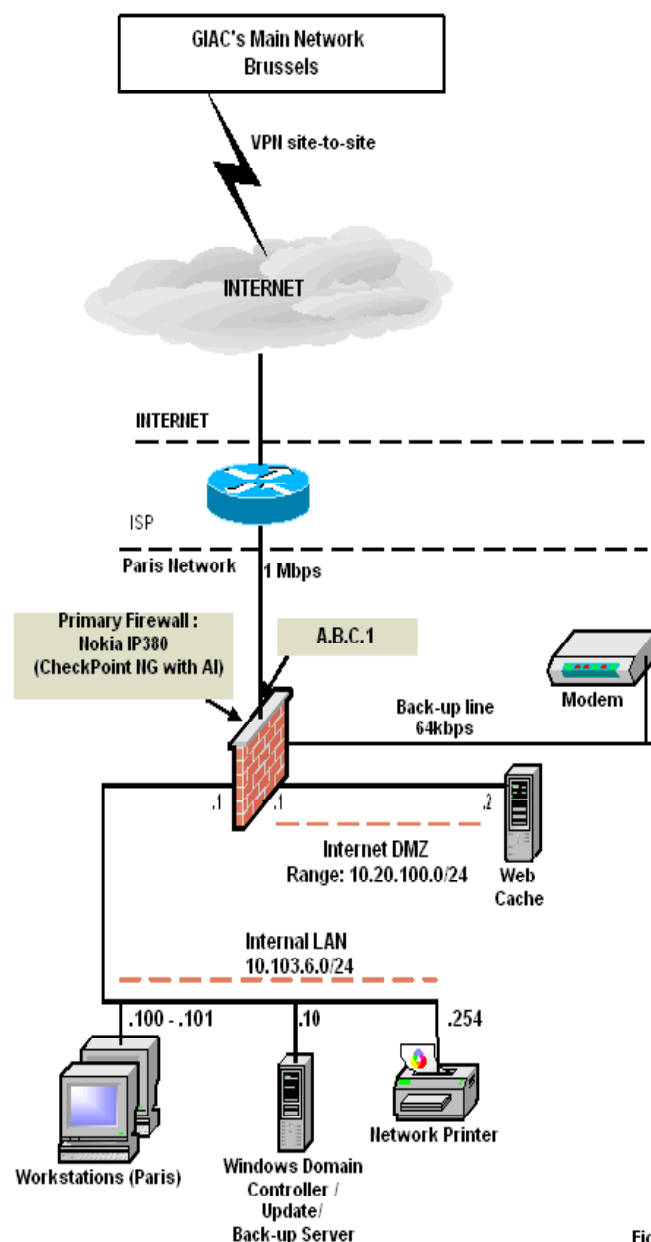


Figure 2.6.1

As mentioned in section 2.2.h the Satellite Networks have the same security architecture. The only difference between the Satellite Networks is the IP addressing scheme. In figure 2.6.2 the security architecture for Paris Network is shown, including the IP addressing for the other Satellite Networks.

Note: In order to reduce the costs, the security architecture of the GIAC Satellite Networks could be simplified by eliminating the Web Cache (since the Satellite Networks connect to the GIAC Main Network via VPN site-to-site, the DNS, NTP, FTP, HTTP and HTTPS requests from the internal users of the Satellite Networks can be answered by the servers located on the GIAC Main Network using an encrypted connection). However, eliminating the Web Cache brings additional security risks - it is more secure to answer to those requests locally than remotely.



The rest of Satellite Networks (Amsterdam, Utrecht and Milan) have the same security architecture with Paris's security architecture and have the following IP addressing scheme (the A.B.C.1 - .4 are public IP addresses):

1. Amsterdam Network

- 1.1 Primary firewall : A.B.C.2
- 1.2 Internet DMZ : 10.20.101.0/24
- 1.3 Internal LAN : 10.103.7.0/24

2. Utrecht Network

- 2.1 Primary Firewall : A.B.C.3
- 2.2 Internet DMZ : 10.20.102.0/24
- 2.3 Internal LAN : 10.103.8.0/24

3. Milan Network

- 3.1 Primary Firewall : A.B.C.4
- 3.2 Internet DMZ : 10.20.103.0/24
- 3.3 Internal LAN : 10.103.9.0/24

Figure 2.6.2

2.6.1 Network Perimeter Devices

All the systems within the GIAC network were hardened according to best practices *Ref [2.2]*.

2.6.1.a Border Router (only for GIAC Main network)

Device: Cisco 2621XM

Operating system: 12.3

Interfaces: 2 fixed 10/100 FastEthernet

The border connects GIAC Main network to the Internet via a 2 Mbps DSL line. It routes IP traffic between the GIAC Main network and the Internet. It is also the first line of defense against malicious attacks initiated by external parties and an attempt to control the traffic initiated by internal users. Access lists (ACL) are constructed and applied to interfaces of router in order to limit the network traffic. Its ACLs will be detailed in section 3.1.

This router is a very critical network perimeter device in the GIAC defense; it needs to be hardened according to best practices *Ref [2.3]*.

A router from Cisco is chosen because of its flexible and advanced-filtering, security integration features and the support available.

2.6.1.b Firewalls and VPN

As part of the “defense-in-depth” *Ref [2.1]* principle the border router, two firewalls (Primary firewall and Secondary) and NetScreen-IDP 10 protect the GIAC Main network. Each of the Satellite Networks is protected only by a Primary firewall (it has been decided by the GIAC board management that due to budget constrains only one firewall can be deployed on each of the Satellite Networks). The Primary and Secondary firewall (located in the GIAC Main network) are chosen from different vendors because if one firewall is compromised due to security vulnerabilities, the other firewall will protect the GIAC internal resources.

