Global Information Assurance Certification Paper

GCFW Practical

Bassam Sakkour

GCFW Practical

Version 4.1

Feb. 22, 2005

Date: Feb. 22, 05

Table of Contents

Preface 3
Assignment 1: Network Intrusion Prevention System 3
Abstract 3
Background / Introduction 4
Problem Domain 4
Intrusion Prevention System 6
Requirements for effective prevention 7
Enhancement Features through IPS 8
Application Protection 8
Infrastructure Protection 8
Performance Protection 9
Commercial Intrusion Prevention Systems 9
Prototypical Network IPS deployment 9
Conclusion 10
Assignment 2: Security Architecture 11
Introduction 11
Access Requirements 11
Customers 11
Suppliers 12
Partners 12
Employees 12
Sales/Teleworkers 13
General Public 13
Data Flows 13
Architecture Components 14
Filtering Router(s) 15
Firewall(s) 15
VPN(s) 16
Network based IDS sensor(s) 17
Additional Components 17
Network Diagram 19
IP addressing scheme 19
Implementing Defense-In-Depth 20
Assignment 3: Router and Firewall Policies 20
General Security Stance 20
Border Router(s) Security Policy 21
Configure and restrict Console, VTY and Auxiliary Port Access 21
Router Hardening by disabling unnecessary Features and Services 23
Logging Configuration 23
Access Control Lists 24
Interface Configuration. 27
Primary Firewall(s) Security Policy 28
Rulebase 29
Firewall Service Definition: 31

Firewall Object Definitions: 32
Firewall Address Translation: 32
References 33

List of Figures

Figure 1: Prototypical Network IPS deployment 10
Figure 2: GIAC Network Diagram 19

Preface

This paper is part of the requirement for obtaining GIAC Certified Firewall Analyst
(GCFW). Practical Assignment version 4.1 is used for completion of the paper. This paper will cover three major sections:

The first section assignment 1 is research and focuses on whether it is worth using an Intrusion Prevention System in the security environment.

Assignment 2 depicts the network infrastructure of the GIAC small company in the fortune cookie saying industry. It describes how to implement security equipment / servers used for the network infrastructure including the border router, perimeter firewall, intrusion detection system and where to place publicly accessible servers and the VPN concentrator. In addition, the type of network infrastructure installed should be able to support access coming from the Internet to the service network DMZ for business operations. Furthermore, home office users and remote users should be able to access the internal network as well as GIAC employees accessing the DMZ and Internet.

In conclusion, assignment 3 includes a detailed configuration of rule sets and policies for security equipment installed in the perimeter network such as Firewall and border router as discussed in Assignment 2.

Assignment 1: Network Intrusion Prevention System

Abstract

As businesses and other institutions increase their online presence and dependency on information assets, the number of computer incidents also increases. Consequently, these organizations are finally increasing their security environments. This is accomplished in three stages. First, organizations have to be proactive in developing and implementing their security plans and controls. Secondly, they must strive to ensure their plans and controls stay effective. These should be reviewed and adapted continually thus guaranteeing that sufficient security is always in place. Finally, when controls are bypassed either intentionally or unintentionally, organizations must be ready to act quickly and effectively so as to minimize the impact of the situation. The goal is to prevent an operational security problem from becoming a business problem which would in turn impact revenue.

It has become widely accepted that security technologies like perimeter firewalls and intrusion detection system (IDS) are no longer sufficient to protect networks from being compromised. Firewalls do not adequately analyze application-layer protocol data for signs of attack, and intrusion detection systems do not take any action to stop an attack that has been detected.

A new solution called an Intrusion Prevention System (IPS) has been developed to fill the void between firewalls and IDS systems and to address the growing threat of Internet malware. IPS systems are in-line networking devices designed to block all types of malicious attacks in real-time.

Background / Introduction

Connecting to the Internet provides an organization with additional access to millions of potential customers, and in turn gives customers easy access to the company. Unfortunately, numerous Websites and internal networks are hacked due to limited personnel and budget resources, or due to the lack of security expertise in implementing safeguards and counter measures throughout the organization. Failure to secure Websites and customer data puts companies at serious risk; one single attack could cost millions of dollars in potential revenue. However, this is just the beginning actual damage resulting from an attack could also cause the following problems: Inconvenience to customers, loss of customer confidence, loss of intellectual property and market advantage, liability for compromised customer data, time and money spent on repairs/recovery.

For many enterprises, information security management has reached a critical crossroads. Stable security technologies like perimeter firewalls, Intrusion Detection System (IDS) and anti-virus software are no longer sufficient protection against the growing number of today's threats and leave companies open to destructive attacks.

More recently, Denial-of-Service (DoS) attacks have become prominent and have seriously crippled major e-commerce sites. Since a DoS attack does not require a TCP connection to the target system or network, there is no connection to terminate, even if it is detected. In these cases, the only effective counter measure is to locate the source of the threat quickly so that the data stream can be terminated without disrupting legitimate business.

New network-based Intrusion Prevention Systems (IPS) complement traditional security products to provide enterprises with unparalleled protection against external and internal attacks. An exponential rise in application vulnerabilities that are easily exploited through standard ports have rendered traditional Firewalls ineffective against attacks. While Intrusion Detection Systems (IDS) can often detect these attacks, these passive systems offer little more than an after-the-fact notification. In contrast, an IPS is designed to examine all traffic that passes through so as to detect and filter out malicious packets.

Problem Domain

2003 is being dubbed the year of the worm. In Jan/03 we were hit by Slammer (MS SQL vulnerability), then in August hit by Blaster (MS RPC DCOM vulnerability) and several variants (Nachi), then came the Sobig.F virus.

Estimates of the total damage incurred vary significantly, but there is little dispute that the damage was substantial. Most recently we were hit by the mydoom virus which at its peak infected up to 1 in 7 emails [1] [2].

Traditionally, the solution has been to patch servers and workstation host-by-host, a time consuming process. For some organizations, the challenge in patching lies in testing each patch to understand how it will affect the performance of critical systems. Others find the biggest challenge in reaching each individual in a diverse user base and persuading them to install the patch. In both cases, the patching process takes time, and is itself not a perfect solution (many organizations don't have 100% control over devices that connect to their network).

Other traditional solutions are to implement technologies such as Intrusion Detection Systems (IDS) and application inspection firewalls. Unfortunately, there are problems with these traditional defenses:

Firewall
Firewalls are the first line of defense in securing a private network from unauthorized entry. They are effective access control devices that determine which packets are allowed to pass in or out of the network and which must be modified before passing. One of the ways packets are modified is by re-addressing them to mask true internal IP addresses. Firewalls can also alert the network administrator of any packets that contain a potential threat to the organization. A good firewall is hacker-resistant and is an absolute necessity for a secure network. Like a good lock on a front door, the firewall will keep most intruders out. However, it must be expected that, from time to time, a savvy intruder will make it past the first defense, for example, even the best of door locks should be supplemented with a motion detector. This would equate to an Intrusion Detection System in an organizational network infrastructure.

Intrusion Detection Systems
An IDS is a complementary solution to firewall technology. An IDS that has sensors both inside and outside the firewall can help determine whether the firewall is configured and operating properly. An IDS also detects attacks against the network that firewalls are unable to see. IDSs fall into four main categories: *Network-based, host-based, hybrid*, and *decoy-based.* Here I will only go into detail on Network-based IDS.

Network-Based IDS
A network-based IDS uses network cards in promiscuous mode to look at every packet that passes on the network. A typical network IDS consists of one or more sensors and a console to aggregate and analyze data from the sensors. Network-based IDSs can't stop attacks on their own. IDSs are out-of-band, passive devices designed to spot but not prevent attacks (seen as being more reactive than proactive). IDS systems compare traffic flow and network packets

to a set of rules and signatures then sound the alarm when something looks amiss. The problem is that IDS systems produce a lot of alerts and interpreting or taking action requires human resources – trained security administrators who are expensive to hire and may not be available in many rural areas

In addition, since IDSs are passive, even with the support of highly skilled security technicians, attacks can only be minimized but not prevented.

