Global Information Assurance Certification Paper

Summary of Contents

Table of Contents

Abstract

This document is a requirement for the GIAC Firewall Analyst certification version 3.0. It discusses the network security architecture of a fictitious company called GIAC Enterprise, which is an online company that sells fortune cookie sayings online. The document is broken up into 3 sections.

Section 1 discusses the future of technology and covers the Intrusion Prevention system, which was taken from the wishlist that is located at www.giac.org/GCFW_wishlist.php. Although IPS are not widely deployed, current trends show that the use of IPS's will increase. Most IPSs integrate current technologies in order to accomplish their functions. We will discuss this further later in the paper.

Section 2 covers the GIAC Security Architecture, which takes into consideration the business requirements of GIAC Enterprises. This will be discussion of border routers, firewall rules, Single Sign On services and IDS configuration. The access-list and configuration files can be found in the appendix.

Section 3 concludes the paper and covers the GIAC Security Policy for the security architecture that was suggested in Section 2. The details and reasons for the firewall and perimeter router rules will be discussed in this section.

Introduction

GIAC Enterprises is an online company that sells fortune cookie sayings online. Thus, all of GIAC Enterprises' income is generated online. GIAC Enterprises also has partner, suppliers and customers with special requirements that need controlled access to their internal database in order to add, translate or purchase fortune cookie sayings. Access must also be provided for GIAC's internal employees and mobile users. In addition to defense in-depth, since GIACs income is generated online, therefore their network must be designed with failover mechanisms for critical services such as web services and network access. In order to facilitate convenient access to their employees, partners and suppliers, GIAC will use a single sign-on solution for their web services. The benefits of a single sign-on solution is that there will be a better user experience for GIAC employees, partners and customers and and secondly, less maintenance for GIACs technical team and therefore not prone to error. For example, if a partner or supplier happens to lost their password token, it will not be difficult for GIACs technical staff to reset his/her credentials.

These companies face a host of security challenges ranging from viruses, worms, Trojans, Bots, denial of service attacks, intrusions and other types of nefarious activities. According to the CSI/FBI Survey the cost of virus/worm attacks have increased by 54 million dollars from last year. The Sobig virus accounted for 29.7 billion in economic damage worldwide. These threats are increasing and trends show that they are becoming even more sophisticated. According to a survey done by Symantec, there are at least 100 new viruses/worms released everyday. This makes it an immense challenge for security personnel to keep up with this volume of attacks. The nature of some of these new viruses and worms are also more disturbing. Some viruses and worms now come with keyboard loggers, password grabbers and a host of other payloads that relates to identity theft and credit card information gathering. The way in which these viruses and worms spread is more sophisticated, using propagation techniques ranging from buffer overflows such as the one found in the RPC protocol found in many versions of the Windows such as Windows 2000, XP and 2003 operating systems. Any unpatched machines running this service was vulnerable to the Welchia and Gaobot worms. and javascript exploits such as the Microsoft IIS vulnerability

1.1 What is an IPS

An IPS can be either host based (hips) or network based (nips). The focus of this whitepaper is on network intrusion prevention. An IPS can be hardware based or software based and is used to enhance security by denying traffic or send alerts based on criterion configured by the security administrator. Like an IDS, IPS systems are either deployed inline with the network, using a network tap or a configuring a SPAN port on a switch. The reason that these devices need this peculiar connection is because in a switched environment even if a NIC is in promiscuous mode, the packets from a sending computer will go only to the port of the receiving computer thus only that computer will see this traffic. In an inline deployment, the IPS has the ability to view bi-directional traffic. IPS's analyze traffic in going in both direction's and to make intelligent analysis according to configured parameters. Some of the most recognized techniques are flow analysis, heuristics and packet analysis.

1.2 Flow Based.

In a flow based IPS, the device is first placed in learning mode, where it defines a baseline for normal network activity. After creating the baseline for normal network activity, anomaly detection protocol can be applied against this baseline in order to determine when unusual network traffic is taking place and the appropriate actions can be taken that was pre-configured by the security administrator. For example, he or she could configure the IPS to send an alarm if worm traffic, network reconnaissance or a bruteforce attack is identified coming from an internal or external host. It is also possible to block this traffic if deemed necessary. Another benefit of flow based IPS is that it can perform rate limiting, which can be useful in the case of a DDOS or a SYN flood. SYN flood protection can be accomplished by using a SYN-Proxy, which ensures that proper protocol rules are followed by the sending hosts, while protecting itself from being overwhelmed by the SYN flood. Performing TCP protocol analysis ensures that the three-way handshake took place before forwarding the connection to the receiving host and to time out incomplete connections quickly. SYN flood protection can also be achieved by setting a threshold, for example to turn on rate limiting if more than 100 SYN packets per second is being received from the same host or network. Not having this capability can also be detrimental in environments that must maintain a bandwidth availability that is enforced by Service Level Agreement.

1.3 Content Based.

Content-based IPS compares all packets to a database of known attack signatures. In some IPS devices, you have the ability to create custom signatures. Two that come to mind are SnortInline and Cisco IDS. The technology is quite similar to IDS systems as they typically sniff network traffic and compare each packet to their attack signature database. The difference is that if an attack is detected, the IPS can respond not only by sending an alert to the security personnel but it can also reset or drop the connection and even block all further traffic from the attacking host. Some IPS also employs heuristics that allow them to make intelligent decisions based on protocol analysis. This

type of scanning can be taxing to performance and efficient hardware must be allotted for this type of work.