- **Primary Firewall** - Its role is to restrict the traffic from the Internet to the GIAC network and between GIAC network segments. The primary firewall (GIAC Main network and for each of the Satellite Networks) is a Nokia IP380 *Ref [2.4]* running CheckPoint Next Generation Application Intelligence (AI) (www.checkpoint.com/products/technologies/ai.html) VPN-1/Firewall-1 software. A firewall from Nokia was chosen because it is a cost-effective system, with support available, for a small network (like GIAC Main network) that demands robust performance for firewall, VPN and intrusion protection. Each of the Primary firewall of the Satellite Networks has a Back-up line (ADSL Modem 64kbps) - in case the main line to one of the Satellite Networks is down, the Sysadmin personnel (located on the Main Network) will still be able to connect to that Satellite Network. The configuration and security policy installed

on each of these primary firewalls are detailed in section 3.1.

- **Secondary Firewall** – It might seem a bit “fancy” to call it firewall, but it does perform traffic filtering through access list. It is included only in the GIAC Main network (for reasons mentioned above). Its role is to restrict, route allowed traffic between the GIAC Main network segments and to create VLANs. It is a layer three switch Cisco 3550-EMI Ref [2.5] with VLANs. It was hardened according to best practices Ref [2.2]. It was chosen because the GIAC Sysadmin personnel are familiar with this product. *“VLANs are useful isolation tools, especially for the purpose of the improving the network’s performance” – Cisco’s “Blueprint for Enterprise Networks”*. However, using VLANs to implement security zones brings additional security risk: *“The capability for human error, combined with understanding that VLAN tagging protocols were not designed with security in mind, makes their use in sensitive environments inadvisable” – Cisco’s “Security Blueprint for Enterprise Networks”*. Plus, a firewall with only packet filter capabilities cannot prevent all types of malicious attacks (e.g.: application layer attacks, viruses and Trojan horses, password attacks, port redirections, worms). Therefore, using Intrusion Detection and Prevention products to prevent malicious attacks coming from within the GIAC internal segments is a must. Why within GIAC internal segments? Because the statistics show that more than 60% of the malicious attacks come from the internal network. The Intrusion Detection and Prevention will be detailed in section 2.6.1.c.

The VPN connections have been setup in “Traditional or Simplified mode per Security policy”. All traffic is protected using IPSEC to tunnel communications. Internet Key Exchange (IKE) is used with 168-bit Triple DES (Triple Data Encryption Standard) key exchange encryption with MD5 (Message Digest) data integrity of the SA (Security Association). The IKE SA (phase 1) is renegotiated every 1440 minutes. The IPSEC SA (IKE phase 2) is renegotiated every 3600 seconds. As shown in figure 2.6.1 the Satellite Networks connect to GIAC Main network via site-to-site VPN. The VPN connections are established between the primary firewall (Nokia IP380) of GIAC Main network and the primary firewalls (Nokia IP380) of the Satellite Networks (Nokia IP380). The Sales Force have installed in their laptops VPN-1 SecuRemote Client from CheckPoint in order to connect to the GIAC Main network via client-to-site VPN. Client-to-site VPN connection is required with the remote users since they don’t have fixed IP address. They are authenticated on the Main Network Primary Firewall using the Radius Server.

Implementing a VPN solution has a lot of advantages (security, cost effectiveness, deployment advantages) but also some disadvantages (processing overhead, packet overhead, hard for troubleshooting) Ref [2.6]. The GIAC Sysadmin personnel were informed about these issues.

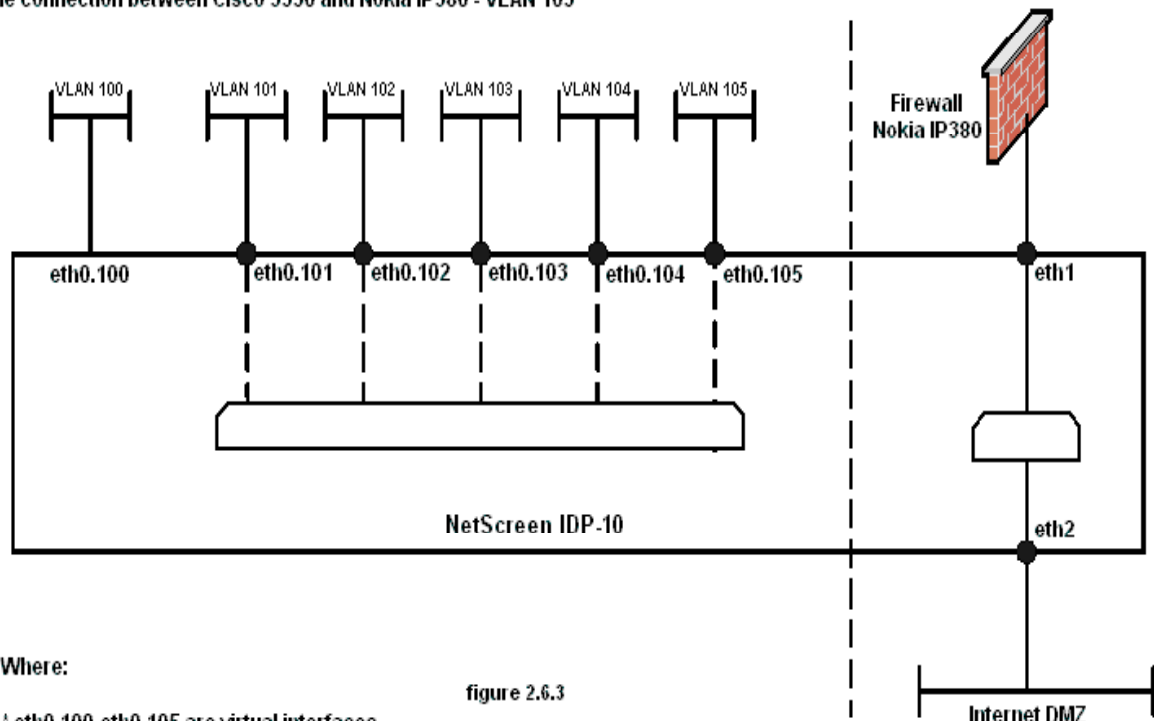
2.6.1.c Intrusion Detection and Prevention

As mentioned in the previous section, IDP products are mandatory on the GIAC network. Its role is to detect and prevent malicious attacks to/within GIAC network segments. A Juniper product NetScreen-IDP 10 was chosen (www.juniper.net/products/intrusion/dsheet/110010.pdf) because it is reliable, widely used and the available support. It has three physical network interfaces and combines multiple detection mechanisms in a single product. The detection methods are:

Mechanism	Description
Stateful Signatures	Detect known attack patterns only in relevant traffic.
Protocol Anomaly	Detect unknown or permuted attacks.
Backdoor Detection	Detect unauthorized interactive backdoor traffic.
Traffic Anomaly	Detect attacks spanning multiple sessions and connections.
Network Honeypot	Detect attackers that are impersonating network resources and tracking attacks against them.
Layer-2 Detection	Detect layer-2 (ARP) attacks.
DOS Detection	Detect certain Denial of Service attacks.
Spoofing Detection	Detect IP spoofing attacks.
Compound Signatures	Combines stateful signatures and protocol anomalies to detect complex attacks in a single session.

