GIAC CERTIFIED FIREWALL ANALYST (GCFW)

PRACTICAL ASSIGNMENT
Version 4.1

Dragana Vasic
February 16, 2005

TABLE OF CONTENTS

Assignment 1: Future State of Security Technology: Host-based Intrusion Prevention

1.1 Abstract

The number, complexity and frequency of intrusion attacks have dramatically increased over the years. Viruses and worms have become a widespread problem for the networking community. A recent Symantec report found that between January 1 and June 30, 2004, new vulnerabilities in operating systems and applications were being discovered at an average rate of 48 per week [1]. Because networking environments are becoming more and more complex, it is becoming increasingly difficult to protect them from attackers that threaten application availability, data integrity and data privacy. This is currently one of the most serious problems that companies are facing.

The Intrusion Prevention System (IPS) is a new technology that evolved from firewalls and Intrusion Detection Systems. It is designed not only to detect possible threats, but also to protect networked systems from unauthorized access, data modification, damage and disruption. There are two types of Intrusion Prevention System: host-based and network-based.

Current network security products such as antivirus software, firewalls, and intrusion detection systems are important defensive tools, and each has a slightly different function and protects from a different set of attacks. According to the SANS institute, an effective approach to network security is not to rely on a single solution, but rather to use a multi-layered, defense-in-depth method where security solutions are placed at different points within the network, all working together [2]. Intrusion Prevention Systems are a significant addition to a layered defense approach, but are not intended to replace other technologies. Only a combination of formal security policies, packet-filtering routers, firewalls and intrusion detection/prevention systems provides the greatest level of protection to a network.

1.2 IPS Overview

As rapidly evolving threats and attacks began to appear, Intrusion Detection Systems (IDS) were developed to identify attacks and report to corporate IT personnel. Unfortunately, while conventional Intrusion Detection technologies can monitor and analyze network traffic, they do not prevent an attack; they have been designed only to detect exploits and send alerts to the IDS Manager device. As the number of deployed IDS systems in company networks increases, the rise in alarm traffic results in increasing delays between the detection of an attack and any corrective action.

Another problem with IDS tools is that they rely on signatures to detect threats [3]. If the IDS system is not updated with the newest signatures, it cannot recognize a new attack. Furthermore, the signature matching approach that IDS products use can generate a huge number of alarms, and while some of them are legitimate, many are not. In order for IDS systems to produce only a small number of valid alerts and eliminate false positives and false negatives, the description of what normal traffic is must be very unrestrictive. Obviously, there was a need for a new mechanism that did not rely on signature matching to respond to an intrusion and that could proactively protect network systems in a timely manner [4].

These shortcomings in current IDS products have driven the development of Intrusion Prevention Systems. While traditional Intrusion Detection systems are reactive in nature, an IPS is a proactive defense system designed to detect abnormal behavior or attacks that may not even have been defined yet and stop them before any damage occurs. The IPS detects abnormal behavior by building a profile of the normal operation of a system. It then compares the currently running system to that profile, and any activity that does not match the profile of “normal” triggers an alarm. In this way attacks can be identified even if the attack mechanism is unknown.

Intrusion Prevention Systems include both signature-based blocking of known attacks and behavior profile or anomaly-based detection algorithms. An IPS compares current network traffic to previously established baselines, and incorporates a policy that defines what variations from the baseline constitute a violation. If there is a violation of the policy the IPS can be configured to react to it immediately rather than simply alerting someone.

There are currently two main approaches to Intrusion Prevention Systems [5]:

1. Host-based Intrusion Prevention System (HIPS) – software that runs directly on the end computer system and prevents attacks directed at the local host; there are some attacks that only host-based IPS can detect and block [11].
2. Network-based Intrusion Prevention System (NIPS) – an appliance deployed in-line in the network segment which provides protection to all of the systems attached to that network segment and downstream from it.

Both of these combine the concepts of a detection system and a prevention system in one, and each is better suited to protect against some types of attacks than others.

1.3 Host-based IPS

With recent devastating attacks such as Slammer, Blaster and NIMDA, the networking community is realizing that current security measures are inadequate. Perimeter security provides only partial protection because with today’s global communication, the perimeter is no longer a well-defined boundary. The development and deployment of wireless networks, SSL, and VPNs has facilitated user access to critical information, but at the same time it has effectively extended the network perimeter and provided more paths for exploits into the enterprise network. Compromised laptops, unpatched software, and unapproved applications are easily brought into organizations and can successfully bypass perimeter security. A new infection introduced this way can rapidly propagate through the organization, as there is practical difficulty in constantly patching and updating antivirus software on all hosts in the network. Another reason for the inadequacy of current security is that perimeter defenses cannot protect against encrypted traffic or attacks that originate from inside the network boundary.

What is needed in addition to perimeter security is host-based protection for individual servers that reside both on the edge and at the core of the network. Host-based security is the "last line of defense" that protects data where it resides by protecting the operating system, data, and applications, and checking for known vulnerabilities and malicious code infections [8]. Host-based intrusion prevention can apply policies based on several detection methods, including predefined rules, signature analysis, and learned behavior analysis, and then automatically block malicious packets.

There are two different host-based intrusion prevention types – the first deploys a software agent that sits between applications and the operating system kernel. The second is implemented as an operating system kernel modification; this is also known as trusted-operating-system.

1.3.1 Trusted Operating Systems

Trusted operating systems provide generic OS hardening and apply greater security controls than those built into normal operating systems. Trusted operating systems provide Mandatory Access Control (MAC) policies that grant users and applications the most limited set of privileges required to perform their tasks. By restricting access, trusted operating systems limit the damage that can result from unauthorized use or compromise.

There are two MAC models: a non-universal model operates under the assumption that a user or application is unrestricted by default and restrictions are subsequently added, while a universal MAC model assumes that a user or application is fully restricted and capability must be explicitly granted to perform an authorized job. Trusted operating systems allow services, network connections, and system resources to be compartmentalized. Individual users may then be granted access to only those services or resources that they require. By separating resources this way trusted operating systems can prevent potential attacks to linked resources even if one service has been compromised. This can be very useful for companies running systems with web-facing services linked to back-end applications, for example. The biggest drawback of these systems is that they are typically harder to configure and manage than standard operating systems, requiring more knowledgeable administrators [6]. Increased complexity can easily result in initial configuration errors.

There are different commercial products available today that include:

Sun Microsystems Inc.’s Trusted Solaris 8
Argus Systems Group’s PitBull LX and Pitbull Foundation
National Security Agency’s SELinux
Immunix Inc,’s Secured OS

1.3.2 Software agent HIPS

Another way to implement host-based intrusion prevention is through a software program or “agent” that is installed on individual systems. Agents bind with the operating system kernel, intercept and monitor system calls between applications and the kernel, check system calls against a predefined policy, and either permit or deny them based on their adherence to the policy. By intercepting application calls at the kernel level, agents effectively have the ability to prevent violations in real time. Agents also have ability to analyze logs and inspect traffic flowing into and out of the system, looking for any indication of an attack. Most of today’s commercial agents have the ability to identify an attack by utilizing both a database of known signatures and the recognition of anomalous behavior patterns. So there are two primary methods for evaluating system calls:

- known-attack or signature detection
- behavior detection

Signature detection is already a well-known technology that has been utilized in Intrusion Detection Systems, but since every attack looks different signature-based systems cannot keep pace with the ever-increasing number and diversity of threats. Behavior detection, where harmful activity can be detected and stopped independently of the type of attack used, is the mechanism that enables HIPS to prevent both known and unknown attacks [10]. Agents have the intelligence to learn how applications and operating systems behave in their normal operation and thereby recognize an attack if the system changes its behavior. If an attack is detected, the Host IPS system can be instructed to block network traffic from attacking the host, direct applications or the operating system to terminate the offending behavior, or send an alarm. Examples of software agent products are:

- Network Associates Inc.’s Entercept
- Internet Security Systems’ RealSecure Server Sensor
- Cisco Systems’ Cisco Security Agent (CSA)
- Sana Security’s Primary Response

1.3.3 Benefits and drawbacks of HIPS

Benefits:

- Protects against internal attacks (those that are initiated within an enterprise perimeter security). Statistically over 80% of security breaches are caused by insiders – most often employees [9]
- Provides a "last line of defense" in cases when attacks have avoided perimeter security
- Since HIPS protects the host even if security patches have not been installed, companies have time to test and install security patches on a predetermined schedule, effectively putting an end to the update race
- Better suited to discover buffer overflow attacks that are hard to catch at perimeter security
- When installed on mobile systems it safeguards from possible attacks and infections coming from the Internet, through which they connect to the company network
- VPN connections and secure web sites pass encrypted traffic through perimeter security and it is therefore impossible to detect an attack at the perimeter, before the traffic is decrypted. If encrypted data arrives at the protected system, HIPS is able to analyze decrypted traffic thus protecting against attacks passed in an encrypted data stream
- Reduces the number of false alarms because they use real-time behavior analysis in addition to signature-detection to recognize possible attacks
- Prevent "day-zero" attacks as they respond to anomalous behavior detection