1.4 Available products

One impressive IPS solution is Radware's DefensePro. The DefensePro is suitable for organizations that have high-speed networks and or for ISP's. The reason for this is the bandwidth capabilities of DefensePro. DefensePro is a hardware solution that is built to facilitate high performance for high-speed networks and supports speeds of up to 3 gigabits per second. The DefensePro appliance accomplishes this by using 10 gigabits SPAN port that is accommodated by switching ASICS that are built to achieve Parallel searches. This architecture affords DefensePro with the ability to search up to 256,000 parallel searches. DefensePro has SYN cookie protection that attempts to protect against most known SYN attacks by only accepting TCP/IP connections that has completed the three-way handshake. It then forwards the connection to the destination host and will drop all other packets that didn't follow TCP/IP protocol rules, which in this case is most likely a SYN attack. This affords DefensePro the ability to block up to 1.3 million SYNS per second or 600MBS of traffic, while at the same time allowing legitimate traffic seamlessly. This solution can be pricey and is more suitable for ISP's or large enterprise networks (Radware Whitepaper on DefensePro)

Cisco's IPS implementation should be a better solution for smaller organizations because the software is included in the Cisco IOS. This is supported in Cisco's IOS version 12.3(8)T and above supports IPS configurations. Therefore, additional cost of training can be avoided since available staff would most likely be familiar with the Cisco IOS. Another benefit is the fact that this new functionality is consolidated with the cost of the router and IOS software. The performance of this configuration will be dependent on the type of router running the software. Like the DefensePro appliance, Cisco also performs parallel signature scanning which gives it the ability to scan multiple attack signatures simultaneously. For better performance, the IPS module could be loaded into Cisco 6500 series switch and take advantage of the 40-gigabit backplane. For protection from false-positives, it is possible to disable the faulty rule without altering the other rules. It is easily configured via a wizard that allows you to make custom signature rules and perform automatic updates. Remote access is secured by SSL via a web browser. Alerts from the IPS can then be investigated via Cisco Works or the Cisco Threat response GUI.

SnortInline is an open source IPS licensed by the GPL and has many great qualities that are not available in other vendor solutions. Snort is freely available on the Internet and is probably the most flexible IPS available today. It's integrated with the Snort IDS and IPTables and allows the user to write their own signatures and deploy them on the fly. Most commercial IPS products do not give the user this ability.

1.5 Problems with IPS

Many of the problems that plague IPS are the same ones that would affect an IDS. The tendency to generate false positives is one of the most troublesome issues affecting IPS devices and should always be considered when considering this type of technology. Since IPS has the ability to reset a connection, perform rate limiting or drop a connection, extreme care must be taken not to perform a DOS by dropping legitimate connections. Another problem is that an attacker can send specially crafted packets to trigger the IPS continually in an attempt to overwhelm the device so that when the actual attack takes place, the IPS will miss the attack. Most critics of this new technology usually mention these two critical flaws and rightfully so but the many benefits that the IPS brings to the table should not be overlooked.

1.6 Benefits to Defense In Depth.

Defense in depth is the concept of creating a layered security infrastructure that incorporates security components such as stateful firewalls, packet filters, IDS, VPNs and proxy servers. The initiative is to create an environment that will thwart an attacker even if one of these security components were compromised. Adding an IPS to this deployment has obvious benefits. The use of these components together can alert the network security staff of network reconnaissance, intrusions and other security related issues.

1.6.1 Deployed outside of the firewall

When deployed just outside the firewall and behind the perimeter router, the IPS can give some insight to the security staff on the effectiveness of the perimeter router configuration. Are the ACLs blocking what they are supposed to? Are spoofed packets getting past the perimeter router? The IPS can answer these questions but the IPS can also reset connections of hostile hosts or perform rate limiting if a DOS attack is detected. The IPS could block many attacks that traditional firewalls are unable to decipher. For example, according to the FBI, 77% of attacks were against port 80. Most traditional firewalls are ineffective against elusive services that have the ability to tunnel through port 80. Applications such as HTTP Tunnel and Hopster are readily available on the internet and can allow employees to bypass firewall rules and use dubious programs such as Kaza, Gnutella and so on, thus inviting viruses, trojans and worms into the network and devouring precious bandwidth. These programs can be identified, logged and blocked by an IPS once it's properly configured. These logs can then be used to tighten security, as they shine some light on what your customers or employees are doing to bypass your firewall. Firewalls can be effectively used to control access such as source, destination and blocking port access but most do not have any idea of what content is coming through the port. IPS and other content aware devices are beneficial in this case because they understand protocol behavior, perform deep packet inspections and can discover zero day attacks, as well as known attacks and can either sound an alarm or block this nefarious traffic.

Placing the IPS outside the firewall will also give you a heads up before any attack makes it through your firewalls. Alarms can be set for low severity attacks such as scans or failed password attempts, which will alert security personnel to investigate before the actual attack takes place. In the case of obviously malicious packets, a strong response such a TCP reset or rate limiting can be performed.

1.6.2 IPS on the Internal Network

When an IPS is placed on the internal network, you will have a good idea of what kind of traffic is making it past your firewall rules and entering your internal network. This can again assist the security personnel on how to make the appropriate adjustments in order to augment security. One of the best benefits of an IPS on the internal network is the ability to identify virus or worm propagation quickly and block this traffic. The network security staff can then respond by cleaning the infected host. Virus or worm propagation will be hampered thus limiting the number of infections. Many DDOS, DOS and SYN floods establish from the internal network and are triggered by worms with built-in time triggered attacks such as the Lovsan worm, which triggered an attack against Microsoft's windows update website. These DDOS/DOS attacks can severely impair not only the targeted domain but as a side effect, they can impinge on the network from which they originate. Evidently, this will depend on the number of infected host on the network, the available bandwidth and if these infected hosts perform a synchronized attack. Lastly, the IPS can inform the network staff of intrusions that somehow circumvented the firewall and has made to the internal network. This intrusion can then be blocked with a TCP reset by the IPS.

1.7 Considerations when deploying an IPS

When deploying an IPS, it is wise to fist put all responses in alerting mode in order to prevent dropping legitimate traffic. This could become burdensome because of many false alarms but after tuning your IPS to the needs of your network, the benefits would be realized. Sending attack traffic as well as normal network traffic to the IPS is a good way to fine-tune the device. For example, sending a SYN flood through the IPS will tell you if the IPS knows what is happening by sending an alert. It is also prudent to modify the traffic slightly (as an attacker would do) to see if this traffic makes it though without being discovered.