More over, this product can perform firewall functions (traffic filtering), therefore it can also restrict traffic between the GIAC Main network internal segments. This was another pro on choosing this product since the Cisco 3550 has quite limited traffic filtering capabilities. A logical diagram of how this product is connected in order to analyze the traffic that crosses the GIAC network is shown in figure 2.6.3.

IDP management LAN - VLAN 100
 Management LAN - VLAN 101
 Workstations LAN - VLAN 102
 Protected LAN - VLAN 103
 Intranet DMZ - VLAN 104
 The connection between Cisco 3550 and Nokia IP380 - VLAN 105



Where:

- ^a eth0.100-eth0.105 are virtual interfaces
- ^a eth1 and eth2 are physical interfaces

figure 2.6.3

One of the biggest weakness of any IPD product, therefore also NetScreen - IDP10, is the false positive reading for normal activities. This weakness can mitigate by properly tuning the IDP product. The NetScreen -IDP10 can be a bottleneck for the network traffic since it has a maximum throughput of 20MB/sec. It is recommended to use NetScreen-IDP100 (maximum throughput 200MB/sec), but its price is too high for the budget offered by the GIAC management board to build the GIAC network.

2.6.1.d Internet DMZ

The Internet DMZ (on the GIAC Main network) houses all the servers that provide services over the Internet or access the Internet directly. In order to separate the external traffic from internal traffic this segment (only in Main network) is connected to the Primary firewall via a Back-end LAN. This provides an extra layer of security for the GIAC network since the internal traffic is very well separated from external traffic - the servers located in this segment access the Internet via routable IP space (see the IP addressing scheme outlined in figure 2.6.1) and the internal servers (located on the Intranet DMZ) or internal users (Workstations LAN) access them via the Back-end LAN with non-routable IP addresses (RFC 1918). The Internet DMZ houses the following servers:

- **External DNS Server (Main Network)** –It provides DNS lookup

service for all the servers in the Internet DMZ and is also configured to allow recursive queries for Internal DNS only. It is running BIND version 9.3.0 in chrooted environment and Fedora Core 2 Linux as underlying operating system. Both BIND and Fedora Core 2 Linux were hardened with the latest security patches. BIND was chosen because of its wide spread use. Split DNS is implemented on GIAC network due to the following reasons:

- To limit information regarding GIAC network's internal infrastructure to external users.
- To decrease the probability that critical internal resources will be affected by a compromised DNS server. It is very well known that many security vulnerabilities (hacker's favorite attack – buffer overflow) have been found in DNS software over the past few years.

This server is not allowed to make DNS connections (zone transfer -TCP port 53) with the Internal DNS server. To add an extra security measure (not to allow DNS request coming all over the Internet), arrangements were made with the ISP to allow the ISP DNS server to slave GIAC public zone. Therefore, the GIAC Primary firewall allows zone transfer only between the ISP DNS server and the GIAC External DNS.

- **External NTP server** - The system clock of the servers within the GIAC network must be synchronized through NTP server in order to provide an effective log analysis. It has Fedora Core 2 Linux as operating system with NTP server running. Both the OS (operating system) and NTP were hardened with latest security patches. A Red Hat OS was chosen because stability and cost were the main concerns. The GIAC Main network Primary firewall enforces the following:
 - Allow the servers housed on the Internet DMZ to connect to the External NTP server via UDP port 123.
 - Allow the Internal NTP server (located on the Intranet DMZ) to connect to the External NTP server via UDP port 123.
 - Not allow the External NTP server to connect to any server located on the GIAC internal segments.
- **Web Server** – It hosts static informational web pages of GIAC for the general public. It can be accessed from the Internet via HTTP port 80. It is not allowed to initiate connections with any server within the GIAC network. Stability and cost were the main requirements on choosing this server. Therefore, Apache 2.0.52 Web server (www.apache.org) and Fedora Core 2 Linux as underlying OS were chosen.
- **Mail Relay** - It forwards the inbound messages to the internal email server (located on Intranet DMZ). It is also configure to relay outbound SMTP traffic that is received only from internal email server. Splitting the mail server into two components reduce the risk that an attacker might get access to the GIAC sensitive information. The Mail Relay is running Postfix 2.1.5 (www.postfix.org) in a chrooted environment with

SpamAssassin to prevent unsolicited commercial emails (UCE) on hardened Fedora Core 2 Linux box. Postfix is also configured to use RBLs (real-time blacklists) as a measure against UCE. Postfix was chosen because it is a free product and is designed with security in mind. Due to licensing cost a virus scanning solution was not implemented on this server; instead it was implemented on the Email server.