Drawbacks:

- No host-based IPS currently supports every operating system– consequently there can be costly overhead of managing HIPS on many different platforms within enterprise
- It is useless against large scale networking attacks that might cause networked computers to disconnect from the network – like denial-of-service attacks
- Since HIPS needs to be installed on every system that needs to be protected initial deployment is time consuming and difficult; it also requires properly trained personnel for initial implementation and later maintenance
- Possible impact on system performance and system stability
- There might be compatibility issues with other software already installed on protected systems
- Because of close integration between HIPS and the host operating system, OS upgrades might cause some problems

1.4 HIPS Implementation - what to look for

There are several issues that should be considered before deploying host-based protection. According to John Pescatore, Gartner analyst: “host-based software that simply locks down the host and only allows certain applications to execute does not meet Gartner’s criteria for host-based intrusion prevention, because it does not protect against flaws in permitted applications [7].” Any chosen solution must be easy to manage and flexible, but there are other requirements as well:

- Behavioral analysis capability – HIPS should not rely only on signatures to provide security as they are reactive in nature – they are only as secure as the latest signature update. The better solution is to use learned behavior analysis in addition to signature-based detection. Anomaly-based detection will establish a profile of what “normal” system and application behaviors are to ensure that the security implemented is proactive.
- Easy deployment – HIPS should allow for fast deployment of new policies, when needed, without requiring any additional IT personnel involvement at the host level - agents should be able to receive code updates and new attack signatures from the centralized Management System
- Flexibility for new policy creation – HIPS should permit the easy customization of existing policies and the creation of new policies
- Must not disrupt normal operation - Since HIPS intercepts all requests to the systems it protects – it should be very reliable, should not negatively impact performance, should prevent violations in a real time, and should not block legitimate traffic
- Centralized reporting and management – all events and alarms generated by the agents should report to the centralized location, where audit logs can be easily archived for incident analysis and reporting. A single administrative console also facilitates the creation and deployment of policies

1.5 HIPS influence on GIAC security architecture design

GIAC Enterprise is experiencing frequent intrusion attempts at the edge of their network lately. Since GIAC expects that critical services and data will be accessible from anywhere, whether in the head office or at the remote site, the IT team has decided to implement a host-based intrusion prevention system on critical systems. HIPS deployment on servers will protect data where it resides and ensure that critical assets remain available. Because GIAC Enterprise has many diverse platforms it would be costly to deploy HIPS on all desktops at this time.

Based on effectiveness and update requirements the GIAC Enterprise IT team has selected Cisco Security Agent (CSA) for its HIPS solution. CSA protects hosts and maintains operating system integrity through behavior analysis, rather than relaying solely on exploit signature matching methods, which will guard GIAC business from known and unknown ("DayZero") threats.

Assignment 2: Security Architecture

2.1 Access requirements and restrictions

GIAC Enterprises is a small business, which markets fortune cookie sayings to customers worldwide. Since all of GIAC Enterprises sales are done via the Internet, and the sole source of its revenue is based upon the fortune cookie sale - security is crucial. With that in mind, the company's CEO wants to invest in a secure and robust network and has charged IT team to design and implement the network and security architecture. In developing the network plan, the IT team defined the company's structure, identified business needs, and took into consideration all different groups and their interaction with GIAC Enterprises. Final results were defined as being: network access policy for customers, suppliers, partners, employees, remote users and general public.

The IT team decided to use Cisco security and networking devices primarily because of the excellent technical support that Cisco provides and because of extensive knowledge base that GIAC's IT team has with Cisco products. GIAC has Cisco SMARTnet support that provides them with access to TAC (Technical Assistance Center) engineers for troubleshooting needs, and also with access to the web site from which they can download the security patches and new software releases. With only one vendor's equipment in the network there will be no finger-pointing when problems arise. GIAC also gets better pricing on their equipment if they use Cisco for all their needs. Another benefit of having all Cisco devices in the network is the possibility to have one Network Management platform – CiscoWorks to manage all devices.

2.1.1 Customers

Customers are companies or individuals that purchase fortune coolies online via the GIAC Enterprises web site. Once at the main page, customers can browse through the product categories, view the listing of fortune sayings they want to order, and also submit purchase orders. Attempting to purchase from the main page redirects the user to the secure web portal that is accessible only via HTTPS. The customer portal will present to the users a login screen where they must enter a valid username and password. For first time customers, after entering some profile information, the initial username and password will be emailed to them. Returning customers already have their profiles created based on their past purchases. All customer profiles, their username and passwords, past purchase orders as well as new purchases requests are stored in a backend database. Use of Secure Socket Layer or SSL (HTTPS) will ensure customers of confidentiality of personal and credit cards information.

Customers also need to be able to send emails to the GIAC sale employees therefore they need to connect to TCP port 25 (SMTP protocol).

For name resolution, UDP port 53 will be allowed to our DNS server residing on the DMZ.

Source	Destination	Port/Protocol	Description
Customers	Web Sever	80/TCP (HTTP)	Access to main web site
Customers	Web Server	443/TCP (HTTPS)	Access to purchase order
Customers	Mail Server	25/TCP (SMTP)	Email communication
Customers	DNS Server	53/UDP (DNS)	Name resolution

2.1.2 Suppliers

Suppliers are companies or contracted individuals that provide fortune cookie sayings for GIAC Enterprises to sell. They need secure access to GIAC network to upload fortune cookie sayings. Suppliers will have the ability to either send files to a GIAC web server through HTTPS (suitable for individual suppliers with small volumes) or use a VPN service (appropriate for huge file uploads).
Suppliers are provided with separate accounts at GIAC Enterprises supplier portal. The supplier's portal is a link accessible from main web page and as with customers is accessible only via HTTPS. Their accounts are accessible only after the supplied username and password are verified. They need to access the portal to upload files with fortune sayings, check the status of their orders and payment status.
Alternatively suppliers can use a VPN connection to get to an SSH server on a screened subnet. They can establish client-to-site VPN connection that will encrypt all traffic traversing the Internet, providing for secure communication with GIAC network. The VPN will be an IPSec tunnel (IKE – 500/UDP, ESP – 50/IP, AH – 51/IP)*. Suppliers will be identified by the IP addresses assigned to them from the outside customers VPN pool – pool A (refer to the internal networks IP address assignment in chapter 2.2.8 for specifics addresses). Once the VPN connection is established they can use SSH Secure File Transfer to transfer files to the company' SSH server.
Files are automatically retrieved from HTTP and SSH servers and uploaded to the internal database server through the use of custom-built application (uses port 5577). In any case, there would be no direct interaction between the suppliers and the internal database.
Suppliers will also need to send email to GIAC support. They need to connect to TCP port 25 and UDP port 53 for name resolution.

Source	Destination	Port/Protocol	Description
Suppliers	Web Sever	80/TCP (HTTP)	Access to main web site
Suppliers	Web Server	443/TCP (HTTPS)	Access to supplier portal

Suppliers	Mail Server	25/TCP (SMTP)	Email communication
Suppliers	DNS Server	53/UDP (DNS)	Name resolution
Suppliers	VPN Concentrator	500/UDP (IKE)	Key negotiation for establishment of VPN
Suppliers	VPN Concentrator	50/IP (ESP)	Permits establishments of VPN tunnel
Suppliers	VPN Concentrator	51/IP (AH)	Permits establishments of VPN tunnel

* IPSec is actually a two-fold process [14]. First, the two endpoints will establish an IKE session to control and provide key management for the IPSec session, and then it will negotiate the parameters of the IPSec tunnel. IPSec consists of two sub-protocols: Encapsulated Security Payload (ESP) and Authentication Header (AH) which can either be used together or separately. ESP protects IP packets by encrypting the contents using cryptography algorithms (like Blowfish, 3DES, etc.), while AH protects IP packet header by computing a cryptographic checksum and hashing the IP packet header with a secure hashing function.
In our implementation of IPSec we have chosen to use both AH and ESP. AH will authenticate the header, while ESP will both ensure the integrity of the payload of the packet and confidentiality using encryption. Therefore we need to pass three protocols in order to successfully establish VPN tunnel – IKE protocol that uses 500/UDP, ESP that is IP protocol 50, and AH that is IP protocol 51.