A centralized server, to which alerts and logs are sent, not only enhances security but also increases manageability. The server can then be protected via firewalls in order to control access to the server.

As mentioned before, the location of the IPS designates its function. Internal threats are mitigated by an internal IPS and external threats are mitigated by an IPS deployed outside the firewall or along the DMZ.

1.8 Conclusion.

Some may argue that IPS technology is somewhat immature but it has great promise and there are many good IPS products on the market today. As I have shown earlier, the IPS's contributions to "defense in depth" are manifold. The IPS can give the network security staff an idea of what kind of traffic is crossing the internal as well as the external network and DMZ. They can also protect the network against DOS or DDOS attacks and virus/worm propagation. Intrusion techniques such as buffer overflows, password attacks, and others, can also be identified via the attack signatures or anomaly detection. The barrage of threats that internet users face today makes it near impossible for human eyes to catch all of them. The IPS is the perfect solution to this problem if proper precautions are taken to avoid false positives.

2 Security Architecture

2.1 Introduction

This section requires that a secure computing and ecommerce environment be deployed for a model company named GIAC Enterprises. GIAC enterprises conduct online services where furtune cookie sayings are sold online. GIAC has a total of 50 employees, most of which are located at GIAC's central office but also has a mobile staff. GIAC also has four branch offices around the world.

GIAC Enterprises has an IT staff comprised of 6 employees. Of these 6 employees, 3 of them are responsible for the integrity of the network. GIACE's network security staff is proficient in using Cisco products and is Unix/Linux savvy. An independent security consultant was consulted to give the networking security staff some tips on improving the network.

2.2 Network Requirements.

- GIACE's mobile workers will need VPN access to the network in order to retrieve fortune cookie sayings from the GIAC database. They will also need access to GIAC's internal network in order to read emails and share files. Since GIACs internal network is a Windows 2000 domain, they will need access to windows RPC (port 135) and Microsoft directory services (port 445). These protocols have many security implications; therefore, access from the Internet is blocked except for authenticated VPN users.

- GIAC's internal users need Internet access in order to conduct research. They will be allowed to use HTTP,HTTPS,SCP, DNS and FTP. On the internal network, they will be able to use GIAC's internal database, Windows Directory services, email services and file and printing services.

- GIAC partner sites need site-to-site VPN access to the GIAC database. They will be granted the same access as mobile users who are authenticated via the VPN concentrator

- Suppliers comprise of companies that traslate and resell fortunes. They will not have VPN access but instead will have an account on GIACE's Oracle Application Server. The application server will allow the suppliers to access the GIACE database in a secure manner and will give them access based on a their configured credentials. They will be able to retrieve and add files to the supplier's database that is located on the GIACE database server.

- GIAC's customers such as high level customers or companies, will have an account on GIAC's Oracle Application Server and will be given appropriate privilege as deemed necessary by GIAC Enterprises.

- The public needs access to the GIACE web server in order to view GIACE's available services and conduct business. Access to the Oracle Application Server (OAS) will be granted only if the user, who is intent on making a purchase, created an account. Default permissions for a new user is limited to only viewing fortune cookie sayings or making purchases.

Below is a table that gives an overview of the services accessible by the aforementioned groups.

GROUP	SERVICE	DESTINATION	REASON
Mobile workers	VPN	GIAC_DB	Access fortune cookie sayings while conducting sales
Internal workers	HTTP,HTTPS,FTP,SCP,DNS	DMZ, INTERNET	Conduct research and carry and daily duties
Suppliers	VPN	GIAC_DB,	Add/Translate fortune cookie sayings
Partner Sites	VPN	GIAC_DB, Internal Network	Conduct daily business
Customers	HTTP, HTTPS	Webserver, Application Server	Make Purchases
General Public	HTTP, HTTPS	Webserver, Application Server	Make Purchases

2.3 Security Components.

Internet

isp-a

isp-b

router-a

HSRP

router-b

Cisco 6509 with reduncant PIX,IDS, VPN & content filtering module

DMZ

WWW

WWW

Oracle Application Server

DNS

SMTP:Symantec GW

services network-vlan 6

GIAC_DB

Internal Mail

Internal DNS

Radius

symantec

Employee Network-vlan 5: Windows 2000 domain, fi le services, ldap directory services and employee workstations

Trunked links

Cisco 6509 with redundant PIX(internal fw) and IDS modules

Security Network

Syslog

Backup Server

CiscoWorks

PDM

KVM

Internet

X.0.31.248/29

X.4.5.32/27

.248

.33

isp-a

isp-b

.249

.250

.34

.35

router-a

HSRP

router-b

.5

192.168.10.0/24

.6

.1

.2

X.4.5.0/27

192.168.20.0/24

websense

.3

WWW

.8

.4

SQUID

Radius

.1

192.168.30.0/24

DMZ

.5

Oracle Application Server

.1

.2

.6

DNS

redundant PIX,IDS,VPN modules

.9

GIAC_EXT

.7

SMTP:Symantec GW

services network-vlan 6

192.168.50.0/24

GIAC_DB

.5

Fetchmail

.6

Internal DNS

.7

symantec

.9

.1

192.168.40.0/24

.2

.2

Employee Network-vlan 5: Windows 2000 domain, fi le services, ldap directory services and employee workstations

.1 Trunked links

192.168.60.0/24

Cisco 6509 with redundant PIX(internal fw) and IDS modules

.1

Security Network

192.168.70.0/24

.1

.2

.3

.4

.5

Syslog

Backup Server

HP Openview

CSPM

KVM

GIAC's requirement for their network is as follows:

- The network should accommodate the access requirements discussed above in a secure manner.

- The network should be built with redundancy for critical components but with the emphasis on security. GIAC Enterprises rationale for this is that since all their capital is generated online, there should be some redundancy in the network. As this infrastructure is the central office, a hardware failure of a critical network component could impair operations for GIAC's satellite offices around the world.