- **Uploading Portal** – It was discussed in section 2.31. It is running Apache 2.0.52 Web server on a hardened Fedora Core 2 Linux box. Those were chosen because stability and cost were the main concerns. The Suppliers can access this server only via https (TCP 443). An agreement was made with each supplier to provide a list of routable IP addresses from which they will connect to Uploading Portal. The GIAC Primary firewall allows HTTPS connection originated only from those IP addresses to the Uploading Portal. This is an extra security measure to protect the Uploading Portal.
- **Proxy Server**– Its role is to secure GIAC employees' access to the Internet. It is running open-source Squid 2.5 (www.squid-cache.org) on hardened Fedora Core 2 Linux. This setup was chosen in order to keep the cost down. Squid is configured to support HTTP, HTTPS and FTP connections. To add extra security measures, Squid is configured to run on TCP port 6120 (instead of the default TCP port 3128) and is used to provide content filtering (using SquidGuard). Plus, Squid is configured to cache frequently accessed pages for bandwidth saving.
- **Web Cache Server (Satellite Networks)** - To keep the cost down, this server is running open-source Squid 2.5 on a hardened Fedora Core 2 Linux box. It is allowed to connect only to the Proxy Server (located on the GIAC Main Network) in order to fulfill the HTTP, HTTPS and FTP requests coming from the Satellite Network internal users. This is a security measure since no IDP product is installed on the Satellite Networks (due to cost reasons). Therefore, the Satellite Network internal users can be exposed to malicious attacks if Squid has direct access to the Internet. Plus, if one of the Satellite Networks is compromised then the Main Network can be compromised as well since the Satellite Networks's internal users have access to internal information located on the Main Network. Squid is configured to cache frequently accessed pages for bandwidth saving and to perform content filtering. Also, the Web Cache server gets DNS information from the External DNS server located on the Main Network and offers internal DNS information to the internal workstations hosted on the Satellite Networks. Plus, it gets synchronized from the External NTP server located on the Main Network and is configured as Internal NTP server for internal workstation located on the Satellite Networks. All the connections mentioned above (HTTP, HTTPS, FTP, DNS and NTP) are made over VPN site-to-site connection (see section 2.6.1.b).

2.6.1.e Intranet DMZ

The Intranet DMZ segment contains servers that offer service only to GIAC internal employees. It is protected by 2 layers of firewall and by NetScreen-IDP10 (see section 2.6.1.c). All the servers within the Intranet DMZ segment are hardened according to best practice. The Intranet DMZ segment houses the following servers:

- **Internal Web Server** – It hosts static or dynamic html pages of the GIAC only for its internal employees. The GIAC internal employees can access this server via HTTP, HTTPS and FTP. Therefore, the GIAC secondary firewall (Cisco 3550 EMI) allows only HTTP, HTTPS and FTP to this server. To keep the cost down, this server is running Apache 2.0.52 Web server on a hardened Fedora Core 2 Linux box.
- **Email Server** – The Email server is running Microsoft Exchange 2003 on a hardened Windows 2000 SP4 box. This solution was chosen because Microsoft Exchange is widely used and the facilities included with it (calendar, etc). The GIAC Main network internal employees access their email through MAPI applications. The GIAC remote users (sales force, internal users from the Satellite Networks) access their email via VPN connection to the GIAC Main Network firewall and then they connect to the Exchange server using the following protocols:
 - SMTP (TCP port 25) for sending email
 - POP3 (TCP port 110) for receiving emailEmail access by MAPI clients for remote users was considered unsuitable since several security vulnerabilities associated with Windows RPC services (TCP port 135) were found in the past years. The Exchange server forwards all the email to the Mail Relay (located on the Internet DMZ segment) and receives all incoming email from the latter. In order to protect email from viruses, the Exchange Server is installed with Symantec Mail Security for Microsoft Exchange 4.0.
- **Internal DNS/NTP Server** – It offers DNS and NTP services only for the GIAC Main network internal users. Since stability and cost were the main concerns, the Internal DNS/NTP server is running open-source BIND 9.3.0 in a chrooted environment (for DNS) and NTP server on a hardened Fedora Core2 Linux box. The Internal NTP server is synchronized from the External NTP server (located on the Internet DMZ). To add an extra layer of security, zone transfer is disabled on the Internal DNS server. The Internal DNS is allowed to make DNS requests (UDP port 53) to the External DNS server and not vice-versa.
- **Windows Domain Controller/Update Server (GIAC Main Network)** – It is hardened Windows 2000 SP4 server. The workstations located on the Workstation LAN are configured to connect to the Update Server

for the latest software updates. The Update server is also running McAfee Virus Scan Enterprises 8.1 for workstation and network servers. This Update server is configured to connect to Squid (installed on the External Proxy) and get the latest anti-virus signatures (via HTTP) from the McAfee site. The internal workstations within the GIAC network are configured to download the latest driver from this server (via HTTP). This setup brings a lot of saving of the bandwidth as otherwise multiple downloads of the same anti-virus signatures by various boxes within GIAC would have been made.

- **Windows Domain Controller/Update/Back-up server (Satellite Networks)** – It is a hardened Windows 2000 SP4 Server. It performs the same tasks like the Windows Domain Controller/Update server located on the GIAC Main Network and is also a back-up box for the systems within the Satellite Networks.

2.6.1.f Protected LAN

The Protected LAN is the segment where all the GIAC most sensitive information (fortune cookie and administration databases) is hosted. Taking in consideration how critical this segment is for the GIAC business, 2 firewalls (with firewall policies based on the least privileges) and NetScreen-IDP10 protect this segment. It contains the following servers:

- **Application Server (AS)** – Since stability, security, support and cost were the main concerns; this server is running open-source application server JBoss (with Apache 2.0.52 Web server) on a hardened Fedora Core 2 Linux box. The Application server's Web server is running on port 443. All the GIAC employees access the application server using their internal user name and one time securID password via HTTPS. In turn, the application servers check the user name and password with the Radius server (located on the Management LAN). All the GIAC employees are divided in groups (on Radius Server) and based on those groups they can access a particular application within the application server (e.g.: financial group is allowed to access the financial application but not the fortune database, the HRM group is allowed to access only personnel application – employee personal file, etc). After the Radius server successfully authenticates a user, it returns to the application server the group to which that user belongs and the application server based on the received group name grant access to a particular application. This mechanism is accomplished via an application running on the application server communicating on TCP port 4321.
- **Databases (Administration and Fortune)** – The installation of the Administration Database on a separated box was necessary since the Administration Database houses very sensitive information (employees personal files, business contacts with customers, financial information) regarding GIAC business and is accessed only by special