2.1.3 Partners

GIAC Enterprises has partnered with different organizations for the advantage of reaching broader markets with its fortune sayings. Partner companies translate fortune sayings and then resell fortune cookies thru their distribution systems in different countries.
As with Suppliers, GIAC Enterprises will provide Partners with link to the specific area from the main web page that will contain their specific information and order forms. This link to the partner portal is accessible only via HTTPS, and they have to authenticate themselves by providing a valid username and password.
For downloading of fortune cookie sayings partners will have to establish site-to-site VPN connection, after which they can access an SSH server to download files. The VPN will be an IPSec tunnel (IKE – 500/UDP, ESP – 50/IP, AH – 51/IP). Again, there would be no direct interaction between the partners and the internal database.
The partners will be identified by their source IP to control their access through the firewall once the VPN traffic is decrypted.
As with customers and suppliers, partners also need to use email, and have access to the DNS server.

Source	Destination	Port/Protocol	Description
Partners	Web Sever	80/TCP (HTTP)	Access to main web site

Partners	Web Server	443/TCP (HTTPS)	Access to partners portal
Partners	Mail Server	25/TCP (SMTP)	Email communication
Partners	DNS Server	53/UDP (DNS)	Name resolution
Partners	VPN Concentrator	500/UDP (IKE)	Key negotiation for establishment of VPN
Partners	VPN Concentrator	50/IP (ESP)	Permits establishments of VPN tunnel
Partners	VPN Concentrator	51/IP (AH)	Permits establishments of VPN tunnel

2.1.4 GIAC Enterprises employees on the internal network

Majority of GIAC employees are located in its head office. All internal employees will have Internet access and will be able to send and receive emails. Access to the Internet will be via a proxy server located on the DMZ network (TCP 8080). The proxy server will support outgoing connections to the Internet on ports 80 and 443. Employees can also access company's public web server (TCP 80 and 443) for company related information. An internal DNS server will handle name resolution for protected networks.

All Internal users will also need to access internal resources, such as Microsoft SQL client access to the company database server (TCP 1433), file and print server (TCP 445 for file sharing – Server Message Block (SMB) protocol). IT team has deployed secure IMAP (TCP port 993) for receiving emails and SMTP (TCP port 25) for sending emails.

IT team members will need access to all networking devices for configuration and management, which will be provided via SSH.

Source	Destination	Port/Protocol	Description
Int. Emp.	Web Sever	80/TCP (HTTP)	Access to main web site
Int. Emp.	Web Server	443/TCP (HTTPS)	Access to secure portals
Int. Emp.	Web proxy	8080/TCP	Access to Internet through web proxy
Int. Emp.	Mail Server	25/TCP (SMTP)	Email communication
Int. Emp.	Mail Server	993/TCP (IMAPS)	Email communication
Int. Emp.	DNS Server	53/UDP (DNS)	Name resolution
Int. Emp.	MS SQL	1433/TCP	Access to database
Int. Emp.	File server	445/TCP (SMB)	Access to file server
Int. IT team	Networking devices	22/TCP (SSH)	Device administration

2.1.5 GIAC Enterprises remote users

Several of GIAC employees are working outside of the main office. These are sales people that are located in four regional satellite offices geographically distributed around the world, as well as mobile sales workers, telecommuters, and members of the IT team performing remote monitoring and administration. These employees require the same access to internal resources as they are connected on the local LAN.
Remote offices use a VPN site-to-site connection to the Cisco 3020 VPN concentrator. Different remote offices will be identified by their source IP to control their access through the firewall once the VPN traffic is decrypted.
Mobile employees access main office resources via client-to-site VPN connection. To further improve security, mobile employees are categorized into 2 groups: remote administrators and remote users, and their access to the GIAC network will be identified by the IP address assigned to them from 2 different VPN pools - pool B for remote users and pool C for remote administrators (refer to the internal networks IP address assignment in chapter 2.2.8 for specifics addresses). The VPN will be IPSec tunnel (IKE – 500/UDP, ESP – 50/IP, AH – 51/IP).
Once a VPN session to the VPN concentrator is established, remote GIAC employees are granted access to internal resources. Both groups, remote administrators and remote users, are given access to internal email server to send and receive email (SMTP –TCP 25; IMAPS – TCP 993); access to the company's public web server TCP 80 and 443); access to the internal database (TCP 1433) for different customer and product information and access to the internal file server (SMB – TCP 445).
In addition, members of the IT team, that perform remote administration function, will need secured access to the managed networking devices, which will be provided via SSH.
The network based IDS on VPN segment will monitor decrypted traffic coming out of the VPN concentrator.

Source	Destination	Port/Protocol	Description
Rem. Emp.	Web Sever	80/TCP (HTTP)	Access to main web site
Rem. Emp.	Web Server	443/TCP (HTTPS)	Access to secure portals
Rem. Emp.	Mail Server	25/TCP (SMTP)	Email communication
Rem. Emp.	Mail Server	993/TCP (IMAPS)	Email communication
Rem. Emp.	DNS Server	53/UDP (DNS)	Name resolution
Rem. Emp.	MS SQL	1433/TCP	Access to database
Rem. Emp.	File server	445/TCP (SMB)	Access to file server
Rem. IT team.	Networking devices	22/TCP (SSH)	Device administration
Rem. Emp.	VPN Concentrator	500/UDP (IKE)	Key negotiation for establishment of VPN
Rem. Emp.	VPN Concentrator	50/IP (ESP)	Permits establishments of VPN tunnel
Rem. Emp.	VPN Concentrator	51/IP (AH)	Permits establishments of VPN tunnel

2.1.6 General Public

The general public is allowed access to the GIAC Enterprises public web site to view the company profile and to find contact information – this access requires connections from Internet using HTTP –TCP 80 to be allowed. Also they can send email to the company (SMTP – TCP 25) and have access to the public DNS for public name to IP resolution (UDP 53).

Source	Destination	Port/Protocol	Description
Public	Web Sever	80/TCP (HTTP)	Access to main web site
Public	Mail Server	25/TCP (SMTP)	Email communication
Public	DNS Server	53/UDP (DNS)	Name resolution

2.2 Architecture

2.2.1 Defense-in-depth principle

GIAC Enterprises IT team will use defense-in-depth principles as guidance while designing the new security architecture for its company. They are going to achieve defense-in-depth by a multilayered security architecture [12] that will involve the deployment of routers – with static and stateful filtering capability, firewalls, VPN, intrusion detection system (IDS), and host intrusion prevention software. All of these components will integrate to form a flexible, layered, and powerful overall defense.

Traffic coming from the Internet is first going to be filtered via packet filtering on the border router, and if it is permitted, it will be forwarded to the firewall. The firewall applies its own rules to the traffic and will discard suspicious packets. Traffic is then sent to the interior screening router, and if permitted, is passed to the internal hosts. If traffic were destined to the critical servers – it would have to pass additional screening of host-based intrusion prevention system residing on those servers. In addition to this, network-based IDS, placed at key points on the GIAC network, will help determine whether an internal organization's systems have been compromised, and will provide IT staff with appropriate logging and alerting. These layers will help prevent direct attacks against critical systems that are on internal network, as they would have to pass multiple barriers.

For remote access, GIAC is going to use a stand-alone VPN gateway, which will provide secure connection through the un-secure Internet. From the VPN concentrator, decrypted packets will be forwarded to the firewall where they will be checked against a rule base before passing them to DMZ or Internal network.