Enabling a successful IDS deployment requires that companies commit the human resources who are skilled in configuring, tuning and monitoring these systems. These resources will only be needed more as IDS evolves to IPS.

In addition, IT capacity can no longer keep up with handling security. It has also become clear that even perfect perimeter protection without IPS is not adequate. Walk-in worms (worms brought into the network on infected laptops) easily bypass perimeter defenses and attack from within. [4] [10] [11]

Intrusion Prevention System

Within the IPS market place, there are two main categories of product: Host IPS and Network IPS. [2] [3]

Host IPS (HIPS)

As with Host IDS systems, the Host IPS relies on agents installed directly on the system being protected. It binds closely with the operation system kernel and services, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them. One potential disadvantage with this approach is that, given the necessarily tight integration with the host operation system, future OS upgrades could cause problems.

Since the Host IPS agent intercepts all requests to the system that it protects, it has certain prerequisites – it must be very reliable, must not negatively impact performance, and must not block legitimate traffic. Any HIPS that do not meet these minimum requirements should never be installed in a host, no matter how effectively it blocks attacks.

Network IPS (NIPS)

The network IPS combines features of a standard IDS, an IPS and a firewall, and is sometimes known as an In-Line IDS. It is true that firewalls, routers, IDS devices and even AV gateways all have intrusion prevention technology included in some form. A true NIPS device, however, is sitting in-line – all the packets have to pass through it and the primary value of an IPS is that it can provide a “virtual patch” functionality that protects vulnerable systems from compromise when host-by-host patches have not been applied and the network is running

the protocol at risk. It is possible for an IPS filter, or a suite of filters, to effectively provide a barrier to all attempts to exploit a particular vulnerability. This means different attackers can come and go, the exploit codes can all be different, attackers can use their polynorphic shell code generators and other evasion techniques, and the filter will reliably block all the attacks, while allowing legitimate traffic through. A filter that operates in this manner is called a "vulnerability filter", and such filters make unpatched systems appear patched from an external attacker's point of view.

Requirements for effective prevention

IPSs must fulfill the requirements for effective prevention [2]:

- **In-line operation** – by operation in-line, an IPS device can perform true protection, discarding all suspect packets immediately and blocking the remainder of that flow.

- **Reliability and availability** – should an in-line device fail, it has the potential to close a vital network path and thus, once again, cause a DoS condition. An extremely low failure rate is thus very important in order to maximize up time, and if the worst should happen, the devices should provide the option to fail open or support fail-over to another sensor operation in a fail-over group. In addition, to reduce downtime for signature and protocol coverage updates, an IPS must support the ability to receive these updates without needing a device reboot.

- **Resilience** – as mentioned above, the very minimum that an IPS device should offer in the way of High Availability is to fail open in the case of system failure or power loss (some environments may prefer this default condition to be "fail closed" as with a typical firewall, however - the most flexible products will allow this to be user-configurable). Active-Active stateful fail-over with cooperation in-line sensors in a fail-over group will ensure that the IPS device does not become a single point of failure in a critical network deployment.

- **Low latency** – when a device is placed in-line, it is essential that its impact on overall network performance is minimal. Packets should be processed quickly enough such that the overall latency of the device is as close as possible to that offered by a layer 2/3 device such as a switch, and no more than a typical layer 4 device such as a firewall or load-balancer.

- **High performance** – packet processing rates must be at the rated speed of the device under real-life traffic conditions, and the device must meet the stated performance with all signatures enabled. Headroom should be built into the performance capabilities to enable the device to handle any

increases in size of signature packs that may occur over the next three years. Ideally, the detection engine should be designed in such a way that the number “signatures” (or “checks”) loaded does not affect the overall performance of the device.

- **Unquestionable detection accuracy** – it is imperative that the quality of the signatures is beyond question, since false positives can lead to a Denial of Service condition. The user MUST be able to trust that the IPS is blocking only the user selected malicious traffic. New signatures should be made available on a regular basis, and applying them should be quick (applied to all sensors in one operation via a central console) and seamless (no sensor reboot required).

- **Fine-grained granularity and control** – fine-grained granularity is required in terms of deciding exactly which malicious traffic is blocked. The ability to specify traffic to be blocked by attack, by policy, or right down to individual host level is vital. In addition, it may be necessary to alert only suspicious traffic for further analysis and investigation.

- **Advanced alert handling and forensic analysis capabilities** – once alerts have been raised at the sensor and passed to a central console, someone has to examine them, correlate them where necessary, investigate them, and eventually decide on action.

Enhancement Features through IPS

In order for an IPS to provide a practical virtual software patch solution, the device must perform the following protections:

Application Protection

Protect:
- Microsoft Applications & Operating Systems
- Oracle Applications
- Linux O/S
- VoIP

From:
- Worms/Walk-in Worms
- Viruses
- Trojans
- DDoS Attacks
- Internal Attacks
- Unauthorized Access

Infrastructure Protection

Protect:
- Routers (e.g. Cisco IOS)
- Switches
- Firewalls (e.g. Symantec, CheckPoint FW1)
- VoIP

From:
- Worms/ Walk-in Worms
- Viruses
- Trojans
- DDoS Attacks
- SYN Floods
- Traffic Anomalies

Performance Protection

Protect:
- Bandwidth
- Server Capacity
- Mission-Critical Traffic

From:
- Peer-to-Peer Apps
- Unauthorized Instant Messaging
- Unauthorized Applications
- DDoS Attacks

Commercial Intrusion Prevention Systems

Several commercial products of intrusion prevention system are available. Most Vendors of commercial products of intrusion prevention system have been publishing information and white papers on their websites. Here are some of the market-leading Network IPS (NIPS) products. Each NIPS product is also available in different models [2] [6]:

- **Netscreen / Juniper** (IDP 10/100/500/1000)
- **NAI / McAffee** (IntuShield 1200/2600/4000)
- **TippingPoint** (UnityOne 200/400/1200/2400)
- **ISS ISS Proventia** (G100/200/400/1000/1200)
- **Radware DefencePro**
- **TopLayer Attack Mitigator** (IPS 5000)

Prototypical Network IPS deployment

More akin to switches than sensors, IPSs are typically installed as part of the network infrastructure [6], both at the perimeter and in the core of the network. A typical IPS deployment is shown in the figure below. In this example, three IPS filter packets on one external and two internal segments. The internal segments in this example are different subnets, connected by a router. To be effective, an IPS must exhibit the same network performance characteristics of other network infrastructure products, like switches and routers, while at the same time performing stateful deep packet security processing to filter out layer 2-7 attacks.

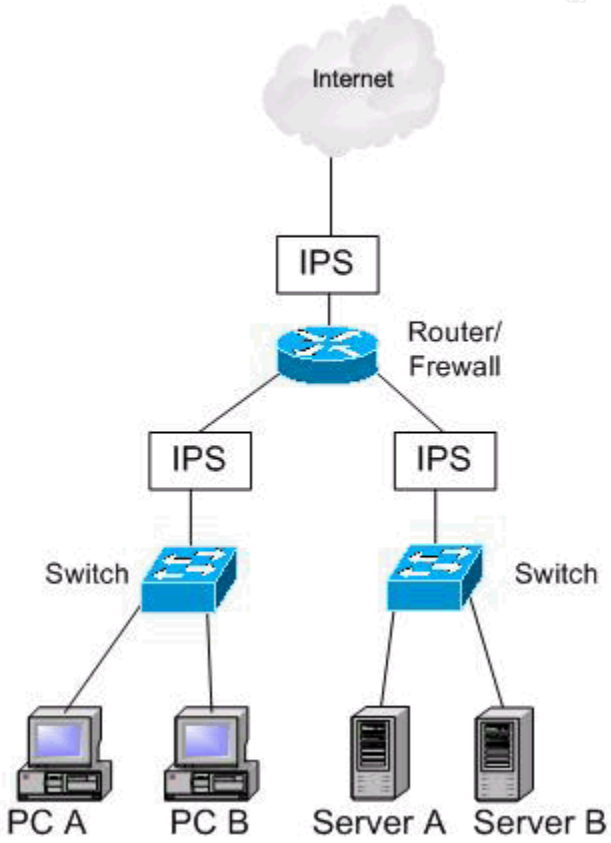

Figure 1: Prototypical Network IPS deployment

Conclusion

The best defense against intruders is a combination of tools and policies that increase the amount of information you have about an intrusion, and that provide the information quickly enough for an effective response. Therefore IPS is an important part of a defense-in-depth infrastructure with benefits that include blocking malicious attacks, improving bandwidth and lowering operating costs.