group of GIAC employees. Additionally, if both databases were installed on the same box it could badly damage the GIAC business if that box would be compromised. The Fortune database houses the fortune cookies gathered from suppliers. Both servers are running open-source database MySQL 4.1 on harden Fedora Core 2 Linux box. MySQL was chosen because robustness and cost were the main concerns. Additionally, MySQL has received several awards in past few years (www.mysql.com/news-and-events/awards/). On the Fortune Database box runs a script as cron job that connects every hour to the Uploading Server to fetch the fortune text files (uploaded there by the suppliers) via SSH and inserts them into database. This is an extra security measure to protect the Fortune Database – if the Uploading server is hacked then the attacker will have lots of difficulties to hack the Fortune Database since no traffic originated from Uploading Server to the Fortune Database is allowed. The script that runs as cron job does also syntax checking of the Fortunes text file (if the it is text file and not binary, if it has the required fields – author, supplier, date, title, fortune itself). The application server connects to the databases via TCP port 3306. All traffic between application server and databases is restricted to this segment. Additionally, both databases are archived on daily basis on CD (both servers- Administration and Fortunes Database- have a CD-Writer).

2.6.1.g Management LAN

The management LAN provides a central point from which the GIAC server and network devices can be managed monitored and critical events analyzed. It is protected by 2 firewalls and NetScreen-IDP10 against malicious attacks. It contains the following servers:

- **IDP management console** – It is the central point from which NetScreen-IDP 10 is managed (policy creations/ installations, log viewing for NetScreen-IDP 10). It is a hardened Red Hat 8.0 Linux box. A Red Hat 8.0 box was chosen due to cost and operating system support.
- **Back-up/Syslog/Management console** - To keep the cost down and to standardize the operating system for easy support and management, a hardened Fedora Core 2 Linux running Syslog daemon was chosen. All Linux servers and network devices within the GIAC networks are configured to log critical events to this server. Therefore, the critical events can be viewed and analyzed by the Sysadmin personnel. Plus, in the event that a Linux server within the GIAC network was compromised and the attacker covered his tracks by modifying the local copy of the log on that box, evidence of the attack would still be retained on this server. It has 2 CD-Writers in order to back-up the daily logs that are the gathered from the GIAC Linux server or network devices.

- **Radius Server** – As positive user identification, protection of GIAC's valuable corporate information (administration information and fortunes cookie saying) and an authentication solution that is strategic is needed, a RSA ACE/Server 4.2 (www.rsasecurity.com) running on a hardened Windows 2000 SP4 box were chosen. This type of strong authentication is designed to mitigate the risk of sniffing and brute force attacks on simple password based authentication mechanisms. It also provides a central point of user administration. Therefore, it offers scalability to GIAC network and an easy and flexible way to manage GIAC internal users. Although, the cost for such product is quite high, the GIAC board management understood the security issues of deploying such product and approved the expenses for it. The requests (from the Application Server or the Main network Primary firewall) are received via UDP port 1645.

2.6.1.h Workstations LAN

It represents the system on which GIAC employees work. In order to standardize the operating system for ease of support and management it has been decided that the only operating system allowed to be installed on the workstations within GIAC network are: Windows 2000 SP4 and Fedora Core 2 Linux. All the operating systems (Windows and Fedora) are hardened according to the best practices. To protect them against viruses, all the windows desktops are installed with McAfee anti-virus that gets anti-virus signature updates from the Update server (located on the Intranet DMZ) via HTTP.

3. Assignment 3 – Router and Firewall Policies

3.1 Introduction

This section will focus on the implementation of router policy on the Main network border router (Cisco 2621XM) and the firewall policy on the GIAC Primary firewalls Nokia IP380 CheckPoint NG AI -VPN-1/Firewall-1- (Main network and Satellite networks).

The separation of the Border Router from the Main network Primary Firewall (Nokia IP380) permits both devices to act in conjunctions in order to offer a more complete line of defense between Internet and GIAC Main network.

The Border Router is the first line of defense - it allows traffic from Internet that is needed by GIAC business and limit access from within the GIAC Main Network to only those protocols required by GIAC business. The Primary Firewall provides a secondary line of defense for the GIAC Main network by performing stateful inspection of packets that are allowed by the Border Router. While the Border Router blocks packets by examining the source, destination and ports of the packets, the Primary Firewall examines the session state of the packet passing into GIAC Main network, and blocks unauthorized connections initiated from Internet.

3.2 Border Router Policy

Some important issues to note are outlined below:

- Packets are compared with ACLs from the top/first rule down. The first rule that match is applied to the packet. Therefore, the order of the rules is very important.
- The most frequently applied rules should be placed near the top of the list to reduce processing overhead.

3.2.a Ingress ACL

This is an ACL that filters inbound traffic from the Internet. This ACL is applied to FastEthernet 0. The ingress ACL of the Border Router is summarized in the following table:

Source	Destination	Protocol/Port	Action	Comment
127.0.0.0/0.255.255.255	any	any	deny	Drops traffic with loopback source address
10.0.0.0/0.255.255.255 172.16.0.0/0.15.255.255 192.168.0.0/0.0.255.255	any	any	deny	Drops traffic with non-routable source address (RFC 2827).
X.Y.Z.0/28	any	any	deny	Blocks traffic with spoofed GIAC public network addresses
224.0.0.0/31.255.255.255	any	any	deny	Blocks traffic with multicast address as source address
Unassigned IPv4 address space	any	any	deny	Blocks traffic with source addresses that are in the unassigned IPv4 address space <i>Ref [3.1]</i> . Since this list of IP addresses is continuously changing, the Sysadmin personnel are manually updating this list on the router.
any	any	ICMP (host redirect and echo)	deny	Block reconnaissance attacks.
any	X.Y.Z.0/28	any	permit	Business requirements.
any	any	any	deny	Blocks anything else.