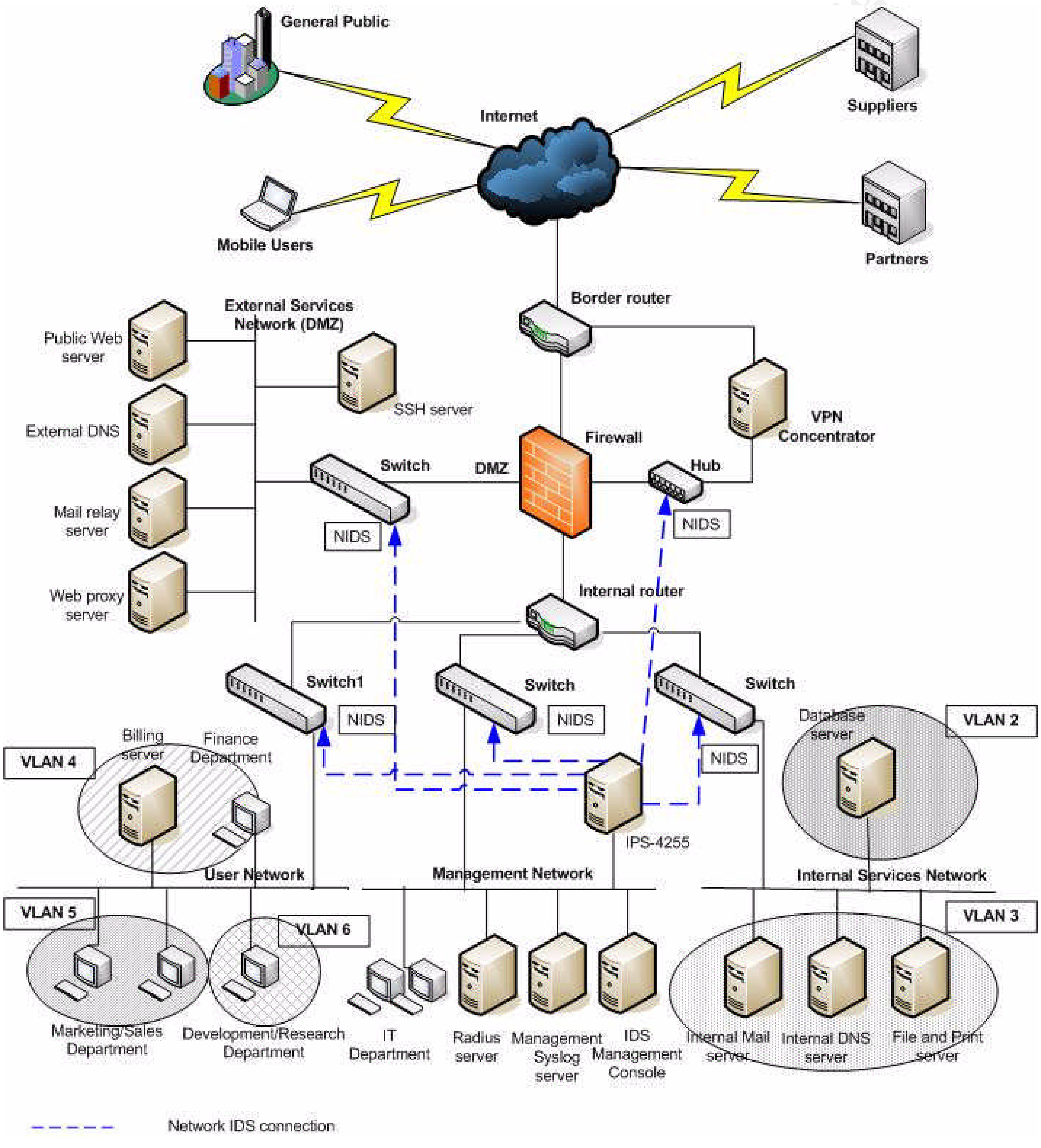
There are additional items that the GIAC IT team implemented that contribute to the layered security principle and will improve overall GIAC security posture:

- Physical security of all critical devices, which includes all networking device and critical servers.
- No dial-up access will be provided.

- Each host has a host-based firewall installed (Kerio) blocking unauthorized access to that host as well as anti-virus software (Sophos).
- All critical servers as well as remote VPN employee users have host based intrusion prevention system installed. Cisco CSA is going to be used.
- New security patches, software upgrades, and service pack releases will be regularly installed - as soon as vendor makes them available – this will mitigate risks associated with known software vulnerabilities.
- At the application layer, the Web proxy server and email relay server provide content filtering of their respective protocols to reduce the risk of malicious code being introduced. GIAC has deployed proxies to deal with both inbound and outbound SMTP and HTTP.
- Logging is configured to take place locally, on the firewall and on the routers, as well as to the central log server. All critical servers and networking devices log to this server. Logs are regularly reviewed.
- Periodic audits of security devices will be performed to verify that security policy is still correctly implemented and there were no unauthorized changes.
- Split DNS infrastructure is implemented where two zones are created for the same domain using separate internal and external name servers. Internal server holds only the DNS records for internal network, and answers only the queries initiated by internal users. Queries that cannot be resolved by the internal server are forwarded to the external name server. External DNS server is configured to contain only a small zone file that lists only publicly accessible resources – public web server and external mail relay server
- Network configuration and management is done by members of the IT team that is connected off Network Management network segment during regular business hours, and through secure VPN connection for after-hours emergencies. They are using CiscoWorks and different SNMP scripts (like MRTG) to control network devices. CiscoWorks is used for configuration archive, configuration change pushes, IOS upgrades, configuration comparison, etc. MRTG (Multi Router Traffic Grapher) is a free tool that is used for displaying router statistics - it monitors the traffic load on router interfaces and other statistics. Both CiscoWorks and MRTG reside on Management/Syslog internal server. All devices are going to be managed either by direct access through console, or by ssh access. Cisco proprietary CDP protocol is going to be enabled locally as it facilitates network troubleshooting and it is also needed for CiscoWorks. SNMP v2 is also needed for CiscoWorks and MRTG.
- RADIUS server does the VPN user authentication and the centralized user ID management. Network devices management access is also controlled using RADIUS protocol.

Even though GIAC IT team realizes importance of redundancy at the network border it is cost prohibitive to implement it today. High level routers with powerful process capabilities and large amount of memory that would be required to handle BGP protocol (needed in cases of dual-homed networks) as well as costs of secondary Internet Service Provider are beyond the network and security architecture budget.

Bellow is the network diagram showing location of all security components. Each component will be discussed in details as important player in overall defense-in-depth schema. IP addressing schema can be found in chapter 2.2.8.



Network Diagram

2.2.2 Border Router

Hardware: Cisco 3725 Multiservice Access Router

Two integrated 10/100 LAN ports

Two Network Module Slots: First slot will be used forT3/E3 Network Module for high-speed WAN access, and second slot will be used for IDS Network Module

Software: Cisco IOS 12.3(10)

Purpose: The main purpose of border router is to connect to the Internet, route traffic between Internet and internal network, and to provide first layer of security through packet filtering.

Security Function: Border router will be used as the first line of defense against hacker's attempts. It will be used for ingress and egress filtering, which will prevent anti-spoofing, and protect against unwanted traffic from entering or leaving our network. Many of the advanced security features that are supported on this router, like TCP intercept and Context-based access control (CBAC) are not going to be implemented at this time because of additional administrative overhead. Reflexive-access lists that are going to provide us with statefull filtering mechanism will be implemented as well as Cisco IOS intrusion detection system by using additional Cisco IDS Network Module.

Placement: Border router is placed at a position to terminate Internet connection and to connect to the firewall. The first fast Ethernet interface (fa0/0) is directly connected to the firewall, while the second LAN interface (fa0/1) is connected to the VPN Gateway.

Discussion: GIAC depends on its Internet Presence and systems that are used to support their online sales demand increased bandwidth. New Network Module T3/E3 that is supported on 3725 provide direct connectivity to a T3 line for full-duplex communication at the rate of 45Mbps while it eliminates the need for an external data service unit (DSU).

Second Network Module slot will be populated with Cisco IDS Network Module that will provide full-featured intrusion protection services within the router. IDS receive copies of packets directly from the router's backplane in a passive mode and then analyze them against a rule set of intrusion activity to identify unauthorized activity. If the captured packets match a defined intrusion pattern, IDS can be configured to either shut down the interface or to send a TCP reset packet to sender to stop session causing the attack. IDS Network module provides up to 45 Mbps throughput.

The Cisco 3725 router delivers the reliability and performance, and the versatility to support new services that the company may deploy in the future, including enhanced voice and video. Also if we need to increase bandwidth in the future, investment in this router would be preserved as it supports ATM OC-3 Network Module, which can add high speed ATM access.

Cisco routers are running Cisco proprietary IOS software that is prone to security problems like other operating systems. Since GIAC owns SMARTnet contract, its IT team can access excellent technical support, as well as IOS patches that Cisco provides to fix security issues. There are several ways of providing system administration access. The most secure ways are to access router directly from the console or authorized users can manage router via SSH. There is also third access option - to telnet to the router, but this require passing of authentication data in clear text over the network. To minimize security risks associated with it – telnet will be disabled.

Cisco proprietary protocol CDP on the outside interface will be disabled and all messages will be logged locally and in a syslog server.

2.2.3 Firewall

Hardware: Cisco PIX 515E
Supports up to six 10/100 Fast Ethernet interfaces
Software: 6.3(3)

Purpose: Firewall plays a vital role in securing GIAC internal network. It also controls and audits traffic flow between different network segments.

Security Function: Firewall is used to enforce access control from customers, suppliers, partners and general public. It will inspect traffic passing through it and allow or deny it based on access control lists. It is also responsible for Network Address Translation (NAT) operation in cases where internal users want to access the Internet. Because of NAT use – the firewall helps hiding GIAC internal network from the Internet, thus providing so called "security by obscurity".