Assignment 2: Security Architecture

Introduction

GIAC Corporate is a small company engaged in the business of selling online fortune cookie sayings. It was founded at the beginning of 1990 and is located in Singapore. The GIAC Company has 60 employees stationed at the company GIAC Corporate. Some of the GIAC employees work as home office users as well as mobile sales.

GIAC Enterprises has a proven business model and has plans to expand. As a result, GIAC is starting to pick up additional business partners and customers throughout the world and will need to employ more staff due to the business goals they have set. Due to the fact that all sales transactions are conducted on the Internet, the GIAC Corporate CEO decided and agreed to invest more money on keeping network security up-to-date.

This decision made the CIO of GIAC IT Department decide to redesign the network including the perimeter infrastructure of the new GIAC Corporate in Singapore. The purpose of this redesign is to allow GIAC Corporate to do the following: perform all of today's business requirements using the GIAC network resources, provide their suppliers with the necessary access to the resources, service their customers' requests and provide home office users and mobile users with access to the new GIAC business network in Singapore. In addition, the GIAC IT has also concluded a contract with ISP for more Internet connection bandwidth.

Access Requirements

Due to the fact that GIAC enterprises has a variety of relationships to different people each with different access authorizations to the GIAC resources, the following section describes each group's role and defines their access requirements to the GIAC resources.

Customers

GIAC has Customers who are located worldwide. These customers access the GIAC fortune cookies via the GIAC websites. This website provides detailed information on GIAC enterprises and how to purchase online fortune cookies. This is the only way to buy the fortune cookies from GIAC.

The first access to the GIAC website is by using the unsecured HTTP protocol on port 80. As soon as customers do any online orders or do any financial transactions by entering a valid credit card or bank transferring information,

Secure Socket Layer (SSL) on port 443 TCP will be used to secure the communication between the customers and the GIAC website. The transaction is recorded on the SQL database server hosted in the GIAC trusted network behind the firewall and a confirmation will be generated and sent to the customers via e-mail port 25 TCP. Customers can also communicate with GIAC enterprises service department by sending emails encrypted via PGP.

Suppliers

GIAC Enterprises has contracts with a set of suppliers who supply the fortune cookie sayings.

GIAC Enterprises website provides their suppliers with strict access accounts "logon name and password". Suppliers use these accounts to access a special application on the GIAC website to view the activities of fortune sayings database. This access is performed via an HTTPS communication on port 443 TCP. Suppliers can also communicate with GIAC enterprises service department by sending emails encrypted via PGP. GIAC is also able to connect to suppliers' websites via https to place orders for sayings.

GIAC Enterprises does not see any need for their suppliers to directly access the internal network.

Partners

GIAC has contracts with several partners who purchase the fortune sayings from GIAC and translate them into various languages and re-sell fortune cookies sayings in other language markets.

GIAC provides each partner with an individual area on the GIAC website to allow them to access the web online via an HTTPS (on port 443 TCP) session. All partners must have strict access accounts "logon name and password" to view or download the translated fortunes. GIAC partners can also communicate directly with GIAC internal service department via SMTP port 25.

Employees

GIAC IT department has rolled out Windows XP SP2 as workstation operating system. Each GIAC user has its own Windows logon account. All user accounts are recorded on the Microsoft active directory (AD). All employees can send emails by using the locally installed Lotus Notes client on each user workstation. The opening of the lotus notes client requires a user password. All inbound and outbound emails are scanned for viruses. Internet access for GIAC users for the protocols (HTTP, HTTPS and Secure Shell) is also possible. To access the Internet via http and https, GIAC users have to authenticate themselves on the Symantec firewall. Symantec firewall supports LDAP authentication and uses the Microsoft active directory as LDAP for user logon data. A request must be made to the IT department for access to the Internet via

Secure Shell.

Sales/Teleworkers

All laptops of GIAC Mobiles Sales Force and Teleworkers are equipped with Cisco VPN Client and Norton Anti Virus program. GIAC Enterprises also provides GIAC Mobiles Sales Force and Teleworkers with RSA SecurID tokens. GIAC Mobiles Sales Force and Teleworkers can access all GIAC Internal resources in the GIAC internal server network from their laptops, they have to use the Cisco VPN client to open an IPSEC VPN connection to the GIAC CISCO VPN concentrator and also use the RAS token ID for authentication before the VPN tunnel can be established.

General Public

General users can access the GIAC website from the Internet via HTTP to get GIAC information published on the GIAC web site. A relationship between GIAC Enterprises and general users has not been established. The only type of relationship available with GIAC Enterprises for these users is via the GIAC service department using SMTP.

Data Flows

The following table shows the flow of network traffic and the necessary services and ports:

Source	Destination	Port(s)/Protocol	Description
Customers	GIAC Public Web server	80/TCP (HTTP)	Allow Customers to access GIAC static information website
Customers	GIAC Public Web server	443/TCP (HTTPS)	Allow Customers to access their application web area (Customers have to use their UID and password)
Customers	GIAC public Anti Spam server	25/TCP (SMTP)	Allow Customers to send mails to the GIAC service department)
Suppliers	GIAC Public Web server	80/TCP (HTTP)	Allow Suppliers to access GIAC static information web site
Suppliers	GIAC Public Web server	443/TCP (HTTPS)	Allow Suppliers to access their application web area (Suppliers have to use their UID and password)
Suppliers	GIAC public Anti Spam server	25/TCP (SMTP)	Allow Suppliers to send mails to the GIAC service department)
Partners	GIAC Public Web server	80/TCP (HTTP)	Allow partners to access GIAC static information web site