3.2.b Egress ACL

This is an ACL that filters outbound traffic. The main purpose of this ACL is to ensure the GIAC Main network is not sending any spoofed packets. If any packet leaving the GIAC Main network has a source address that does not belong to the GIAC Main network, it was most likely spoofed. The Egress ACL is applied to FastEthernet 1. The egress ACL is summarized in the following table:

Source	Destination	Protocol/Port	Action	Comment
any	any	TCP 135, 139 (NETBIOS) UDP 135,139 (NETBIOS) TCP 445 (microsoft-ds) TCP 69 (TFTP) UDP 514 (SYSLOG) TCP 6000-6063 (X11)	deny	Blocks the dangerous traffic that could potentially leak information regarding GIAC's internal network.
any	any	ICMP (echo reply)	deny	Blocks incoming ICMP host-redirect and echo messages. This will prevent attackers to use ICMP messages to map GIAC network and disrupt network traffic
Primary Firewall Internet DMZ Sysadmin staff Management Server	any	any	permit	Business requirements
-	-	-	deny	This rule prevents the GIAC network from being involved in DDOS attacks against other organizations. Traffic that originates from the GIAC internal network but whose source is not one of the GIAC public addresses probably is spoofed. To identify the hosts that spoofed their source address, the log-input parameter is used to log the MAC address of these hosts.

any	any	any	deny	Deny anything else
-----	-----	-----	------	--------------------

3.3 Firewall Policy

Before providing the firewall policy, some important points to note are:

- Packets are compared with firewall policy from the top/first rule down. The first rule that match is applied to the packet. Therefore, the ordering of the rules is extremely important.
- The security policy for these firewalls is configured from the CheckPoint Policy Editor GUI client that connects to the Management Server (installed on Nokia IP380). The Management Server allows connections only from the IP addresses (2 addresses – see section 2.2.g) that belong to Sysadmin personnel.
- VPN-1/Firewall-1 is a stateful packet filtering firewall *Ref [3.2]*.
- All the connections to firewall (either they are accepted, encrypted or rejected) are logged. Why also rejected logs? Because a potential attack can be anticipated from rejected logs.
- All the rules that have “encrypt” on Action column are established over VPN
- To minimize processing overhead, the rules with the most common packets matches should be as close to the top of the firewall policy as possible

The first rules in the security policy are the implicit rules. Implicit rules are defined by VPN-1/Firewall-1 to allow certain connections to and from the firewall with a variety of different services. The implicit rules are configured using the Global Properties screen. There two types of implicit rules:



































- VPN-1/Firewall-1 Control Connections - This rule allows traffic such as: management (communication between GUI clients and enforcement module –firewall), logging of the enforcement module, key exchange, IKE and RDP (communication and encryption purposes) and communication with the RADIUS server.
- Outgoing Packets – This rule accepts outgoing packets originating from the firewall. It is useful for updates needed by Nokia IPSO. It is inserted in the firewall policy as before the last rule. The following options included in the Global Properties are disable since they are not required by GIAC infrastructure and may lead to less secure network: “Accept RIP”, “Accept Domain Name over UDP (Queries)”, “Accept Domain Nam over TCP (Zone Transfer)”, “Accept ICMP request”, “Accept CPRID connections (SmartUpdate)” – it is more secure to manually update the firewall, “Accept dynamic address Modules’ DHCP traffic”.

The GIAC Primary Firewalls are the following:
























- gw-be.giac.com – Brussels
- gw-fr.giac.com – Paris
- gw-nl1.giac.com – Amsterdam
- gw-nl2.giac.com – Utrecht
- gw-it.giac.com – Milan

3.3.a Firewall Policy (Main network Primary Firewall)







































The security policy that is installed on Main network Primary Firewall (including comments for each rule) is summarized in the following table

No. Rule	Source	Destination	Service	Action	Comment
1	 sysadmin	 gw-be.giac.com	TCP ssh ?? icmp-proto TCP ident	 accept	Allow Sysadmin personnel to connect via SSH to the firewall and to perform ping (troubleshooting purposes) to firewall. Where sysadmin group has the IP addresses: 10.103.5.29 10.103.5.30
2.	 gw-be.giac.com  gw-fr.giac.com	 gw-fr.giac.com  gw-be.giac.com	UDP IKE  IPSE C	 accept	IPSEC Site-to Site VPN with Primary Firewall Paris. Where IPSEC group has the protocols: ?? AH ?? ESP ?? SKIP
3.	 gw-be.giac.com  gw-nl1.giac.com	 gw-nl1.giac.com  gw-be.giac.com	UDP IKE  IPSE C	 accept	IPSEC Site-to-Site VPN with Primary Firewall Amsterdam
4.	 gw-be.giac.com  gw-nl2.giac.com	 gw-nl2.giac.com  gw-be.giac.com	UDP IKE  IPSE C	 accept	IPSEC Site-to- Site VPN with Primary Firewall Utrecht.
5.	 gw-be.giac.com  gw-it.giac.com	 gw-it.giac.com  gw-be.giac.com	UDP IKE  IPSE C	 accept	IPSEC Site-to- Site VPN with Primary Firewall Milan.
6.	* Any	 gw-be.giac.com	* Any	 drop	Stealth Rule
7.	* Any	 X.Y.Z.7 (web_server_ext)	TCP http	 accept	Allow HTTP traffic originated from Internet to External Web server (its routable IP address). Reason – section 2.6.1.e External Web server.
8.	 X.Y.Z.6 (proxy_ext)	 internal_NET	TCP http TCP https TCP ftp	 accept	Allows HTTP, FTP, and HTTPS traffic originated from proxy server (its routable IP address) to Internet. Reason-section 2.6.1.e – Proxy Server. Where the (not) internal_NET are the GIAC internal network segments.