Placement: Firewall is placed in-line, between the border router and the internal network. It has four interfaces. First interface is connected to the border router – public network interface; second is connected to the internal router – private network interface; third connects to the switch of DMZ network; fourth connects to VPN gateway.

Discussion: The reason for choosing PIX over other brands was performance – it delivers up to 188Mbps throughput with the capability to handle more than 130,000 simultaneous sessions [13]. Cisco PIX delivers network defense through the use of stateful inspection (that incorporates Cisco Adaptive Security Algorithm), advanced application and protocol inspection and inline intrusion prevention. It tracks the state of all authorized network communication and evaluates new connection requests based on information contained in dynamic state tables.

The integrated inline intrusion prevention capabilities of the Cisco PIX 515E can protect GIAC Enterprises networks from many popular forms of attacks, including Denial-of-

Service (DoS) attacks and malformed packet attacks. “Using a wealth of advanced intrusion-prevention features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can provide real-time notification to administrators.” [15]
Weaknesses in the firewall usually come from bugs in the firewall software that can introduce vulnerability in firewall implementation of the policy. To mitigate these risks software patches need to be applied as soon as the vendor releases them.
The second problem that can arise with firewall use is configuration errors. Firewalls can be difficult to set up and misconfigurations can leave the network vulnerable. Cisco PIX firewall GUI is not as intuitive as some other firewalls (like CheckPoint), so special attention should be given to the education and technical expertise of the firewall administrator. Firewall misconfiguration can also be somewhat mitigated by testing the rules to be implemented in the initial phase and by regular periodic auditing of rules and access abilities. In the case of firewall misconfiguration, other layers of security in the network will mitigate unwanted access. Border and internal router packet filtering will reduce some attacks, as well as the host security measures such as personal firewall (Kerio), antivirus software (Sophos), and host-based intrusion prevention system (CSA) that will be mandatory for all critical servers.

2.2.4 VPN Gateway

Hardware: Cisco VPN 3020 Concentrator
Supports three 10/100 Fast Ethernet interfaces
Software: 4.1.7.D

Purpose: It acts as the termination point for VPN connections.

Security Function: VPN Concentrator performs an essential business need as it provides secure channel for data that is passing through un-trusted public Internet. It does that by establishing encrypted tunnel for communication between the remote clients and itself, therefore allowing remote clients to securely access services on GIAC network. It is also a point of authentication for connections coming from partners, suppliers, regional offices, and mobile users. Only after successful authentication encrypted channel is established.

Placement: External interface of VPN gateway is connected to the border router, while internal interface is connected to the firewall, which gives the ability for decrypted traffic to be monitored and restricted in entering internal network. Beside improved access control for remote users this configuration also gives a better logging capability.

Discussion: Even though our border router has capability to support a VPN module, we decided to go with separate piece of hardware as a VPN gateway. This way we are not going to task the router with extra load that comes with the encrypting and decrypting process. The router is not going to be affected with possible exploits related with VPN

functionality. Cisco VPN 3020 was chosen because it supports T3/E3 bandwidth (50Mbps performance), up to 750 simultaneous IPSec sessions, and a maximum of 200 LAN-to-LAN sessions that is not only enough for current GIAC needs, but will allow for future growth as well. Cisco VPN 3020 is also the lowest model in 3000 VPN series that supports hardware-based encryption.
Cisco VPN Concentrator supports RADIUS authentication mechanisms and is configured to forward all authentication requests to a RADIUS server located on Management network segment. Once authenticated successfully, remote users will have appropriate access to either DMZ and/or internal resources. Additionally, dynamic access control lists (ACLs) can be applied to all remote user sessions, and based upon their rules, can permit or deny user access to specific networks, subnets, hosts, and applications.

Each mobile employee has been given a company purchased laptop that is setup by the system administrator. GIAC Enterprises has a Cisco SMARTnet support contract and may download Cisco VPN Client from Cisco web site at no additional cost. Cisco Systems VPN Client software version 4.6 is installed on remote users laptops and preconfigured with appropriate connection profiles by the administrator, so that they can connect to a VPN gateway at the main office through their ISP. As noted before, there are couple of different groups that are connecting to VPN Concentrator. VPN Administrator will create separate user profile configuration file (.pcf file) for each group that includes parameters like: what authentication to be used, IPSec group name and password, use of a log file, etc. A different pool of IP addresses and access restrictions are placed on each of these connection profiles based on these addresses.

In addition to providing secure channels of communication, VPN enables GIAC to reduce communication expenses to their remote offices by using the local connection infrastructure of Internet Service Providers.

The main disadvantage of VPN services is that once a tunnel has been established, it practically extends corporate network perimeter to the remote VPN users systems. The corporate network becomes as secure as the laptops and PCs connected to it. These laptops are connected to the Internet through their own ISP and exposed to the vulnerabilities coming from it without the protection of the corporate secure perimeter. Having multilayer security approach in mind, GIAC will implement different desktop security products that will provide a significantly higher level of protection against today's complex threats. Therefore, GIAC is mandating complementary host security measures, such as personal firewall (Kerio), antivirus software (Sophos), and host-based intrusion prevention system (CSA) for all remote employees that are using VPN services.

2.2.5 Network based IDS

Hardware: Cisco IPS-4255
Four built-in 10/100/1000 copper sniffing interfaces

Four additional optional 10/100/1000 TX interfaces – allowing a total of 8 monitoring interfaces

Software: 4.1

Purpose: Network Intrusion Detection System (IDS) provides detection of malicious activity and alerting for monitored network segments.

Security Function: NIDS will compare all packets against its signature base, and log and send the alert to IDS Manager. Network-based IDS perform a rule-based analysis of traffic using parameters set up by the security administrator, and the signatures, which detects suspicious activity. The systems analyze network packet headers to make security decisions based on source, destination, and packet type. They also analyze packet data to make decisions based on the actual data being transmitted. In addition, sensors placed on the different network segments can be configured to report back to a central site.

Placement: IPS-4255 has 8 monitoring interfaces and one command or controlling interface that communicates with the IDS manager. The monitoring interfaces are connected to DMZ segment, VPN segment, and all internal network segments. Since these segments are switched, monitoring interface will be connected to a switch's Switched Port Analyzer (SPAN) port. VPN internal segment (interface that connects VPN to firewall) does not have a switch so we are going to place dumb hub to connect to the IDS monitoring interface – this way all VPN traffic coming from remote users will be monitored. The monitoring interfaces are in promiscuous mode, which means that they do not have IP addresses and are not visible on the monitored segments. The appliance itself is going to be connected with its control interface on Management segment and will have IP address to communicate with IDS manager located on the same segment.

Discussion: IPS-4255 can monitor up to 600 Mbps of aggregate network traffic on multiple sniffing interfaces. By using IPS-4255 GIAC is going the minimize the total cost of ownership as it has ability to simultaneously monitor multiple network segments through support for multiple sniffing interfaces, effectively delivering up to 8 sensors in one. Cisco labeled this appliance Intrusion Prevention System (IPS) meaning that we can configure it to respond to preconfigured signatures. "These responses include logging the event, forwarding the event to the IDS manager, performing a TCP reset, generation an IP log, capturing the alert trigger packet, and/or reconfiguring a router."[16] Intrusion detection system complement the systems deployed in network perimeter security by detecting attempts to exploit service vulnerabilities and by identifying misconfiguration in the firewall and packet filtering routers, thus significantly enhancing GIAC's security posture. Furthermore, firewall and border router will not protect corporate network against attacks originating from inside. NIDS is deployed to monitor activity at key points in the internal network.

IDS Manger is a web-based application that allows for managing and configuration of IDS sensor (IPS-4255). IDS Manager (IDM) is where network alerts are processed and reports are generated.

Maintenance and configuration errors are probably the biggest threat for network based IDS. Configuration tweaking is required to reduce initial high number of false positives and is prone to mistakes. The effectiveness of the IDS depends heavily on up to date signatures. If there is a new type of attack and NIDS has no signature for it, it will not recognize attack. New release signatures must be uploaded on a regular basis.

2.2.6 Internal Router

Hardware: Cisco 3745 Router
Two integrated 10/100 LAN ports
Four Network Module Slots: First 2 slot will be used for One-port Fast Ethernet interfaces network module (NM-1FE-TX)

Software: Cisco IOS 12.3(10)

Purpose: route packets between different internal LAN segments and provide uplink to the firewall for external connectivity. It provides inter-VLAN routing services between VLANs (Virtual LAN) configured on Catalyst 3550 switches.

Security Function: It isolates network management and data network from the general corporate LAN and using a combination of extended access lists and reflexive access lists controls communication between different parts of internal network thus providing an additional protection of the servers on Internal Services Network.