- Components of the network that do not have redundancy should at least have a 24/7 x 4 onsite labor SLA with the vendor, so that in the event of a hardware failure, the component can be replaced in a timely manner.

- In case of a network failure of GIAC's primary ISP, the border routers should failover to a backup ISP by configuring BGP peers. The border routers will also be redundant and use Cisco's HSRP protocol. Only one router is active at any
- GIAC uses Cisco content scanning engine to facilitate secure web surfing, proper use of company time by employees and to increase performance via the caching mechanism in the content engine.

In describing the network, we will start from the border routers and then work toward the internal network.

2.4 Border routers.

Two cisco 7206 routers will be used as the edge devices. Each router will be connected via a DS3 connection to two separate ISP's. Load balancing will not be configured and the justification for this is because uRPF cannot be configured in an asymmetric environment and thus will not be able to protect the network against many spoofing attacks such as DDOS and other kinds of attacks. The routers will use the HSRP protocol so that in the event of a hardware failure of one of the routers, the other will take over. BGP peer groups will be used to enable the fail-over mechanism in the case of a network outage by one of the ISP's.

Due to the security issues concerning the BGP protocol, appropriate measures must be taken in order to overcome these inherent vulnerabilities within the BGP protocol. These issues ranges from session termination – which could cause the router to reset it's routing table and causing loss of internet access through the ISP, prefix hijacking – when a compromised BGP autonomous system (AS) advertises incorrect information and a man-in-the-middle attacks – which can result in a DOS by modifying routes and possibly sending traffic to a "blackhole". In order to mitigate these threats, the border routers are configured to use the MD5 algorithm, which uses shared secrets between the border routers and the ISP's routers. This can deter the act of spoofing and route modification. The draw back to this solution is that the shared secrets must be changed

frequently in order to ensure their integrity. Bogus address blocks are blocked using inbound BGP prefix-lists these bogus blocks are frequently used in DOS attacks. BGP dampening is also used in order to mitigate the effects of flapping routes, which could possibly be caused by an improperly configured router, DOS attack against the flapping router or hardware problem. Prefix-list will also be used to prevent the border routers from advertising ISP-A to ISP-B and vice-versa. Therefore, we will use prefix-list to sanitize what we advertise to our ISP's, which should only be our public address block. The BGP maximum-prefix commands will also be used to protect our border routers in the case that one of the ISPs suffered from an attack against it's routing tables. This attack could occur when a particularly large network prefix is announced by an attacker claiming to be a legitimate peer, which results in router having huge routing tables which consequently, affects the routers overall performance.

Other noteworthy security criteria for the border routers are as follows: disable source-route, unnecessary ICMP traffic – (redirects, outbound unreachables and echo requests), http, telnet, SNMP, Syslog, RPC, Inbound/Outbound Windows RPC services, TFTP (used by many worms) and CDP. Identical ingress and egress filtering will be configured on the routers. Ingress filtering will be configured on the WAN interfaces and egress filtering on the Ethernet interface. The reason for applying the filters to these particular interfaces is because it enhances performance by allowing the router to drop the packets before having to route it. Logging packets that violate the egress filters can alert the security personnel to determine which internal hosts are either compromised or infected with a worm. For additional security, the firewall feature on the Cisco 7206 is used to mitigate SYN flooding and DDOS attacks via rate limiting thus stopping many attacks at the border. Static routes will then be used to send all packets to the next component in line, the Cisco 6509 Layer3 switch (SANS – Packet Filtering Couseware).

2.5 Firewalls.

Two firewalls are used in this network design in order to facilitate defense in depth. Both firewalls are PIX modules that are used in two separate Cisco 6509 layer 3 switches. Each 6509 switch has duplicate PIX modules for failover in the event that one of the devices should fail. Although this is a very expensive solution, the ROI on these devices are reasonable since the Cisco 6509 is very modular and can be configured to use up to 9 different device modules (ie: Gigabit blades, IDS, VPNs and more). The PIX was chosen because of the many security features that it comes with out of the box. The PIX comes with SYN flood protection, Frag Guard (protection from fragmentation attacks), Content filtering and VPN (SANS – Firewalls Courseware). This type of firewall was also chosen because it is configured with Cisco's familiar CLI, which is an administrative benefit to GIAC's network security staff. It can provide a secure infrastructure and has great performance, since the PIX module as opposed to the dedicated PIX device, will be able to take advantage of the fast backplane of the switch. Another benefit in choosing the PIX module over a dedicated PIX device is because it is cost effective. GIAC enterprises maintain a 24/7 support contract with Cisco's TAC support center. Choosing firewalls from different vendors could conceivably create a stronger security stance because vulnerability that affects one vendor may not affect the other. For

example while Checkpoint's proprietary RDP protocol was vulnerable, Cisco pix firewall was not affected. Cisco Pix platform also had vulnerabilities in the way it handled FTP connections which were not present in Checkpoint software. GIAC chose the Cisco pix module because of it's flexibility and because it is not subjected to the vulnerabilities of the underlining operating system, which must be patched in a timely manner and stripped of unnecessary services in order to unsure a secure policy.

The external firewall will police all traffic coming from the border router (Internet) that is going toward the DMZ (web and email services) or the internal firewall (or internal network). This allows for granular control of how the DMZ is accessed by traffic coming from the Internet and regulates traffic coming from the DMZ toward the internal firewall. In fact, the only traffic that will be allowed from the DMZ to the internal firewall are authentication requests coming from the application server to the RADIUS server, return traffic from connections initiated from the internal network and SMTP traffic coming from the external mail server to the internal mail server. Authenticated VPN traffic will then be scrutinized by the internal firewall before being allowed access to network resources.