GIAC Certified Firewall Analyst (GCFW) Practical v4.1

9.	 10.103.5.0/24 (Workstation LAN –Brussels)  10.100.2.5 (Update server)	 10.12.8.4 (proxy_int)	TCP squid	 accept	<p>Allow Squid (TCP port 6120) traffic originated from internal users (Workstation LAN) to the proxy server (its back-end IP address). Reason – see section 2.6.1.d -Proxy Server.</p> <p>It also allows Squid traffic originated from Update server (need for the virus signatures updates) to the proxy server Reason – see section 2.6.1.e – Windows Domain Controller/Update Server</p>
10.	 Suppliers_IP	 X.Y.Z.9 (uploading_portal)	TCP https	 accept	<p>Allow HTTPS (TCP port 443) traffic originated from Suppliers IP addresses to Uploading Portal (its routable IP address). Reason- see section 2.6.1.d - Uploading portal</p>
12.	 10.101.3.120 (Fortune Database)	 10.12.8.7 (uploading_portal)	TCP SSH	 accept	<p>Allow the SSH (TCP port 22) traffic originated from Fortune Database to Uploading Server. Reason: section 2.6.1.f –Databases</p>
13.	* Any	 X.Y.Z.8 (mail_relay_ext)	TCP smtp	 accept	<p>Allow inbound mail traffic from Internet to mail relay (its routable IP address) via TCP port 25. Reason – section 2.6.1.e Mail Relay</p>
14	 10.100.2.3 (email server)  10.12.8.6 (mail_relay_int)	 10.12.8.6 (mail_relay_int)  10.100.2.3 (email server)	TCP smtp	 accept	<p>Allow email server to forward outbound mail to the Mail relay server (its non-routable IP address). It also allows the Mail relay server to forward inbound mail to email server via SMTP (TCP port 25). Reason- sections 2.6.1.e – Mail relay, 2.6.1.f – Email Server</p>
15	 Web Cache (Satellite Networks)	 10.12.8.4 (proxy_int)	TCP squid	 encrypt	<p>Allows Squid (TCP port 6120) traffic originated from Web Cache group (includes all the Web Cache for each Satellite Network) to External Proxy Server (its non-routable IP address). Reason -section 2.6.1.d - Web Cache</p>
16.	 Internal employees (Satellite Networks)	 10.101.3.100 (application server)	TCP https	 encrypt	<p>Allow internal users from the Satellite Networks to connect to the Application Server via https. Reason- sections 2.6.1.f - Application Server</p>

GIAC Certified Firewall Analyst (GCFW) Practical v4.1

17.	 Internal employees (Satellite Networks)	 10.100.2.3 (email server)	 smtp  pop3	 encrypt	Allows internal users from internal from Satellite Networks to access their emails. Reason- section 2.6.1.e - Email Server.
18.	 Web Cache (Satellite Networks)	 10.12.8.2 (dns_ext_int)	 domain-udp	 encrypt	Allows DNS requests (UDP port 53) originated from Web Cache group to External DNS server (its non-routable IP address). Reason – section 2.6.1.d - Web Cache
19.	 Web Cache (Satellite Networks)	 10.102.4.10 (Syslog server)	 syslog	 encrypt	Allows critical logs from the Web Cache group to be logged on the Syslog Server.
20	 Web Cache (Satellite Networks)	 10.12.8.3 (ntp_ext_int)	 ntp-udp	 encrypt	Allows NTP requests (UDP port 123) originated from Web Cache group to External DNS server (its non-routable IP address). Reason – section 2.6.1.d - Web Cache
21	 sysadmin	 gw-fr.giac.com  gw-it.giac.com  gw-nl1.giac.com  gw-nl2.giac.com  Web Cache (Satellite Networks)	 SSH	 encrypt	Allow Sysadmin personnel to connect via SSH to the Primary Firewalls and Web Cache located in Satellite Networks. Reason – see section 2. 2.i
22.	 All Users@Any	 10.101.3.100 (application server)	 https	 clientencrypted	Allows sales force to connect application server in order to download the fortunes database for the suppliers.
23	 All Users@Any	 10.100.2.3 (email server)	 smtp  pop3	 clientencrypted	Allows sales forces to access their email. Reason- section 2.6.1.e –Email Server.
24.	 DNS_Server_ISP	 X.Y.Z.4 (dns_ext_ext)	 dns	 accept	Allow DNS traffic (zone transfer -TCP port 53 and DNS requests – UDP port 53) originated from to DNS Server of the ISP to the External DNS Reason (its routable IP address) – see section 2.6.1.e – External DNS server.

GIAC Certified Firewall Analyst (GCFW) Practical v4.1


























25.	10.100.2.4 (dns_internal)	10.12.8.2 (dns_ext_int)	UDP domain	accept	Allow DNS requests traffic originated from Internal DNS server to External DNS server (its back-end IP address). Reason – see section 2.6.1.f Internal DNS Server
26.	X.Y.Z.5 (ntp_ext_ext)	NTP_server_ISP	UDP ntp	accept	Allow NTP traffic (UDP port 123) originated from External NTP server (its routable IP address) to ISP NTP server. Reason – see section 2.6.1.e External NTP server
27	10.100.2.4 (ntp_internal)	10.12.8.3 (ntp_ext_int)	UDP ntp	accept	Allow NTP traffic originated from Internal NTP server to External NTP server (its back-end IP address). Reason – see section 2.6.1.f Internal NTP server.
28	10.12.8.0/24	10.102.4.10 (syslog_server)	UDP syslog	accept	Allow critical logs from Internet DMZ (via back-end LAN) to be logged on the central syslog server via syslog (UDP port 514). Reason – see section 2.6.1 – Back-up/Syslog.
29	Sysadmin	10.12.8.0/24	TCP ssh	accept	Allow Sysadmin personnel to connect to Internet DMZ (via Back-end LAN) via SSH. Reason- section 2.2.i
30	10.102.4.10 (Management S.)	X.Y.Z.1 (border router)	UDP snmp UDP snmp-trap TCP ssh	accept	Allow remote management of the Border Router. Reason- section 2.6.1.g – Back-up/Syslog/Management Server
31	Any	Any	Any	drop	Cleanup Rule

3.3.b Firewall Policy (Satellite Networks Primary Firewall)











All the Primary Firewall located on the Satellite Networks (Paris, Amsterdam, Utrecht and Paris) enforce the same following policy:

No. Rule	Source	Destination	Service	Action	Comment
1	Primary Firewall (Satellite Network) gw-be.giac.com	gw-be.giac.com Primary Firewall (Satellite Network)	UDP IKE IPSEC C	accept	IPSEC Site-to Site VPN with Primary Firewall Brussels (Main Network)