Placement: It is placed between the firewall and internal switches.

Discussion: Cisco 3745 router belongs to the same 3700 series of routers as 3725 Router. We chose 3745 because it is highly modular and since it can share Network Modules with 3725 it makes a very cost effective solution. Like 3725, it is designed to meet evolving needs in the future by supporting multiservice integration of voice, video, and data. For example, with support of in-line power option of 16-port 10/100 EtherSwitch network module, it can be used to power Cisco IP phones. Platform performance was also primary concern, as GIAC wanted a solution that can provide the connectivity for multiple LAN segment at full wire speed – 3745 has high performance of 225 Kpps. 3745 is chosen over 3725 so that we can have 2 empty Network Module slots that will allow for future growth.
As with 3725 possible security weaknesses are the IOS bugs and software needs to be regularly updated.

2.2.7 Internal Switches

Hardware: Cisco Catalyst 3550-24 and 3550-24 PWR

Software: 12.2(25)SE

Purpose: Provides multiple, high-speed layer 2 data exchanges between devices on the same segment. It helps containing broadcasts by implementing VLANs.

Security Function: Enhances network security by means of logical segmentation of users and groups (creating VLANs) that effectively disables communication between different VLAns on the same physical segment, unless a layer 3 device, such as router, is used. With these switches GIAC can implement port security, where the MAC address of each device connecting to the switch is hardcoded into the switch itself and no other devices can connect to the network from that port. Port monitoring or so-called SPAN (Switched Port Analyzer) feature of the switches allows network traffic from selected interfaces to be analyzed by IDS. Also network sniffing is eliminated in switched environment.

Placement: Switches are placed on different segments of the GIAC network. One (3550-24) is placed off of the firewall, on the DMZ zone to provide connectivity to the public servers. Other three are placed off internal router to provide connectivity to the Internal network segments: User Networks (stack of two 3550-24 PWR), Management Network (3550-24 PWR), and Internal Services Network (3550-24).

Discussion: Catalyst 3550-24 switches are multilayer switches that, with the EMI (Enhanced Standard Multilayer Software Image) version of the code, have a possibility to provide routing and security access control lists. As with Cisco 3725 and 3745 routers, these switches are chosen because they are ideal for integrated voice, video and data application, that GIAC might need in the future. 3550-24 PWR provide security, quality of service (QoS), and have integrated inline power that can power Cisco IP phones thus providing support for IP telephony that GIAC is considering implementing in future.
As with all Cisco equipment, Catalyst switches are running proprietary IOS software that occasionally has security problems, and vendor provided IOS patches need to be regularly installed.

2.2.8 IP addressing schema

GIAC's assigned public address space is a class C network 30.1.1.0/24. This network will be divided into several smaller networks (subnets). Internally, GIAC is using non-routable addresses in 10.80.0.0/16 space. For internal users to connect to the Internet, their private addresses needs to be translated into assigned public address space. This translation is called Network Address Translation (NAT) and it is performed by PIX firewall. GIAC is also going to use NAT to offer publicly available services from private address space that is going to use on the servers in the DMZ. Bellow are tables that are detailing IP address assignments for internal and external network as well as addresses assigned to specific servers.

External networks	Network/IP Addresses
ISP assigned Link connection	105.10.10.0/30
ISP router interface	105.10.10.1/30
Border router external interface	105.10.10.2/30
Border router to firewall network segment	30.1.1.0/30

Border router internal interface	30.1.1.1/30	
Firewall external (public) interface	30.1.1.2/30	
VPN public segment	30.1.1.4/30	
Border router interface to VPN	30.1.1.5/30	
VPN external interface to border router	30.1.1.6/30	
DMZ servers NAT pool (static)	30.1.1.96/27	
Internal users NAT pool (dynamic)	30.1.1.128/25	
Internal networks	Network/IP Addresses (Private)	Translated IP Addresses (Public)
VPN private segment	10.80.220.0/30	
VPN internal interface to firewall	10.80.220.1/30	
Firewall interface to VPN	10.80.220.2/30	
VPN outside customers - pool A	10.80.250.0/25	
VPN GIAC remote users - pool B	10.80.250.128/26	
VPN GIAC remote admins - pool C	10.80.250.192/26	
Firewall internal (private) interface to Internal router	10.80.200.0/30	
Firewall internal (private) interface	10.80.200.1/30	
Internal router external interface	10.80.200.2/30	
Management network	10.80.50.0/24	
IDS Management Console	10.80.50.2/24	
IPS-4255	10.80.50.3/24	
Management/Syslog server	10.80.50.4/24	
Radius server	10.80.50.5/24	
User network: Finance Dep. (VLAN 4) Marketing/Sales Dep. (VLAN 5) Development/Research Dep. (VLAN 6)	 10.80.10.0/24 10.80.20.0/24 10.80.30.0/24	
Billing server	10.80.10.2/24	
Internal Services Network: Database network (VLAN 2) Servers Network (VLAN 3)	 10.80.70.0/24 10.80.80.0/24	
Database server	10.80.70.2/24	
File and Print server	10.80.80.2/24	
Internal DNS server	10.80.80.3/24	
Internal Mail server	10.80.80.4/24	
External Services network (DMZ)	10.80.230.0/24	
Public Web server	10.80.230.2/24	30.1.1.98/27
SSH server	10.80.230.3/24	30.1.1.99/27
External DNS server	10.80.230.4/24	30.1.1.100/27
Mail relay server	10.80.230.5/24	30.1.1.101/27
Web proxy server	10.80.230.6/24	30.1.1.102/27

Assignment 3: Router and Firewall Policies

3.1 Border router policy

As we said before border router is the first line of defense against attacks in multilayered security approach that GIAC has adopted. Its primary function is protecting itself and the rest of security perimeter against possible intrusions, by filtering unwanted traffic. IT team will take extra precaution to harden it properly so that it does not get compromised.

Access control lists (ACLs) are used to filter traffic based on various criteria. A Cisco router supports many different types of access control lists –the most popular ones being: standard, extended, and reflexive. GIAC IT team has decided to use reflexive access list on a border router. Reflexive access lists implement a stateful packet filtering capability, which means that the information on each connection is stored in a table and new packets are checked against that table to verify if they are part of existing connection. Access lists are applied to specific interface in inbound (traffic coming into the router) or outbound direction (traffic leaving the router). An important consideration when building access list on the router is the order of processing. Rules are processed in a top-down fashion and processing stops when first match is found. Therefore, placing most frequently used rules at the top of the access list can help speed up the performance of the router. Also if there are specific rules that are exception to the general rule, they should be placed earlier in the configuration. Another important point regarding Cisco router access lists is that there is implicit deny on the end – effectively meaning, “all that is not expressly permitted is prohibited”.

Bellow we will first detail how to protect the router itself from being compromised, by disabling features and services that are not needed on both a global and interface level. Then we present inbound and outbound ACLs that will filter unneeded traffic heading for GIAC internal network.

3.1.1 Router hardening

Command	Comments
Global configuration	
no service tcp-small-servers	Disable TCP services such as Echo and Chargen that can be used for a DOS
no service udp-small-servers	Disable similar UDP services

no ip source routing	Disable packet specified routes or so-called source routing
no ip domain lookup	
no service finger	Disable finger requests that gives information on who is logged
no ip http server	Disable web-based access to the router
no ip bootp server	Disable bootp server functionality
no enable password	Disable clear text password in configuration file – use enable secret instead
Interface configuration	
no ip unreachables	Disable ICMP packets used to notify sender of incorrect address, can be used for network mapping
no ip redirects	Disable ICMP redirects
no ip directed-broadcast	Disable sending packets to all hosts on the network, can be used for smurf attack
no ip proxy-arp	Disable router to act as a proxy for layer 2 address resolution
no ip mask-reply	Disable sending of ICMP mask replay messages
no cdp enable	Disable CDP on external interface of border router

There are also some features that we want to enable to provide for better security and functionality, as shown bellow:

Setting proper debug timestamps

```
service timestamps debug datetime localtime
service timestamps log datetime localtime
```

Encrypt all clear text passwords in configuration except SNMP community strings

```
service password-encryption
```

Set the name of the router and assign domain name

```
hostname Border-Router
ip domain-name giac.com
```

Configure required Radius authentication and authorization for users

```
aaa new-model
aaa authentication login default group radius
aaa authentication enable default group radius
aaa authorization exec default group radius if-authenticated
aaa authorization commands 1 default group radius if-authenticated
```

Configure Radius server

```
radius-server host 10.80.50.5
radius-server key Rad1usServerKey
```

Configure password for privileged access – use instead ‘enable password’ command

```
enable secret 123SecreT
```

set router timezone

```
clock timezone MST -7
```

Send logs to Syslog server

```
logging 10.80.50.4
logging trap informational
logging facility local0
```