Partners	GIAC Public Web server	443/TCP (HTTPS)	Allow partners to access their application web area (Partners have to use their UID and password)
Partners	GIAC public Anti Spam server	25/TCP (SMTP)	Allow partners to send mails to the GIAC service department)
GIAC Employees PC's network	Any Internet web server + GIAC web server	80/TCP (HTTP)	Allows Employees to access to the Internet
GIAC Employees PC's network	Any Internet web server+ GIAC web server	443/TCP (HTTPS)	Allows Employees to access to the Internet
GIAC Mobiles and Teleworkers	VPN Concentrator	500/UDP (IKE)	Required for VPN connection "IKE" (Internet Key Exchange)
GIAC Mobiles and Teleworkers	VPN Concentrator	IP 50 (ESP)	Required for VPN connection "ESP" (Encapsulation Security Payload)
General Public	GIAC Public Web server	80/TCP (HTTP)	Allow anybody to access GIAC static information web site
General Public	GIAC public SMTP server	25/TCP (SMTP)	Allow external users to send mails to the GIAC service department)
DMZ II SMTP Relay	Internet Any	25/TCP (SMTP)	Allows SMTP Relay to deliver mails coming from GIAC domain to Internet
DMZ II SMTP Relay	Internal SMTP server	25/TCP (SMTP)	Allows SMTP Relay to deliver mails to the GIAC internal SMTP server
DMZII Anti Spam	Symantec Anti Spam update site "http://aztec.brightmail.com"	80 /TCP (HTTP), 443/TCP (HTTPS)	Allows Anti Spam server to download filter update from the Anti Spam update server "aztec.brightmail.com.
DMZII Web server	GIAC internal database server	1433/TCP (SQL)	Allows GIAC web server to communicate with internal Database server.
Cisco Border Router and VPN Concentrator	RSA server	1645/UDP (RADIUS_AUTH), 1646/UDP (RADIUS_ACC)	Allow Cisco external devices to communicate with internal RSA server for checking user authentication
Cisco Border Router and VPN Concentrator	Syslog server	514/UDP (SYSLOG)	Allow Cisco external devices to send logs to the syslog server.
DMZ I VPN IP Pool (10.100.2.64/26)	Internal server network	ALL	Since access filter rules have been configured on the VPN concentrator, the firewall will allow any traffic coming from the VPN IP pool to the GIAC internal network.
Internal SMTP server	GIAC public SMTP server	25/TCP (SMTP)	Allows SMTP communication between internal and external GIAC SMTP servers.
Management workstation 1 & 2	Cisco VPN Concentrator	443/TCP (HTTPS)	Allow secure https connection for GIAC IT administrators
Management workstation 1 & 2	Cisco Border Router, VPN Concentrator and Anti Spam server	22/TCP (SSH)	Allow secure shell connection for GIAC IT administrators
Management workstation 1 & 2	GIAC web server and SMTP relay in DMZ II	3389/TCP (MSTS)	Allow terminal service connection for GIAC IT administrators

Architecture Components

There are lots of security components that work together to allow the external

world to do business with GIAC Enterprises. The main GIAC security components included in the GAIC network architecture will prevent unauthorized access and provide lines of Defense between the Internet and GIAC internal network. The main GIAC security components are:

1. Border Router (Packet Filtering Router)
2. Firewall (Application Gateway)
3. VPN Concentrator (Cisco VPN Concentrator, which also provides Packet filtering)
4. Network based IDS sensors

Filtering Router(s)

The border router of GIAC is the first layer of filtering for packets coming into the GIAC Network. As the first line of Defense its function is to prevent obvious unwanted packets from entering the network, such as attacks from spoofed private addresses. It is also the last layer of egress filtering for packets leaving the GIAC network.

GIAC has decided to install a Cisco router (Cisco 3745, running version 12.3 IOS.). All of the GIAC network staff are experienced and have a good knowledge of Cisco.

Firewall(s)

GIAC has chosen the Symantec Security Gateway 5440 for their firewall solution. The Symantec Security Gateway 5440 is an appliance firewall based on hardening Linux operating system. Symantec Security Gateway 5440 is a packet filter, a stateful packet inspection and application gateway. Although Symantec Security Gateway 5440 supports additional functionalities like IPSec tunneling (client-to-gateway and gateway-to-gateway) and IDS (Intrusion Detection System), GIAC has decided to delegate the VPN functionality and to install a separate VPN gateway based on CISCO VPN concentrator. The purpose of which is to terminate their VPN tunnels, as well as to install a separate IDS on different devices based on Symantec IDS Manhunt. The Symantec Security Gateway 5440 also provides Split DNS service, NTP Time Service as well as Network Address Translations.

The Symantec Security Gateway 5440 acts as a second Defense device after the border Router. The first interface of the Symantec firewall eth0 is an inside interface connected to the GIAC LAN and assigned as a trusted interface. Second interface eth1 is connected to the Internet and assigned as an outside untrusted interface. The third firewall interface eth2 is connected to DMZ. GIAC has decided to enable the fourth interface as VPN DMZ to connect it to the inside interface of the Cisco VPN Concentrator

Further measures were taken by the GIAC IT department:

- Enabling the Content Filtering on the Symantec Security Gateway 5440.
- Enabling the LDAP authentication service on the Symantec Security Gateway 5440 for Internet http browsing.
- Enabling the NTP time service on the Symantec Security Gateway 5440 for GIAC DMZ servers. All the GIAC DMZ servers have to synchronize their time with the firewall by taking the IP address of the firewall DMZ interface as NTP server.
- Enabling the DNS service on the Symantec Security Gateway 5440. The firewall will act as public DNS server for the GIAC public domain "GIAC.com". The external IP address of the firewall is registered as the DNS server responsible for resolving GIAC public DNS records. There is a Secondary external DNS server hosted at the ISP, which performs zone transfer to the Primary.
- A SGMI (Symantec Gateway Management Interface) is required to manage the Symantec Security Gateway 5440. The administration / configuration of the Symantec Security Gateway 5440 can only be carried out from both of the management terminal servers. The management of the Symantec Security Gateway 5440 via SGMI is protected by source IP, as well as by UID / password. As a result, the IP addresses of both management terminal servers are assigned as management stations on the Symantec Security Gateway 5440.
- The staff who are going to administrate/configure the firewall should first take training courses.
- Back up the current configuration of the Symantec Security Gateway 5440 every day.
- The daily Symantec Security Gateway 5440 logging files should be sent directly to the logfile server.
- Buying a second Symantec Security Gateway 5440 as a cold standby firewall and installing it next to the productive firewall should the main firewall crash. This means a restore can be performed on the cold standby firewall to prepare it for taking the role as productive firewall.
- Firewall Notification of specific alert events should be emailed to firewall staff for immediate attention.

VPN(s)

GIAC Enterprises has chosen the Cisco VPN Concentrator 3030 to provide secure remote access to the internal network via a VPN. Cisco VPN concentrator supports all the required IPSEC security services and protocols for creating and maintaining secure tunnels. Filtering is configured on the Cisco VPN Concentrator to only allow traffic that is absolutely necessary.

The inside interface of the concentrator connects to the second DMZ of the firewall. All the traffic that leaves the Cisco VPN Concentrator to enter the GIAC internal network should pass through the firewall. The administration /

configuration of the Cisco VPN Concentrator can be carried out only from the management terminal servers that are installed in the GIAC internal network.

Network based IDS sensor(s)

GIAC Strategy is to monitor incidents in the network for additional security. As a result, it has decided to install several intrusion detection systems IDS sensors. GIAC chose to buy Symantec Manhunt as IDS. GIAC concluded a contract with Symantec for maintaining and supporting all Symantec security products installed in GIAC network.

The first IDS sensor is installed in the network between Symantec Gateway Security 5440 and the border router. The second IDS sensor is installed in the public DMZ II and the last IDS sensor is installed on the internal network directly behind the firewall.

All IDS sensors monitor the network, detect and alarm the firewall staff about any major alerts via emails. The IDS logging files are saved daily on the Log file server in LAN.

Additional Components

GIAC LAN Servers

Database Server

The database server is a Windows 2000 Server with Service Pack 4. Microsoft SQL 2000 server has been installed on the server with the latest Service Pack and with all the Windows 2000 Hotfixes (pre-SP4). The primary function of the SQL database server is to act as a repository of customer data for record keeping and data retrieval for accounting and marketing purposes. In additional, Symantec Anti-virus software for Windows 2000 server has been installed to scan for potential viruses.

DNS Server

A Split DNS architect (Public and Private DNS Servers) has been implemented. The private internal name server is a DNS BIND 9.2 running on RedHat Enterprise Linux 3 AS. It acts as the domain name resolver for the internal network. The private internal name server directs all requests for external domains to the firewall internal interface (eth0). The firewall then asks the main root name server in the Internet to resolve external domains and forwards the responses back to the internal name server.

SMTP Server

The internal SMTP server is a Domino server version 6.0 running on Windows 2000 Operating System with Service Pack 4 and all the Windows 2000 Hotfixes (pre-SP4). The internal Lotus Notes server forwards all outbound SMTP traffic to

the external Lotus Notes SMTP relay in the DMZ. In addition, Symantec Anti-virus software for Lotus Notes and Windows 2000 server has been installed to scan for potential viruses.