The VPN is also integrated with the external firewall (which saves money and has great performance) and will terminate at the external 6509 but the decrypted traffic will be sent over a separate network interface from the interface that carries DMZ and Internet traffic but both are directly connected to the internal firewall. The internal firewall will then apply access controls on this decrypted traffic. This design was chosen so that VPN traffic could be closely monitored and controlled. The external firewall will not be able to make any intelligent decisions on the VPN traffic because it is encrypted. A thorough discussion of the VPN configuration will be discussed next.

The internal firewall is also a PIX module deployed in a Cisco 6509. This firewall will monitor all traffic coming from the DMZ, the Internet and the VPN. This creates a layered defense so that even if the first firewall is compromised, there is still some form of protection in place to prevent further intrusion into the network. This firewall also controls access from internal network to internal network. For example

2.6 VPN device

Two PIX Firewall modules are installed in the external Cisco 6509 switch for stateful failover. This allows most applications to seamlessly continue operating in the even that one of the VPN modules should fail. This was chosen because of the nature of GIACE's business model (online enterprise) and because all partner and supplier sites must have 24/7 access to GIACE's internal network.

An IPSEC VPN created with the appropriate access control list will be created in for the 3 groups that will need VPN access: Partner-Site, Supplier-Site and GIACE-remote users. For the partner sites and suppliers, a site- to-site VPN tunnel will be used, while the remote users will use a Digital certificates or CA based authentication. This was

chosen because while we almost guarantee that the Partner-Sites and Supplier-Sites will be connecting with the same IP address, the remote users could be connecting from a hotel room, internet café or from their home network. Thus, the GIACE remote employees will require greater security. To add to this necessity is the fact that GIACE remote users may have access to more confidential information.

IPSEC will be used to provide confidentiality by encrypting the packets before they traverse the network and thus ensuring data integrity, prevent man-in-the-middle attacks by certifying that you are communicating with the expected sender of data and offers strong user and device authentication.

Summary of VPN network configuration.

User	**Conection Type**	**Authentication**
Partner Site	Site-To-Site	IKE-esp-3des esp-sha-hmac,pre-shared
Supplier Site	Site-To-Site	IKE-esp-3des esp-sha-hmac,pre-shared
GIAC remote employees	Remote Access VPN	Verisign CA

Partner Sites:
The partner sites will use a PIX VPN configured with pre-shared keys and IPSEC to connect to the GIAC network. This configuration uses the IKE protocol and will use a RADIUS server for user authentication. The pre-shared keys and IPSEC provides some confidence that the connecting device is who they say they are. However, digital certificates provided by a CA would provide better validation. The border router routes only IKE, ESP and SSL traffic to the VPN interface and all normal traffic will be sent to the External Firewall. The 3DES algorithm or SHA will be used for encryption. After successful authentication and decryption, an access-list will then be used to regulate the subnets that have access to the internal network. A NIDS is deployed on the external 6509 and is configured to trigger an alarm if either, unsupported protocols, worm or virus traffic, recognized attack signatures or prohibited networks are found that are targeting the VPN. Obviously, a VPN can potentially act as a conduit for worm or viruses coming from the Partner or Supplier networks. Therefore, the IDS has been tweaked to key in on these kind of attacks. A single class C network is allowed access and all other disallowed source addresses that are discovered in the tunnel are denied.

Supplier Sites.
The supplier sites also uses a PIX VPN to connect to the GIACE VPN with pre-shared keys. They will have a similar configuration as the partner site, except that they will have more credential on the database server. They will be able to add and files to the supplier database, which is located on the GIAC_DB. All traffic from this network will be subjected to the same scrutiny as the supplier and remote employees.

GIAC remote employees:
GIACE employees will use Verisign as the Certificate Authority (CA) in order to gain access to the GIAC network. As mentioned before, method was chosen because it offers a high level of security for the remote users as they require the ability to connect to the network from any location. CA provides great flexibility because it allows any device to connect to the company's VPN and allows a the CA certificate on a compromised laptop to be annulled and placed on a list that will be checked by the VPN whenever a client tries to establish a connection.

Each employee's laptop is equipped with Zone Alarm personal firewall and Symantec client in order to maintain the integrity of the laptop. Split tunneling will be disabled and all Internet connections will go through the company's ISP once successfully connected to the VPN. This will help to prevent the ability of an attacker to attack the employee's laptop while they are connected to the VPN.

2.7 IDS

The IDSM-2 is an integrated solution that can be deployed as a module in the Cisco Catalyst 6500 series L3 switch. The Cisco IDS was chosen because of its high performance in high-speed networks (600 Mbps) and its ability to monitor multiple networks segments through SPAN/RSPAN. The IDSM-2 is a line-card in the 6509, where it could take advantage of the backplane of the 6509. The Cisco IDS parses a copy of the traffic and so, does not affect the switches performance. The nature of the IDS causes it to be dependent on performance because if the IDS becomes overwhelmed by packets and therefore fails to evaluate all packets traversing the network, then there is a great possibility that an attack could slip through. It is possible that an attacker could send traffic designed to overwhelm the IDS before sending the actual attack.

One of these IDS modules are installed in the external 6509 and it monitors the VPN, DMZ and traffic coming to and from the Internet. The IDS will be tuned to inspect VPN traffic that has been decrypted. It will be looking for worm, virus and attack signatures coming from the partner sites, supplier sites or from remote users and will send an alarm to the cisco-works box that is located on the security network. It also searches for attack traffic that targets the DMZ and internal network. This can assist in verifying that filters placed on the border routers are effective such as verifying that spoofed traffic and reconnaissance scans. It also checks for worm traffic that is being propagated by our internal network. The Welchia worm had a timed DOS attack against microsoft's windows update website. This DOS attack can even take down the firewalls and routers of the network that is initiating the DOS attack. This was GIACE's the grounds for looking for these signatures that are leaving the network.

The IDS module that is deployed on the internal 6509 will key in on any attack that makes it past our 2 firewalls. It will also give us advanced notification if a host on the

internal network is propagating worm or virus traffic, brute force attacks, and illegal attempts to access the security network where the latter is responded to with a TCP reset. The internal IDS can also give the security staff an idea of any prohibited traffic that is getting through the internal firewall, coming from the Internet, DMZ or the VPN. Both IDS Modules are remotely administered from the security network via IDS Device Manager and IDS Event Viewer.