Sync to the Stratum 1 clock at Palo Alto, CA, and Pasadena, CA, respectively

```
ntp server 204.123.2.5
ntp server 192.12.19.20
```

Enable SNMP communication and sending of traps to Management Server

```
snmp-server community SpeciaLROSnmp RO 95
snmp-server community SpeciaLRWSnmp RW 95
snmp-server enable traps snmp
snmp-server enable traps config
snmp-server host 10.80.50.4 traps version 2c SpeciaLROSnmp
```

Restrict SNMP access to Management Server only

```
access-list 95 permit host 10.80.50.4
access-list 95 deny any log
```

Secure console access with password and 15 min terminal timeout

```
line con 0
 exec-timeout 15 0
 password SecureConsolePassword
```

Enable only ssh connection and set the password to VTY line

```
line vty 0 4
 exec-timeout 15 0
 password SecureSSHPassword
 transport input ssh
```

To enable the SSH server key needs to be generated

```
crypto key generate rsa
```

3.1.2 Inbound border router access list

```
ip access-list extended border-router-in
```

Deny RFC 1918 addresses

```
deny ip 192.168.0.0 0.0.255.255 any
deny ip 172.16.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.255.255.255 any
```

Deny packets with localhost and multicast addresses

```
deny ip 127.0.0.0 0.255.255.255 any
deny ip 224.0.0.0 15.255.255.255 any
```

Deny unsigned IP addresses – list of those can be found at the Internet Assigned Names Association (IANA) http://www.iana.org/assignments/ipv4-address-space.

```
deny ip 0.0.0.0 0.255.255.255 any
deny ip 1.0.0.0 0.255.255.255 any
…..
…..
deny ip 255.0.0.0 0.255.255.255 any
```

```
Deny all ICMP requests, ICMP replies will be passed with reflexive rule
deny icmp any any

Prevent spoofing – deny IP packets that have our publicly assigned IP addresses
deny ip 30.1.1.0 0.0.0.255 any
deny ip host 105.10.10.2

Permit HTTP and HTTPS access to Public web server
permit tcp any host 30.1.1.98 eq 80 log
permit tcp any host 30.1.1.98 eq 443 log

Permit DNS queries to external DNS server
permit udp any host 30.1.1.100 eq 53 log
Permit email (SMTP) traffic to mail relay
permit tcp any host 30.1.1.101 eq 25 log

Permit IPSec traffic to VPN Concentrator
permit 50 any host 30.1.1.6 log
permit 51 any host 30.1.1.6 log
permit udp any host 30.1.1.6 eq 500 log

Permit from inside established connection
evaluate border-router-reflexive

Deny everything else
deny ip any any
```

Inbound access list will be applied on external serial interface that is connecting border router to the ISP. Following command should be used on Cisco Routers:

```
ip access-group border-router-in in
```

3.1.3 Outbound border router access list

```
ip access-list extended border-router-out
Deny internal addresses as destination addresses
deny ip any 30.1.1.0 0.0.0.255

Deny RFC 1918 addresses
deny ip 192.168.0.0 0.0.255.255 any
deny ip 172.16.0.0 0.0.255.255 any
deny ip 10.0.0.0 0.255.255.255 any

Deny packets with localhost and multicast addresses
deny ip 127.0.0.0 0.255.255.255 any
deny ip 224.0.0.0 15.255.255.255 any

Permit IPSec traffic from VPN Concentrator
permit 50 host 30.1.1.6 any log
permit 51 host 30.1.1.6 any log
permit udp host 30.1.1.6 any eq 500 log

Permit outbound connection from GIAC internal network
permit ip 30.1.1.0 0.0.0.255 any reflect border-router-reflexive log

Permit outbound connection from border router to the two Stratum 1 clocks – allow ntp traffic
permit udp host 105.10.10.2 host 204.123.2.5 eq 123 reflect border-router-reflexive log
permit udp host 105.10.10.2 host 192.12.19.20 eq 123 reflect border-router-reflexive log

Deny everything else
deny ip any any
```

Outbound access list will be applied on external serial interface that is connecting border router to the ISP. Following command should be used on Cisco Routers:

```
ip access-group border-router-out out
```

3.2 Firewall policy

Firewall is the primary line of defense in GIAC's new security architecture. It provides blocking of any harmful traffic that was missed by the border router, and access control between different segments, including access control for decrypted traffic coming from VPN concentrator. It is also a NAT'ing device that maps internal private IP addresses to the publicly routed addresses.

The PIX firewall will be configured with 4 interfaces. Each interface is assigned a number between 0 and 100, which correspond to the different security level (lowest to highest). The security level is the level at which interface will be "trusted", generally the inside interface is configured with Secuirty100 (trusted), and the outside with Secuirty0 (not trusted). Traffic from higher to lower security level is permitted, by default. Once a connection has been initiated from the high to low security interface, the return traffic will be permitted by the stateful functionality. Stateful inspection is used to verify that incoming packets are legitimate responses based on previously established connection table. Communication from a low to high security interface is denied, by default, unless access lists explicitly permit it. Like a router, rules in an access list are evaluated in sequential order, top to bottom, and once a matching rule is found for a particular packet, the action assigned to that rule is applied to the packet and processing stops. Consequently, like with router, ordering of rules is important and most commonly matched rules should be placed on the top of the access list. Firewall configuration philosophy is also same as for the router – block everything unless explicitly permitted.

What is different for access lists on the firewall though is that they are only applied inbound on PIX interfaces.

Since GIAC has private addresses deployed in their network, they are going to use the PIX firewall to translate these addresses to public address space. Static translation, where an administrator manually maps single private address to another public, is going to be used for public servers that need to be reached by external users from Internet. For internal users, dynamic translation is going to be used, where a pool of public IP addresses is created and the PIX is randomly going to assign public addresses to the devices needing to connect to the Internet [17].

Naming the interfaces and assigning the appropriate security level

```
nameif ethernet0 outside security0
nameif ethernet1 dmz security50
nameif ethernet2 vpn security70
nameif ethernet3 inside security100
```

Assign the passwords and hostfile

```
enable password BigFirewallPassword encrypted
password SmallFirewallPassword encrypted
hostname pixfirewall
```

Add application layer protection for http, dns, and smtp

```
fixup protocol http 80
fixup protocol smtp 25
fixup protocol domain 53
```

Dynamic translation for internal uses with NAT pool defined

```
global (outside) 1 30.1.1.128 netmask 255.255.255.128
nat (inside) 1 10.80.0.0 255.255.0.0
```

Static translation for publicly accessible servers

```
static (dmz, outside) 30.1.1.98 10.80.230.2
static (dmz, outside) 30.1.1.100 10.80.230.4
static (dmz, outside) 30.1.1.101 10.80.230.5
static (dmz, outside) 30.1.1.102 10.80.230.6
```

Disable translation between dmz and inside interfaces

```
static (inside, dmz) 10.80.230.0 10.80.230.0 netmask 255.255.255.0
access-list no_nat permit ip 10.80.10.0 255.255.255.0 10.80.230.0 255.255.255.0
access-list no_nat permit ip 10.80.20.0 255.255.255.0 10.80.230.0 255.255.255.0
access-list no_nat permit ip 10.80.30.0 255.255.255.0 10.80.230.0 255.255.255.0
access-list no_nat permit ip 10.80.50.0 255.255.255.0 10.80.230.0 255.255.255.0
access-list no_nat permit ip 10.80.70.0 255.255.255.0 10.80.230.0 255.255.255.0
access-list no_nat permit ip 10.80.80.0 255.255.255.0 10.80.230.0 255.255.255.0
access-list no_nat permit ip 10.80.250.0 255.255.255.0 10.80.230.0 255.255.255.0
nat (inside) 0 access-list no_nat
```

3.2.1 Outside – ethernet0 interface access list

Permit HTTP,HTTPS access from Internet to public web server

```
access-list acl_outside permit tcp any host 30.1.1.98 eq 80
access-list acl_outside permit tcp any host 30.1.1.98 eq 443
```

Permit DNS queries from Internet

```
access-list acl_outside permit udp any host 30.1.1.100 eq 53
```

Permit SMTP from Internet to the public mail relay server

```
access-list acl_outside permit tcp any host 30.1.1.101 eq 25
```

Permit HTTP replies to the web proxy

```
access-list acl_outside permit tcp any eq 80 host 30.1.1.102
```

Permit border router logging to Syslog server

```
access-list acl_outside permit udp host 30.1.1.1 host 10.80.50.4 eq 514
```

Permit border router NTP replies to the internal network

```
access-list acl_outside permit udp host 30.1.1.1 eq 123 10.80.0.0 255.255.0.0
```