Syslogd and Log File Server
The server is a Windows 2000 Server with Service Pack 4 and all the Windows 2000 Hotfixes (pre-SP4). Windows Syslog software has been installed on the server. The firewall's logging files are saved daily on to the internal log file server. All other Cisco network devices are configured to send logging traffic to the syslog server. In addition, Symantec Anti-virus software for Windows 2000 server has been installed to scan for potential viruses.

RSA ACE/Server
The server is a Windows 2000 server with Service Pack 4 and with all the Windows 2000 Hotfixes (pre-SP4). The primary function of the token-based RSA ACE/Server is to provide centralized authentication of all remote connections. In addition, Symantec Anti-virus software for Windows 2000 server has been installed to scan for potential viruses.

Management Workstation
The server is a Windows 2000 server with Service Pack 4 and all the Windows 2000 Hotfixes (pre-SP4). Only the IT Staff can administrate and configure the firewall as well as other Cisco network devices (Border Router, Switches, VPN concentrator) via HTTPS. In addition, Symantec Anti-virus software for Windows 2000 server has been installed to scan for potential viruses.

GIAC DMZ Servers

Anti Spam Server
The GIAC external Anti Spam server is Symantec Brightmail Anti Spam 6.0.1 running on Redhat Enterprise Linux 3 WS. This Anti-Spam server acts as public SMTP server. All inbound SMTP traffic coming from the Internet goes to the Anti-Spam server. After the SMTP traffic is checked for Anti Spam, the server forwards the SMTP traffic to the SMTP relay in the same DMZ.

SMTP Rely Server
This SMTP relay server is a Domino Server version 6.0 running on Windows 2000 operating system with Service Pack 4 and all the Windows 2000 Hotfixes (pre-SP4). This SMTP relay will forward outbound SMTP traffic coming from the internal SMTP server directly to the Internet as well as forwarding inbound SMTP traffic coming from the Anti Spam server directly to the internal SMTP server. In addition, Symantec Anti-virus software for Lotus Notes and Windows 2000 server has been installed to scan for potential viruses.

Web Server
GIAC's web server is an Internet Information Server 5.0 running on Windows

2000 operation system with Service Pack 4 and all the Windows 2000 Hotfixes (pre-SP4). Additional operating system hardening has been done by running only the services necessary to support web server functionality. This web server also supports SSL/HTTPS for Customers, Suppliers and Partners. In addition, Symantec Anti-virus software for Windows 2000 server has been installed to scan for potential viruses.

Network Diagram

This network diagram of GIAC will give an overview of the different zones listed below:

1- Internet zone
2- DMZ I VPN zone
3- DMZ II GIAC public Server zone
4- GIAC internal network

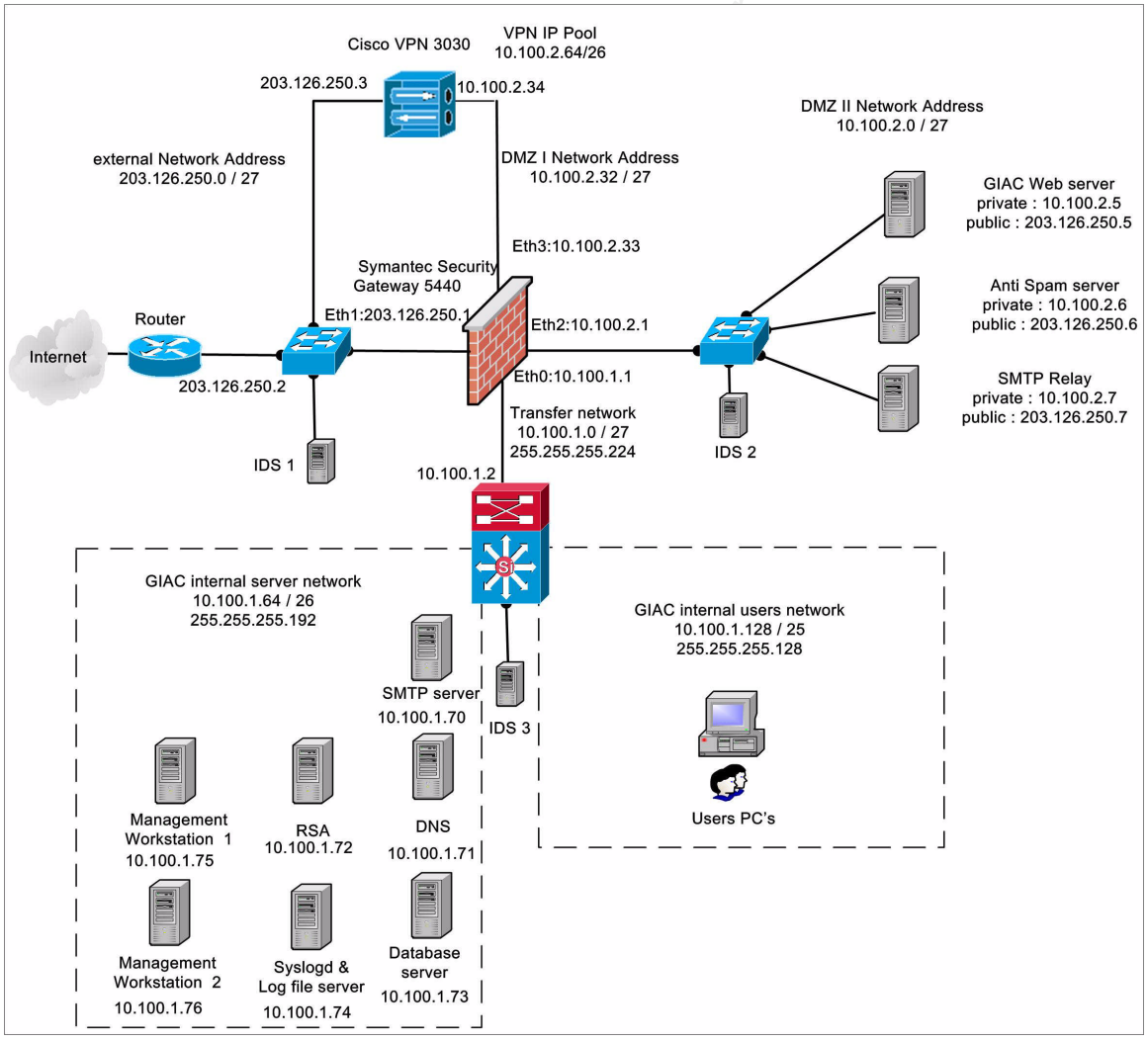

Figure 2: GIAC Network Diagram

IP addressing scheme

The following table shows the IP addressing schema and individual addresses used as the basis of the GIAC perimeter design. All internal IP addresses are non-routable (RFC 1918). Each DMZ server has a physical IP address and an additional public IP address. The DMZ servers can be reached from the Internet using this additional public IP address. The firewall will use Static NAT (Network Address Translation) to re-route the traffic to the real IP addresses of the DMZ servers. The firewall will use its public interface's outside IP address that is connected to the Internet as Static NAT (Network Address Translation) for all access to the Internet.

Network zone	**Network Address**	**Subnet Mask**
External network	203.126.250.0	255.255.255.224
VPN DMZ	10.100.2.32	255.255.255.224
Public server DMZ	10.100.2.0	255.255.255.224
GIAC internal server Network	10.100.1.64	255.255.255.192
GIAC internal users network	10.100.1.128	255.255.255.128
VPN IP Pool	10.100.32.64	255.255.255.192

Implementing Defense-In-Depth

The implementing of defense-in-depth in today's work is complex and the first step is to incorporate it into multi-layer security architecture. There are many security devices that play a role in the complete security structure. The defense-in-depth is not only provided by multi hardware layer and software such as Firewall, Border Router, IDS, VPN tunneling and Anti Virus software, but it also includes Corporate and security policies as well as employee awareness and training. All of this can lead to realize defense-in-depth successfully within modern security organizations.