2.8 Content Manager

The Cisco Content Switching module will be used in the 6509 to facilitate GIAC's web services. Again, this product was chosen because it can be deployed seamlessly in the switch and can be configured via CLI thus decreasing administrative overhead. In addition to ease of use, the CCS is very flexible and scallable because like most Cisco device modules, multiple CSS modules can be added for redundancy and for increased performance.

The Cisco Content Switching Module is deployed in the external 6509 and is managed by Websense to provide safe web browsing and protection for GIACE employees as they browse the Internet. This design was chosen in order to provide a better user experience for both GIACE's employees and can increase productivity in the network because employees will be aware that the websites that they visit are being logged and can also be blocked. The content switch acts as a proxy by verifying that the request is safe with the Websense server, which understands layer 4 – 7 protocols and which gives it the ability to ensure proper protocol behavior and can block web browser attacks. It can also decrease the consummation of traffic by mal-ware and can block web sites that are deemed illicit by GIAC enterprises. Some worms and Trojans are also propagated via malicious javascript programs and Activex programs. The content engine can detect these malicious programs and worms by checking its signature database. The signature database is automatically updated everyday with new signatures.

The Content manager can provide great performance by caching previously viewed web sites and can be configured to time out these web sites after a predetermined amount of time. It provides additional security to the network infrastructure since it understands the L4 – L7 protocols and can filter many attacks against the publicly accessible web servers and against employee's who are browsing the Internet or DMZ web services. Therefore, it adds a second layer of defense against web attacks that the IDS may have missed.

2.9 Host IDS

Tripwire is deployed on the DMZ and the servers in the security network. The general policy is to trigger an alarm on failed password attempts, changed files, and could also be tuned to run command line arguments based on some criteria. For example, it is possible to add a null route to a network if is discovered that the network is hostile. Tripwire can also be used for patch management and to issue an alert of the attempt to patch a system failed for some reason. HIDS are also deployed on the internal network servers, such as the Radius server, DNS servers and Mail servers. This way, if an attacker made it past the firewall and IDS systems without being detected then our last line of defense is the HIDS.

2.10 Internal Switches

On the Internal network, there are 3 Cisco 2924 switches. The switches are configured to use VLANS. Therefore, all traffic going between the Security network, Services network and the Employee network must be routed through the switch. Thus, the Firewall and IDS devices will be able to scrutinize the traffic, looking for internally generated attacks. However, ARP cache poisoning, CAM table flooding and IP spoofing can conceivably still threaten the integrity of the network. Thus, proper configuration was put in place to prevent this from occurring.

ARP cache poisoning can be mitigated by binding a specific IP address to one MAC addresses. This feature can be enabled by configuring VACLS on the switch. Thus, helping to limit or disable the capability of an attacker to spoof his MAC address.

CAM table flooding can be mitigated by configuring a MAC address for each port on the all of the access switches. The switch will then block any attempt from MAC addresses that are not configured in the CAM table configuration.

A “man in the middle” attack can occur if an attacker is able to fool the switch into thinking that he is the root bridge by faking BPDU packets. This will then allow the attacker to view sensitive network traffic that would otherwise be unavailable. Using the Cisco switch’s ‘bpdu-guard’ command can mitigated this effect. The switch should also disable the ability for rogue DHCP servers to hand out address and gateway information, thus giving them the potential to conduct a man in the middle attack or a DOS attack.

Thus, this configuration can limit the effect or ability of local attacks to be successful or in the case of a DHCP snooping, could even be a misconfigured device. The architecture of the internal switches also gives the security staff the ability to police all inter-vlan traffic and also inspects this traffic with the IDS.

2.11 KVM Switch

Whenever possible, networking devices and servers will be managed via the Raritan KVM switch via the host’s serial connection Out Of Band (OOB). SSH version 2 will be

used if OOB management is not available on some of the servers or networking equipment. SSH version 2 is deployed across all network devices and servers in order to prevent the possibility of sniffing passwords off the wire. Therefore, all Cisco devices are deployed with the latest Cisco IOS. SSH version 2 support is available in IOS 12.3(4)T and higher.

2.12 Centralized Syslog Server

A central logging server is set up on the security network. All security and networking devices and servers send their syslog entries to this server. This server was especially designed (lots of disk space) for this purpose. The networking devices in question, also uses NTP in order to synchronize all system clocks. In case an intrusion should occur, the intrusion analyst will have accurate time stamps in the logs in order to conduct his/her investigation. A log server like this could quickly overwhelm the security staff with data. When this happens, it is human nature to just simply ignore the logs. This can be detrimental to network security. In order to avoid this scenario, swatch is installed on the Syslog server in order to monitor the log files looking for known attack signatures that are configured by the security staff. This will assist GIAC's busy security staff in monitoring what's in the logs and create greater productivity.

2.13 Squid

The web proxy server has been deployed to protect the GIACE web server and OAS server. The DNS Servers will only advertise the address of the Squid server instead of the addresses of the OAS and the web server. The firewall blocks all traffic coming from the Internet, going toward the web server or OAS server. Only traffic from the security network is allowed to access the web server and the OAS server. This provides maximum protection for GIACE's web services. This design not only adds an extra defense layer but also enhances performance since it caches the web queries. Further requests are then retrieved from RAM (2 gigs) thus bypassing the need for the Proxy to access the network.