Permit RADIUS for access authentication to the border router

```
access-list acl_outside permit udp host 30.1.1.1 host 10.80.50.5 eq 1645
```

Permit sending of SNMP traps to Management Server

```
access-list acl_outside permit udp host 30.1.1.1 host 10.80.50.4 eq 162
```

Deny everything else

```
access-list acl_outside deny ip any any
```

Outbound access list will be applied on outside interface (ethernet0) that is connecting firewall to the border router. Following command should be used

```
access-group acl_outside in interface outside
```

3.2.2 DMZ – ethernet1 interface access list

Permit HTTP,HTTPS from public web server

```
access-list acl_dmz permit tcp host 10.80.230.2 eq 80 any
access-list acl_dmz permit tcp host 10.80.230.2 eq 443 any
```

Permit ssh communication from SSH server

```
access-list acl_dmz permit tcp host 10.80.230.3 eq 22 10.80.0.0 255.255.0.0
```

Permit ssh communication from SSH server to 2 different partners

```
access-list acl_dmz permit tcp host 10.80.230.3 eq 22 host 180.1.1.1
access-list acl_dmz permit tcp host 10.80.230.3 eq 22 host 210.2.2.2
```

Permit custom built application from SSH and HTTPS server to database

```
access-list acl_dmz permit tcp host 10.80.230.2 host 10.80.70.2 eq 5577
access-list acl_dmz permit tcp host 10.80.230.3 host 10.80.70.2 eq 5577
```

Permit DNS replies and queries from external DNS server

```
access-list acl_dmz permit udp host 10.80.230.4 eq 53 any
access-list acl_dmz permit udp host 10.80.230.4 any eq 53
```

Permit SMTP from public mail relay server

```
access-list acl_dmz permit tcp host 10.80.230.5 any eq 25
```

Permit HTTP from web proxy

```
access-list acl_dmz permit tcp host 10.80.230.6 any eq 80
access-list acl_dmz permit tcp host 10.80.230.6 eq 8080 10.80.0.0 255.255.0.0
```

Permit syslog traffic from public servers to the Syslog host

```
access-list acl_dmz permit udp 10.80.230.0 255.255.255.0 host 10.80.50.4 eq 514
```

Permit NTP traffic from public servers to our border router that is serving as NTP server

```
access-list acl_dmz permit udp 10.80.230.0 255.255.255.0 host 30.1.1.1 eq 123
```

Permit RADIUS authentication

```
access-list acl_dmz permit udp 10.80.230.0 255.255.255.0 host 10.80.50.5 eq 1645
```

Permit sending of SNMP traps to Management Server

```
access-list acl_dmz permit udp 10.80.230.0 255.255.255.0 host 10.80.50.4 eq 162
```

Deny everything else

```
access-list acl_dmz deny ip any any
```

DMZ access list will be applied on dmz interface (ethernet1) that is connecting firewall to switch on External Services Nettwork. Following command should be used

```
access-group acl_dmz in interface dmz
```

3.2.3 VPN – ethernet2 interface access list

Permit ssh communication to SSH server from VPN pools and 2 different partners

```
access-list acl_vpn permit tcp 10.80.250.0 255.255.255.0 host 10.80.230.3 eq 22
access-list acl_vpn permit tcp host 180.1.1.1 host 10.80.230.3 eq 22
access-list acl_vpn permit tcp host 210.2.2.2 host 10.80.230.3 eq 22
```

Permit VPN GIAC's remote users and remote administrators to Internal Services Network

```
access-list acl_vpn permit tcp 10.80.250.128 255.255.255.192 host 10.80.70.2 eq 1433
access-list acl_vpn permit tcp 10.80.250.192 255.255.255.192 host 10.80.70.2 eq 1433
access-list acl_vpn permit ip 10.80.250.128 255.255.255.192 10.80.80.0 255.255.255.0
access-list acl_vpn permit ip 10.80.250.192 255.255.255.192 10.80.80.0 255.255.255.0
```

Permit VPN GIAC's remote administrators to Management Network

```
access-list acl_vpn permit ip 10.80.250.192 255.255.255.192 10.80.50.0 255.255.255.0
```

Permit syslog traffic from VPN concentrator to the Syslog host

```
access-list acl_vpn permit udp host 10.80.220.1 host 10.80.50.4 eq 514
```

Permit NTP traffic from VPN concentrator to our border router that is serving as NTP server

```
access-list acl_vpn permit udp host 10.80.220.1 host 30.1.1.1 eq 123
```

Permit RADIUS authentication

```
access-list acl_vpn permit udp host 10.80.220.1 host 10.80.50.5 eq 1645
```

Permit sending of SNMP traps to Management Server

```
access-list acl_vpn permit udp host 10.80.220.1 host 10.80.50.4 eq 162
```

Deny everything else

```
access-list acl_vpn deny ip any any
```

VPN access list will be applied on vpn interface (ethernet2) that is connecting firewall to VPN concentrator. Following command should be used

```
access-group acl_vpn in interface vpn
```

3.2.4 Inside – ethernet3 interface access list

Permit Internet access for all company employees

```
access-list acl_inside permit tcp 10.80.0.0 255.255.0.0 host 10.80.230.6 eq 8080
```

Permit web access to company's public web server

```
access-list acl_inside permit tcp 10.80.0.0 255.255.0.0 host 10.80.230.2 eq 80
access-list acl_inside permit tcp 10.80.0.0 255.255.0.0 host 10.80.230.2 eq 443
```

Internal users access to the SSH server

```
access-list acl_inside permit tcp 10.80.0.0 255.255.0.0 host 10.80.230.3 eq 22
```

GIAC IT team access for device management

```
access-list acl_inside permit tcp 10.80.50.0 255.255.0.0 10.80.230.0 255.255.255.0 eq 22
access-list acl_inside permit tcp 10.80.50.0 255.255.0.0 host 10.80.220.1 eq 22
access-list acl_inside permit tcp 10.80.50.0 255.255.0.0 host 30.1.1.1 eq 22
```

Management Server SNMP access for managing devices

```
access-list acl_inside permit udp host 10.80.50.4 10.80.230.0 255.255.255.0 eq 161
access-list acl_inside permit udp host 10.80.50.4 host 10.80.220.1 eq 161
access-list acl_inside permit udp host 10.80.50.4 host 30.1.1.1 eq 161
```

Inside access list will be applied on inside interface (ethernet3) that is connecting firewall to internal network. Following command should be used

```
access-group acl_inside in interface inside
```

References

[1] "Symantec Latest Internet Security Threat Report Findings" http://www.symantec.com/press/2004/n040922.html

[2] Sans Institute http://www.sans.org/resources/idfaq/layered_defense.php

[3] E. Carter, "Intrusion Detection Systems," Cisco Press http://www.ciscopress.com/articles

[4] "Intrusion Prevention Systems: deciphering the inline Intrusion prevention hype, and working toward a real-world, proactive security solution" http://www.secuirecomputing.com

[5] "Intrusion Prevention Systems (IPS) http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm

[6] Trusted Operating Systems: The Ultimate Defense http://www.computerworld.com/securitytopics/security/story/0,10801,53293,00.html

[7] Prescatore, J. "Enterprise Security Moves Towards Intrusion Prevention" http://www.csoonline.com/analyst/report1771.html

[8] Intrusion Prevention Systems (IPS) http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=http%3A%2F%2Fhosteddocs%2Eittoolbox%2Ecom%2FBW013004%2Epdf

[9] Oganesyan, A. “Corporate Secuirity” http://security.ittoolbox.com/documents/document.asp?i=3363

[10] “A New Approach To Intrusion Detection: Intrusion Prevention” http://cnscenter.future.co.kr/resource/security/ids/IDSWhitePaper.pdf

[11] “Massive proliferation of client-side attacks shift focus from Net server security” http://www.infoworld.com/articles/op/xml/00/07/17/000717opswatch.html

[12] “Defense in Depth” http://nsa1.www.conxion.com/support/guides/sd-1.pdf

[13] “Cisco PIX 515E Firewall” http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/ps4094/index.html

[14] Spenneberg, R. “IPSec HOWTO” http://www.ipsec-howto.org/ipsec-howto.pdf

[15] “Cisco PIX Security Appliance Software Version 6.3” http://www.cisco.com/en/US/customer/products/hw/vpndevc/ps2030/products_data_sheet09186a0080148714.html

[16] “Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide version 4.1” http://www.cisco.com/en/US/customer/products/sw/secursw/ps2113/products_installation_and_configuration_guide_chapter09186a0080358053.html#wp479565

[17] Deal, R. “Cisco PIX Firewalls”