Assignment 3: Router and Firewall Policies

General Security Stance

Before an organization connects to the Internet, a policy should be established for governing this connection. However, the organization must be aware that policy development is a process which is not finished until all firewall, border router and other technologies to be correctly implemented have been chosen.

Security policies should also be designed to provide effective and economically efficient directives for risk mitigation. Policies should be based upon a formal security stance that is determined by management. This policy should also address three major areas: security, use, and management and administration [24].

In general, a security stance of 'least privilege' can be used in most commercial, financial, Internet, and governmental environments. A typical security stance is: “All data defined as confidential must be protected on a need to know basis only to properly identified and authenticated entities, in all of its forms and on all media, during all phases of its life, from generation to destruction, such that it cannot be compromised, released to any unauthorized entity, or otherwise have its confidentiality or integrity placed at risk. All processing resources, including all applications, systems, network, hardware and software, are only accessible on a need to know basis, only to properly identified and authenticated entities.”

Border Routers are an important part of a network and provide a capability to help secure the perimeter of a protected network. Border routers are used as part of defense-in-depth. They act as the first line of defense and their security is a vital part of the overall security for the networks they serve. They contain static routes that pass all connections intended for the protected network to the firewall.

Firewalls provide additional access control over the content of the connection. They can also perform user authentication. This approach is recommended rather than only using a router because it offers more security.

However, there are many devices that play a role in the overall security structure. Individually, any one of them might easily be broken. However, when tied together they complement each other resulting in a much more secure system area than any one of the individual components on their own could provide.

Border Router(s) Security Policy

The first purpose of the border router is to route traffic between the Internet and the GIAC Enterprises network. The second purpose of the border router is the first layer of defense and is used for ingress and egress network layer packet filtering.

Configure and restrict Console, VTY and Auxiliary Port Access

First enable the password-encryption service to store passwords not in clear text. Cisco provides two types of passwords, one is weak and has to disable and the other uses MD5 and is much stricter. The latter type of password will be used.

```
Router(config)# service password-encryption
```

```
Router(config)# enable secret <password>
Router(config)# no enable password
```

Set warning for unauthorized access as login banner on the border router

```
Router(config)# banner motd #
Warning: Any unauthorized use of this system is prohibited.
#
```

Configure console login, set exec idle time out to 5 minutes, authentication is local and disable output transport.

```
Router(config)# line con 0
        exec-timeout 5 0
        login local
        transport output none
        end
```

Configure AUX line, set exec idle time out to 1 second, authentication is local, disable output transport and disable exec.

```
Router(config)# line aux 0
        exec-timeout 0 1
        login local
        transport input none
        no exec
        end
```

The VTY access is filtered with access-list 90, set exec idle time out to 10 minutes, logging is synchronous, authentication is local, restrict accepting traffic from ssh required line configuration mode and transport is restricted to SSH.

```
Router(config)# access-list 90 permit 10.100.1.15 0.0.0.0
Router(config)# access-list 90 permit 10.100.1.16 0.0.0.0
Router(config)# access-list 90 deny ip any any log
Router(config)# line vty 0 4
        Access-class 90 in
        exec-timeout 10 0
        logging synchronous
        login local
        ip ssh time-out 150
        ip ssh authentication-retries 3
        transport input ssh
        end
```

Configuring of AAA services at login will be as follow:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default group tacacs+ enable
Router(config)# aaa authentication enable default enable
Router(config)# aaa authorization exec default group tacacs+ if-
authenticated
```

```
Router(config)# aaa accounting commands 15 default stop-only group
tacacs+
Router(config)# aaa session-id common
```

Configuring tacacs server:

```
Router(config)# tacacs-server host 10.100.1.72 single-connection key ***
```

Router Hardening by disabling unnecessary Features and Services

CDP (Cisco Discovery Protocol) is a proprietary protocol that Cisco routers use to identify each router on a network. CDP is almost never needed:

```
Router(config)#no cdp
```

Disable the TCP and UPD standard network services:

```
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
```

Disable finger service, which allows remote listing of users:

```
Router(config)# no ip finger
Router(config)# no service finger
```

Disable Cisco web-based configuration service

```
Router(config)# no ip http server
Router(config)# no ip https serve
```

Disable the Bootp server. This service allows other routers to boot from this one:

```
Router(config)# no ip bootp server
```

Disable auto-loading. By enabling this configuration, the router will attempt to load its configuration via TFTP:

```
Router(config)# no boot network
Router(config)# no service config
```

Disable IP source routing. This allows packets to specify their own routers:

```
Router(config)# no ip source-route
```

Disable SNMP service which can be used by an attacker to get information about network configuration:

```
Router(config)# no snmp-server
```

Disable router and DNS name resolution:

```
Router(config)# no ip name-server
```

Configure NTP service:

```
Router(config)# ntp source FastEthernet0/1
Router(config)# ntp server 203.126.250.1
Router(config)# service timestamps debug datetime msec localtime show-
```

timezone
Router(config)# service timestamps log datetime msec localtime showtimezone

Logging Configuration

Logs are useful for monitoring the general performance of the router as well as forensic evidence in the event of an attack.

Enable and configure logging to send logs through the internal interface to the internal syslog server.

```
Router(config)# logging on
Router(config)# logging 10.100.1.13
Router(config)# logging source-interface eth 0/1
Router(config)# logging buffer information
```

Disable logging to the IOS console

```
Router(config)# no logging console
```

Access Control Lists

Inbound Access Control Lists (Ingress Filtering)

The inbound (ingress) filters will be placed upon the Internet facing serial interface. The following common services or IP addresses have to be restricted because they can be used to gather information on the protected network or they have weaknesses that can be exploited against the protected network

```
! Deny section
! ####################################
! Reject GIAC's subnet if it comes from the outside.
access-list 100 deny ip 203.126.250.0 0.0.0.31 any log

! Reject traffic which has IP address reserved used in RFC 1918 and for
Loopback address
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log

! Reject traffic with the IP address 127.0.0.0 and none address
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log

! Reject any packets with multicasting source addresses.
access-list 100 deny ip 224.0.0.0 31.255.255.255 any log
```

```
! Reject IANA reserved IP addresses.

access-list 100 deny ip 1.0.0.0 0.255.255.255 any log
access-list 100 deny ip 2.0.0.0 0.255.255.255 any log
access-list 100 deny ip 5.0.0.0 0.255.255.255 any log
access-list 100 deny ip 7.0.0.0 0.255.255.255 any log
access-list 100 deny ip 23.0.0.0 0.255.255.255 any log
access-list 100 deny ip 27.0.0.0 0.255.255.255 any log
access-list 100 deny ip 31.0.0.0 0.255.255.255 any log
access-list 100 deny ip 36.0.0.0 1.255.255.255 any log
access-list 100 deny ip 39.0.0.0 0.255.255.255 any log
access-list 100 deny ip 41.0.0.0 0.255.255.255 any log
access-list 100 deny ip 42.0.0.0 0.255.255.255 any log
access-list 100 deny ip 58.0.0.0 1.255.255.255 any log
access-list 100 deny ip 60.0.0.0 0.255.255.255 any log
access-list 100 deny ip 70.0.0.0 1.255.255.255 any log
access-list 100 deny ip 72.0.0.0 7.255.255.255 any log
access-list 100 deny ip 80.0.0.0 15.255.255.255 any log
access-list 100 deny ip 96.0.0.0 31.255.255.255 any log
access-list 100 deny ip 197.0.0.0 0.255.255.255 any
access-list 100 deny ip 222.0.0.0 1.255.255.255 any