Device/Network	Network Address	Subnet Mask
ISP-A	X.0.31.248	255.255.255.248
ISP-B	X.4.5.32	255.255.255.224
GIACE – PUBLIC IP's	X.4.5.0: X.4.5.1 – X.4.5.30	255.255.255.224
Security Network	192.168.70.0	255.255.255.0
Employee Network	192.168.50.0	255.255.255.0
Services Network	192.168.60.0	255.255.255.0
VPN Network	192.168.30.0	255.255.255.0

3 Security Policy

3.1 General Requirements

GIAC Enterprises general security policy consists of the following:
Everything is denied by default and services are added as deemed necessary. For example, HTTP is allowed in order for employees to access GIAC Enterprises web server and in order to conduct research. All protocols that transmit passwords in clear text are disallowed. For example: Telnet, FTP, RSH and RCP are all denied. The Secure Shell (SSH) and Secure Copy (SCP) must be installed on all routers, switches, servers and employees' desktop. All passwords should contain letters and numbers and must be at least 9 characters long. In addition to that, passwords must be changed every 3 months and is enforced via software. Since GIAC networking equipment are all Cisco, the latest version of the IOS software (12.2A) must be installed on the routers, release (12.b) on the switches and pix firewall. All windows services are blocked at the perimeter router.

3.2 Desktop Requirements.

Employees are equipped with a Windows 2000 Professional with Service Pack 4 software on there desktop and patches and security fixes are maintained by remote patching software that is capable of keeping all the desktops current. Spy-sweeper is deployed on all desktops in order to mitigate the effects of spyware, adware, trojans and bots. Spy-sweeper is simple to use and all employees are trained to use this product. Symantec client version is installed on all desktops and is managed remotely by the Symantec Server, which download new virus definitions daily in order to alleviate the effects of viruses and worms. Zone alarm is deployed on all desktops.

3.3 Server Requirements.

All servers are installed with Solaris 8 and all the latest patches installed and monitored with Tripwire HIDS, which as was mentioned before, is also used for patch management. All services that are not being used are disabled via startup scripts. SSH/SCP must be installed on all servers for remote administration.
File and Print services are only used on the print server and all patches are installed. Since lpd and rpc contains known security vulnerabilities.
GIAC Enterprises' Email services are comprised of 2 servers. All MX records for the GIAC Enterprises points to a Solaris 8 server installed with Symantec Enterprise Gateway Server, which is equipped to scan for viruses and contains a hook to RBL+ in order to reduce spam. It updates it's Virus definitions once every hour, everyday. All email attachments ending with: cmd, .com, .pif, .tiff, .exe, .vbs, .scr etc are all dropped. After being scanned for viruses and evaluated against custom and RBL spam-lists, the email is then forwarded to a Solaris 8 server with Iplanet Messaging Server 5, located on the internal network, which has all security fixes.

3.4 Firewall Rules for External Firewall

hostname external

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 intf3 security10

fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa authentication ssh console TACACS+
```

This rule allows for stateful inspection of HTTP, FTP and SMTP Traffic.

```
global (outside) 1 X.4.5.15 - X.4.5.22 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0
```

Creates a global NAT pool for the internal network.

```
static (inside,outside) X.4.5.23 192.168.20.7 0 0 mail server
```

Does one to one NAT for the Mail Server.

```
static (inside,outside) X.4.5.24 192.168.20.4 0 0
```

Does one to one NAT for the Squid Server.

```
static (inside,outside) X.4.5.25 192.168.20.6 0 0
```

Does one to one NAT for the DNS Server

```
static (inside,outside) X.4.5.26 192.168.20.5 0 0
```

Does one to one NAT for the OAS Server

```
access-list 101 permit tcp any host X.4.5.23 eq www
access-group 101 in interface outside