GIAC Certified Firewall Analyst (GCFW) Practical v4.1

2.	 Sysadmin	 Primary Firewall (Satellite Network)	<u>TCP</u> SSH	 encrypt	Allow Sysadmin group SSH access to Satellite Networks Primary Firewall for management purposes.
3	 Any	Primary Firewall (Satellite Network)	 Any	 drop	Stealth Rule
4.	 Web Cache	 10.12.8.4 (proxy_int)	<u>TCP</u> squid	 encrypt	Allows Squid (TCP port 6120) traffic originated from Web Cache to the Main network External Proxy Server (its non-routable IP address). Reason -section 2.6.1.d - Web Cache
5.	 Internal employees (Satellite Networks)	 10.101.3.100 (application server)	<u>TCP</u> https	 encrypt	Allow internal users from the Satellite Networks to connect to the Main network Application Server via https. Reason- sections 2.6.1.f - Application Server
6.	 Internal employees (Satellite Networks)	 10.100.2.3 (email server)	<u>TCP</u> smtp <u>TCP</u> pop3	 encrypt	Allows internal users from internal from Satellite Networks to access their emails. Reason- section 2.6.1.e - Email Server.
7.	 Workstation LAN (Satellite network)  Update Server (Satellite network)	 Web Cache (Satellite network)	<u>TCP</u> http <u>TCP</u> https <u>TCP</u> ftp <u>UDP</u> domain <u>UDP</u> ntp <u>TCP</u> squid	 accept	Allow HTTP, HTTPS, FTP, NTP, DNS (UDP only) and squid requests originated from Satellite network internal users to Web Cache. Reason: section 2.6.1.d Web Cache.
8.	 Web Cache	 10.12.8.2 (dns_ext_int)	<u>UDP</u> domain	 encrypt	Allows DNS requests (UDP port 53) originated from Web Cache to Main Network External DNS server (its non-routable IP address). Reason – section 2.6.1.d - Web Cache
9.	 Web Cache	 10.102.4.10 (Syslog server)	<u>UDP</u> syslog	 encrypt	Allows critical logs from the Web Cache group to be logged on the Syslog Server.

GIAC Certified Firewall Analyst (GCFW) Practical v4.1

10.	 Web Cache	 10.12.8.3 (ntp_ext_int)	<u>UDP</u> ntp	 encrypt	Allows NTP requests (UDP port 123) originated from Web Cache to External DNS server (its non-routable IP address). Reason – section 2.6.1.d - Web Cache
11.	 Sysadmin	 Web Cache	<u>TCP</u> ssh	 encrypt	Allows Sysadmin group to connect via SSH to Web Cache for management purposes.
12.	 Any	 Any	 Any	 drop	Cleanup Rule

© SANS Institute 2005, Author retains full rights.

4. References

4.1 Assignment 1

Ref [1.1]: Lance Spitzner, “Honeypots - Definitions and Value of Honeypots”, December 2002,

http://www.secinf.net/honeypots/Honeypots_Definitions_and_Value_of_Honeypots.html

Ref [1.2]: Brian Scottberg, William Yurcik, and David Doss, “Internet Honeypots: Protection or Entrapment?”, June 2002,

<http://www.sosresearch.org/publications/ISTAS02honeypots.PDF>

Further readings:

- Kellep A. Charles, “Decoy Systems: A New Player in Network Security and Computer Incident Response”,
http://www.ijde.org/docs/04_winter_v2i3_art3.pdf, Winter 2004
- Alberto Gonzalez and Jason Larson, “Fun Things To Do With Your Honeypot”, <http://www.linuxsecurity.com/content/view/117375/49/>, July 2003
- Lance Spitzner, “Honeytokens: The Other Honeypot”,
<http://www.securityfocus.com/infocus/1713>, July 2003
- Honeyd – <http://www.honeyd.org/>
- Honeyd for Windows -
<http://www.securityprofiling.com/honeyd/honeyd.shtml>
- Laurent Oudot, “Fighting Internet Worms with Honeypots”,
<http://www.securityfocus.com/infocus/1740>, October 2003
- Ryan C. Barnett, “Open Proxy Honeypots”,
http://honeypots.sourceforge.net/open_proxy_honeypots.pdf, Mart 2004
- Laurent Oudot, “Wi-Fi Honeypots a New Hacker Trap”,
<http://www.securityfocus.com/news/552>, February 2004
- Lance Spitzner, “Dynamic Honeypots”,
<http://www.securityfocus.com/infocus/1731>, September 2003

4.2 Assignment 2

Ref [2.1]: SANS 2.4: Firewalls, Perimeter Protection & Virtual Private Networks – *Defense In-Depth*

Ref [2.2]: <http://www.linux-sec.net/Harden/howto.qwif.html>, December 2004

Ref [2.3]: Cisco Systems, Inc., “Improving Security on Cisco Routers”
<http://www.cisco.com/warp/public/707/21.html>

Ref [2.4]: Nokia,
http://www.nokia.com/BaseProject/Sites/NOKIA_MAIN_18022/CDA/Categories/Business/LargeBusiness/NetworkSecurity/IPSecurityPlatforms/Enterprise_s&ServiceProviders/Content/StaticFiles/sec_nokia_ip380_datasheetna.pdf.

Ref [2.5]: Cisco Systems, Inc.,
<http://www.cisco.com/en/US/products/hw/switches/ps646/ps3813/>, October 2004

Ref [2.6]: SANS - Stephen Nothcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick and Ronald W. Ritchey, *"Inside Network Perimeter Security"* – chapter *Virtual Private Networks*, New Riders Publishing, 2003

4.3 Assignment 3

Ref [3.1]: Mark Mentovai, *"IPv4 Address Space Allocation"*,
<http://www.mentovai.com/network/ipv4-allocation.html> , July 2004

Ref [3.2]: Internet Security Systems,
http://www.iss.net/security_center/advice/Countermeasures/Firewalls/Stateful_Packet_Filter/default.htm

© SANS Institute 2005, Author retains full rights.