! Reject incoming echo requests.
access-list 100 deny icmp any any echo log

! Reject any NetBIOS traffic and 445 (tcp and upd) for Windows 2000
access-list 100 deny tcp any any range 135 139 log
access-list 100 deny udp any any range 135 139 log
access-list 100 deny tcp any any eq 445 log
access-list 100 deny udp any any eq 445 log

! reject any incoming traffic for SNMP, Syslog, TFTP, FTP, ssh, finger, RPC(tcp
and UPD)
access-list 100 deny tcp any any range 161 162 log
access-list 100 deny udp any any range 161 162 log
access-list 100 deny udp any any eq 514 log
access-list 100 deny udp any any eq 69 log
access list 100 deny tcp any any eq 21 log
access list 100 deny tcp any any eq 22 log
access list 100 deny tcp any any eq 79 log
access list 100 deny tcp any any eq 111 log
access list 100 deny upd any any eq 111 log

! reject Network Time Protocol
access list 100 deny tcp any any eq 123 log
```

```
! Some other services have to be restricted on the border router too.
access-list 100 deny tcp any any eq tcpmux log
access-list 100 deny udp any any eq tcpmux log
access-list 100 deny tcp any any eq echo log
access-list 100 deny udp any any eq echo log
access-list 100 deny tcp any any eq discard log
access-list 100 deny udp any any eq discard log
access-list 100 deny tcp any any eq systat log
access-list 100 deny tcp any any eq daytime log
access-list 100 deny udp any any eq daytime log
access-list 100 deny tcp any any eq netstat log
access-list 100 deny tcp any any eq chargen log
access-list 100 deny udp any any eq chargen log
access-list 100 deny tcp any any eq time log
access-list 100 deny udp any any eq time log
access-list 100 deny tcp any any eq whois log
access-list 100 deny udp any any eq bootp log
access-list 100 deny tcp any any eq supdup log
access-list 100 deny udp any any eq xdmcp log
access-list 100 deny tcp any any eq rexec log
access-list 100 deny tcp any any eq rlogin log
access-list 100 deny upd any any eq who log
access-list 100 deny tcp any any eq lpr log
access-list 100 deny upd any any eq talk log
access-list 100 deny udp any any eq ntalk log
access-list 100 deny tcp any any eq uucp log
access-list 100 deny tcp any any eq 550 log
access-list 100 deny upd any any eq 550 log
access-list 100 deny tcp any any eq 1900 log
access-list 100 deny udp any any eq 1900 log
access-list 100 deny tcp any any eq 5000 log
access-list 100 deny udp any any eq 5000 log
access-list 100 deny udp any any eq 2049 log
access-list 100 deny tcp any any range 6000 6063 log
access-list 100 deny tcp any any eq 6667 log
access-list 100 deny tcp any any range 12345 12346 log
access-list 100 deny tcp any any eq 31337 log
access-list 100 deny upd any any eq 31337 log

! Permit section
!##########################################

! permit HTTP HTTPS traffic to GIAC web server
access-list 100 permit tcp any host 203.126.250.5 eq www
access-list 100 permit tcp any host 203.126.250.5 eq 443
```

```
! permit Allow SMTP traffic to GIAC Anti Spam server
access-list 100 permit tcp any host 203.126.250.6 eq smtp

! permit DNS traffic to the GIAC public DNS server and zone transfer to
secondary DNS
access-list 100 permit udp any host 203.126.250.1 eq domain
access-list 100 permit tcp host  x.x.x.240 host 203.126.250.1 eq domain

! permit traffic to the VPN Concentrator.
access list 100 permit udp any host 203.126.250.3 eq 500
access list 100 permit esp any host 203.126.250.3

! permit traffic with the ack bit set to 1.
access list 100 permit tcp any 203.126.250.0 0.0.0.31 established

! - Explicitly deny all other addresses
access-list 100 deny ip any any log-input
```

Outbound Access Lists (Egress Filtering)

The outbound (egress) filters will be placed on the FastEthernet interface. All outbound IP traffic from the GIAC public network will be permitted. All other addresses, which are not specifically permitted, will be denied. The restriction of traffic in and out of GIAC network will be carried out on the perimeter firewall by enforcing the policy rules.

```
! – permit outbound IP packet of GIAC address.
access-list 101 permit ip 203.126.250.0 0.0.0.31 any
! - Explicit deny
access-list 101 deny ip any any log-input
```

Interface Configuration.

Set the configuration parameters for the internal and external interfaces of the border router:

Define the IP address and subnet mask of the internal interface:

```
Router(config)# interface FastEthernet0/0
Router(config-if)# description Internal Interface connected to the Firewall
Router(config-if)# ip address 203.126.250.2  255.255.255.224
```

Apply the access-list to all traffic coming into this interface

```
Router(config-if)# ip access-group 101 in
```

Define the IP address and subnet mask of the external interface:

```
Router(config)# interface Serial0/0
Router(config-if)# description External Interface connected to the Internet
Router(config-if)# ip address X.X.X.46 255.255.255.248
```

Apply the access-list to all traffic coming into this interface

```
Router(config-if)# ip access-group 100 in
```

The following services are unnecessary and have to be disabled pre interface in the interface configuration mode.

Disable IP redirect that can be used by an attacker to redirect the packets to unintended destinations

```
Router(config-if)# no ip redirect
```

Disable directed broadcast which can be used for attacks:

```
Router(config-if)# no ip directed-broadcast
```

Disable IP unreachable notification, Redirects and Mask Replies:

```
Router(config-if)# no ip unreachables
```

Disable proxy ARP:

```
Router(config-if)# no ip proxy-arp
```

Primary Firewall(s) Security Policy

The GIAC perimeter firewall is a Symantec Gateway Security 5440. The firewall provides and meets the business requirement for the GIAC firewall policy. All necessary communication through the perimeter firewall must be configured according to rules on the Symantec Gateway Security 5440 in order to permit only specifically required services. By default, the Symantec Gateway Security denies any connection that is not explicitly allowed by an authorization rule. The Symantec Gateway Security evaluates rules on a “best fit” basis, which ensures use of the most conservative and specific rule for each connection attempt. A Symantec Gateway Security evaluates each connection based on a wide range of criteria, including:

- Source and destination address of the connection
- Type of service
- Network interface of the incoming connection
- Time of day and date restrictions
- Group and user restrictions based on strong authentication methods

A Symantec Gateway Security compares all the rules for each connection attempt, except those that have time criteria which are not applicable at the present time. It does not necessarily apply the first rule but rather the best fit

rule. Therefore, it is considered to be nonorder-dependent.

The best fit rule is the most specific one. Specificity ranking is as follows:

- Host entity is more specific than subnet entity.
- Subnet entity is more specific than interface entity.
- Network interface is more specific than universe entity.

Rulebase

Rule ID: 1
Description:Allow access from any IP address in the Internet to the GIAC web server via http/https
Access Mode: Allow
Services: http https
In Via Interface:eth1
Out Via Interface:eth2
Source: universe
Destination: he_giac_public_web_server
Authentication: none
Application Data Scanning: enabled

Rule ID: 2
Description: Allow access from any IP address in the Internet to the GIAC public Anti Spam server
Access Mode: Allow
Services: smtp
In Via Interface: eth1
Out Via Interface: eth2
Source: universe
Destination: he_giac_public_antispam_server
Authentication: none
Application Data Scanning: enabled

Rule ID: 3
Description: Allow access from the GIAC public SMTP server to the Internet
Access Mode: Allow
Services: smtp
In Via Interface: eth2
Out Via Interface: eth1
Source: he_giac_public_smtp_server
Destination: universe
Authentication: none
Application Data Scanning: enabled

Rule ID: 4

Description: Allow access from the GIAC public SMTP server to the internal GIAC SMTP server
Access Mode: Allow
Services: smtp
In Via Interface: eth1
Out Via Interface: eth0
Source: he_giac_public_smtp_server
Destination: hi_giac_lan_smtp_server
Authentication: none
Application Data Scanning: enabled

Rule ID: 5
Description: Allow access from GIAC Anti Spam server to the Brightmail update server
Access Mode: Allow
Services: https
In Via Interface: eth2
Out Via Interface: eth1
Source: he_giac_public_antispam_server
Destination: he_aztec_brightmail_com
Authentication: none
Application Data Scanning: enabled

Rule ID: 6
Description: Allow access from GIAC public web server to the internal GIAC SQL server
Access Mode: Allow
Services: MSSQL
In Via Interface: eth2
Out Via Interface: eth0
Source: he_giac_public_web_server
Destination: hi_giac_lan_sql_server
Authentication: none
Application Data Scanning: disabled

Rule ID: 7
Description: Allow access from the GIAC border router to the GIAC internal RSA server
Access Mode: Allow
Services: 1645/UDP 1646/UDP
In Via Interface: eth1
Out Via Interface: eth0
Source: he_giac_border_router
Destination: hi_giac_lan_rsa_server
Authentication: none
Application Data Scanning: disabled

Rule ID: 8
Description: Allow access from the GIAC border router to the GIAC internal syslog server
Access Mode: Allow
Services: 514/UDP
In Via Interface: eth1
Out Via Interface: eth0
Source: he_giac_border_router
Destination: hi_giac_lan_syslog_server
Authentication: none
Application Data Scanning: disabled

Rule ID: 9
Description: Allow access for remote users from the VPN IP pool to the GIAC internal GIAC network
Access Mode: Allow
Services: all
In Via Interface: eth3
Out Via Interface: eth0
Source: ne_giac_vpn_ippool
Destination: ni_giac_lan_server_network
Authentication: none
Application Data Scanning: enabled

Rule ID: 10
Description: Allow access for GIAC employees to the Internet
Access Mode: Allow
Services: http https
In Via Interface: eth0
Out Via Interface: eth1
Source: ni_giac_users_network
Destination: universe
Authentication: ldap
Application Data Scanning: enabled

Rule ID: 11
Description: Allow access for GIAC IT administrators from GIAC internal management workstion 1 & 2 to GIAC order router, GIAC VPN concentrator and GIAC DMZ servers
Access Mode: allow
Services: ssh MSTS
In Via Interface: eth0
Out Via Interface: any
Source: he_giac_lan_management1, he_giac_lan_management2
Destination: he_giac_border_router, he_giac_vpn_concentrator,

ne_giac_public_dmz
Authentication: none
Application Data Scanning: disabled

Firewall Service Definition:

Protocol Name	Port	Protocol
Smtp	25	TCP
http	80	TCP
https	443	TCP
Ssh	22	TCP
MSSQL	1433	TCP
radius_auth	1645	UDP
radius_acc	1646	UDP
Syslog	514	UDP
All	1 – 1023	TCP UDP
MSTS	3389	TCP

Firewall Object Definitions:

Object Name	Network Address	Network Mask
Universe	0.0.0.0	0.0.0.0
he_giac_public_web_server	10.100.2.5	255.255.255.255
he_giac_public_antispam_server	10.100.2.6	255.255.255.255
he_giac_public_smtp_server	10.100.2.7	255.255.255.255
hi_giac_lan_smtp_server	10.100.1.70	255.255.255.255
he_aztec_brightmail_com	216.250.16.32	255.255.255.255
hi_giac_lan_sql_server	10.100.1.73	255.255.255.255
he_giac_border_router	203.126.250.2	255.255.255.255
hi_giac_lan_rsa_server	10.100.1.72	255.255.255.255
hi_giac_lan_syslog_server	10.100.1.74	255.255.255.255
Source: ne_giac_vpn_ippool	10.100.2.64	255.255.255.192
ni_giac_lan_server_network	10.100.1.64	255.255.255.192
ni_giac_users_network	10.100.1.128	255.255.255.128
he_giac_lan_management1	10.100.1.75	255.255.255.255
he_giac_lan_management2	10.100.1.76	255.255.255.255
he_giac_vpn_concentrator	10.100.2.34	255.255.255.255
ne_giac_public_dmz	10.100.2.0	255.255.255.224

Firewall Address Translation:

Requested Address	In Via Interface	Redirected Address	Out Via Interface	Protocol Name
203.126.250.5	Eth1	10.100.2.5	Eth0	http
203.126.250.5	Eth1	10.100.2.5	Eth0	https
203.126.250.6	Eth1	10.100.2.6	Eth0	smtp

References

[1] The Science of Vulnerability Filter, Victor Irwin, TippingPoint http://www.tippingpoint.com/news_inthenews.html

[2] NSS Group IPS test Results, Intrusion Prevention System (IPS), published January 2004 http://www.nss.co.uk/ips/edition2/introduction.htm#Intrusion_Prevention_Systems_(IPS) http://www.nss.co.uk/

[3] TippingPoint Press Release, January 2004, http://www.tippingpoint.com/pdf/press/2004/NSSGold_011904.pdf

[4] Reducing Network Security Risk, Intrusion Prevention, Symantec Corporation http://www.symantec.com/

[5] Cricket Liu, Jerry Peek, Russ Jones, Bryan Buus, Adrian Nye; Managing Internet Information Services; O'Reilly & Associates, 1994

[6] Preferred Computer System; IPStesting.pdf http://www.preferredcomputers.com/whitepapers/download/IPSTesting.pdf

[7] Symantec Security Gateway 5440 v. 2.0 product manuals http://www.symantec.com/techsupp/enterprise/products/sym_gateway_security/sym_gw_security_2_5400/manuals.html

[8] Symantec Network Security 4.0 product manuals http://www.symantec.com/techsupp/enterprise/products/sns/sns_4/manuals.html

[9] Symantec Manhunt 3.0 product manuals http://www.symantec.com/techsupp/enterprise/products/manhunt/manhunt_3.0/manuals.html

[10] The CERT Guide to System and Network Security Practices; Julia H. Allen; Addison-Wesley May 2001

[11] Incident Response; Kenneth R. van Wyk & Richard Forno: O'Reilly July 2001

[12] IT Security- Risking the Corporation; Linda McCarthy foreword by Gene Spafford, Pearson Education Inc. 2003

[13] Network of Excellence
http://www.networks-of-excellence.com

[14] Mukherjee, Heberlein, Levitt; "Network Intrusion Detection"
http://seclab.cs.ucdavis.edu/papers/mhl94.pdf

[16] Building Internet Firewalls - 2nd Edition; D. Brent Chapman & Elizabeth D. Zwicky; O'Reilly 2000

[15] Assembly Instructions Included (Cisco Routers); Gilbert Held; Network Magazine, January 2001

[17] Cisco IOS 12 Network Security; Cisco Press/Macmillan Technical Publishing; 1999

[18] Cisco Security Architectures; Gil Held & Kent Hundley; McGraw-Hill; 1999

[19] Router-Based network Defense; Gilbert Help; Sys Admin; March 2000

[20] Cisco Intrnetworking Technologiy Overview
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc

[21] Cisco IOS Release 12.x Security Configuration Guide; Cisco Press 1999

[22] Cisco IOS Dial Services Configuration Guide; Cisco Press 2000.

[23] IANA Port and protocol Number Assignments
http://www.iana.org

[24] Weise, Joel and Martin, Charles R., Sample Data Security Policy and Guidelines Template, Sun BluePrints OnLine, December 2001
http://www.sun.com/blueprints/tools/samp_sec_pol.pdf

[25] William R. Cheswick, Steven M. Bellovin; Firewalls and Internet Security - Repelling the Wily Hacker; Addison-Wesley Professional Computing Series, Addison-Wesley Publishing Company, 1994