access-list 101 permit tcp any host X.4.5.23 eq https
access-group 101 in interface outside
```

This rule allows any host from the Internet to access HTTP and HTTPS on the http-proxy server.

access-list acl-outside permit udp any host X.4.5.25 eq domain This rule allows any host from the Internet to query the external DNS. Thus, allowing the use of email and web server resources

access-list acl-outside permit tcp any host X.4.5.24 eq smtp

This rule allows domains on the internet to send emails to the external email server.

access-list acl-outside permit tcp any host X.4.5.24 eq www

access-list acl-outside permit tcp any host X.4.5.26 eq https

This rule allows hosts on the internet to access the secure HTTP port on the OAS server.

access-list acl-inside permit tcp 192.168.50.6 255.255.0.0 host X.4.5.26 any

access-list acl-inside permit tcp 192.168.40.0 255.255.255.255.0 host X.4.5.24 eq www

access-list acl-inside permit tcp 192.168.40.0 255.255.0.0 host X.4.5.26 eq https

access-list acl-inside permit tcp 192.168.40.0 255.255.0.0 host X.4.5.26 eq https

access-list acl-inside permit tcp 192.168.50.6 255.255.0.0 host X.4.5.26 eq smtp

This rule allows the internal mail server to send email to any domain on the Internet. However, it does not specify that any other networks besides the security network could access any domain with port 25. This was done because of the recent trends of worms and virus with built-in SMTP engines that could essentially create a DOS attack, send SPAM to other domains or propagate worm or viruses via email without the desktop user's knowledge.

access-list acl-inside permit tcp 192.168.50.7 255.255.0.0 host X.4.5.26 eq domain

This rule is quite similar to the rule before it, in that it only allows DNS queries coming from the internal DNS. Again, recent worms came with time or command triggered DOS attacks against targeted domains by executing exorbitant amounts of DNS queries. Thus, the DOS attacks will either overwhelming the targeted network or the network that the attack was initiated (GIACE internal network).

filter java 80 0 0 0 0
url-server (dmz) host 192.168.1.42 timeout 10

Sends GIAC employee web qureries to the WebSense server so that it can be checked for attacks, worms or viruses.

3.5 Rules for the Internal Firewall

Rule Number	SRC	DST	Traffic Type	SRC Port	DST Port	Action	TRACK
1	Security Network	ANY	ANY	ANY	ANY	Allow	LOG
2	External-Mail	Internal-Mail	SMTP	ANY	25	Allow	LOG
3	OAS	GIAC_DB	Sql_net	ANY	1521	Allow	LOG
4	WWW	GIAC_DB	Sql_net	ANY	1521	Allow	LOG
5	Internal-Mail	ANY	SMTP	ANY	25	Allow	
6	Internal-DNS	External-DNS	Domain-udp	ANY	53	Allow	
7	External-Devices	Sylog Server	Syslog	ANY	514	Allow	
8	Services Network	Security Network	ANY	ANY	ANY	Deny	LOG
9	Employee Network	Security Network	ANY	ANY	ANY	Deny	LOG
10	Employee Network	Internal DNS	Domain-udp	ANY	53	Deny	LOG
11	Employee Network	Internal Mail	ANY	ANY	143,25,110	Allow	
12	Employee Network	ANY	ANY	ANY	80,443,21,22	Allow	
13	VPN Network	Services Network	ANY	ANY	53,80,443,21,22,25 1521	Allow	LOG
14	VPN Network	Employee Network	ANY	ANY	ANY	Allow	LOG
15	OAS	Radius	ANY	ANY	1641	Allow	LOG
16	VPN Network	Security Network	ANY	ANY	ANY	Drop	LOG
17	ANY	ANY	ANY	ANY	ANY	Drop	LOG

The rationale for Internal Firewall Rules will be discussed below:

1	Security Network	ANY	ANY	ANY	ANY	Allow	LOG

This rule allows the Security and network operations team to monitor all services without any access problems caused by firewall rules. System administrators could

remotely administer all the servers in the enterprise. For example, Telnet could be used for troubleshooting purposes but not for remote administration.

2	External-Mail	Internal-Mail	SMTP	ANY	25	Allow	LOG

This rule allows access from the external mail server to the internal mail server on the SMTP port and acts as a second layer of security. This traffic is monitored with the IDS for attack traffic.

3	OAS	GIAC_DB	Sql_net	ANY	1521	Allow	LOG

This rule allows access from the Oracle Application Server to the GIAC_DB oracle database on port 1521.

4	WWW	GIAC_DB	Sql_net	ANY	1521	Allow	LOG

Allows the GIAC web server to access the Oracle database. There is no need for the SQUID Web Proxy to access the GIAC_DB because it sends all web queries to the web server, the web server will then make the database query.

5	Internal-Mail	ANY	SMTP	ANY	25	Allow

This rule allows the internal mail server to send email to any domain on the Internet. However, it does not specify that any other networks besides the security network could access any domain with port 25. This was done because of the recent trends of worms and virus with built-in SMTP engines that could essentially create a DOS attack, send SPAM to other domains or propagate worm or viruses via email without the desktop user's knowledge.

6	Internal-DNS	External-DNS	Domain-udp	ANY	53	Allow

This rule is quite similar to rule 5, in that it only allows DNS queries coming from the internal DNS. Again, recent worms came with time or command triggered DOS attacks against targeted domains by executing exorbitant amounts of DNS queries. Thus, the DOS attacks will either overwhelming the targeted network or the network that the attack was initiated (GIACE internal network).

7	External-Devices	Sylog Server	Syslog	ANY	514	Allow

This rule allows the external security devices such as the IDS, routers and switches to send logs to the syslog server.

8	Services Network	Security Network	ANY	ANY	ANY	Deny	LOG

This rule prevents unauthorized access to the security personnel network. For example, in the event that the internal mail server was compromised, this rule would add an added layer of security.

9	Employee Network	Security Network	ANY	ANY	ANY	Deny	LOG

Similar to rule number 8, this rule prevents unauthorized access to the security personnel network. For example, in the event that a Trojan was installed on a desktop that caused the attacker to gain control over that desktop, this rule would add an added layer of security.

11	Employee Network	Internal Mail	ANY	ANY	143,25,110	Allow

This rule allows employees to receive email from the Internal email server. Users could send email or use the POP or IMAP protocols in order to obtain email.

12	Employee Network	ANY	ANY	ANY	80,443,21,22	Allow

This rule allows the employees to conduct routine business that require internet access.

13	VPN Network	Services Network	ANY	ANY	53,80,443,21,22,25 1521	Allow	LOG

This rule allows VPN users to access the services network and will log all traffic.

14	VPN Network	Employee Network	ANY	ANY	ANY	Allow	LOG

This rule allows VPN users to access the employee network in order to share files and conduct routine business and will log all traffic.

15	OAS	Radius	ANY	ANY	1641	Allow	LOG

This rule allows the Oracle Application Server to query the Radius server for authentication purposes and will log all traffic.

16	VPN Network	Security Network	ANY	ANY	ANY	Drop	LOG

This rule prevents authenticated VPN users from accessing the security network and logs all attempts.

17	ANY	ANY	ANY	ANY	ANY	Drop	LOG

This rule will drop any traffic that was not defined in the rules above and log the traffic.

hostname external
nameif ethernet0 outside security0

This interface is connected to the other 6509. Traffic going to the DMZ or to the internet are routed through this interface.

nameif ethernet1 inside security100
This is the Security network. The security network has critical systems, such as the Cisco Security Policy Manager, HP Openview, the central Syslog server and so on.

nameif ethernet2 dmz security50
This interface is connected to the employee network.

nameif ethernet3 intf3 security50
This interface terminates the VPN and hands out DHCP addresses.

fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25

This rule allows for stateful inspection of HTTP, FTP and SMTP Traffic.

4. References

1. SAFE: IDS Deployment, Tuning and Logging in Depth
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801bc111.shtml

2. SAFE: VPN IPSEC – VPN in Depth
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml

3. SAFE: A Security Blueprint for Enterprise Networks
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b6.shtml

4. RADWARE WhitePaper on Defense Pro
http://www.radware.com/content/products/wsd/whtpaper/default.asp

5. Layer 2 Security
http://64.233.187.104/search?q=cache:cl3GQrUsFYsJ:www.ciscoeventreg.net/go/presentations/event5/emarin.pdf+Cisco+Layer+2+ARP+control&hl=en&start=3&client=firefox-a

5. Cisco IDS Sensors
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_data_sheet09186a008014873c.html

6. Snort Home Page
http://www.snort.org/docs/#deploy