Global Information Assurance Certification Paper

Collin P.B. Freebourne Jr.

GCFW Practical version 4.0

"GIAC Enterprise Online"

Global Information Assurance Certification (GIAC)
Certified Firewall Analyst (GCFW) Certification

Table of Contents

Abstract……3

Assignment 1 – Future State of security technology

Network Intrusion Prevention System ……4

Assignment 2 – Security Architecture

Introduction……8

1.1. What is Information Security and how is it provided……9
1.2. Access Requirements, Justification and Business Operations ……10
1.2.1. Customer Access and Operations……..10
1.2.2. Supplier Access and Operations……12
1.2.3. Partner Access and Operations……..12
1.2.4. Local Employee Access and Operations……..12
1.2.5. Remote Employee Access and Operations……14
1.2.6. Public Access and Operations……...15
1.3. Intended function of security devices & justification of placement.15
1.3.1. Network Design ……..16
1.3.2. Filtering Border Routers……17
1.3.3. Stateful Firewalls……19
1.3.3.1. "Internet Firewalls and the services it protects"……...20
1.3.3.2. "Extranet Firewalls and the services it protects"……22
1.3.4. IDS ……..23
1.3.5. "Host and Other security measures"……..24
1.3.5.1. "General rules Linux servers" ……..25

1.3.5.2. "General rules for workstations and laptops"……25

Assignment 3 – Security Policy

What is Information Security and how is it provided……..25

References……

Abstract

Why me? Why me, inquired the tired system administrator? I was a good boy growing up; I ate my veggies and drank my milk; I didn't play hooky from school except for the must "senior skip day". I went to college, but now on a nice 80 degree California Saturday & Sunday I am stuck here because of that BLAS!# WORM, CODE R#@, … Script Kidd!#, Hack@# !! I don't even know who or what cause this mess, but I can't stand whatever did this. Why me!! Why me!! This was the typical scenario that GIAC Enterprises found itself in quite too often. After seeking some outside advice at a handsome cost I might add, the organization has been advised that they need to improve their security posture to enhance the service level they provide to their computing resource users both locally and remotely.

This document covers Network Intrusion Prevention Systems and discusses the purpose, how the technology works, as well as its possible impact. Then a "Defense in Depth" based solution is provided to the woes of GIAC Enterprise by carefully analyzing their business operations and designing a security infrastructure that will seek to balance their urgent need for securing their computer assets with the overall business need for uninterrupted, uncompromised and profitable service to their customers. "Defense in Depth" is a concept, which seeks to provide security by implementing layers of security vs. a single bullet layer. With multiple layers, attacks will have to circumvent various technologies and implementations to compromise its target. However, security is not a task, thus this solution provided will be a framework which has to be at least maintained and monitored as well as improved as new technologies and threats become known. Some of the components utilized include technologies such as clustering and other redundancy technologies, filtering routers, stateful inspection firewalls, personal firewalls, VPN, proxy devices, network segmentation, network IDS, host IDS, centralized logging, synchronized time, centralized and automated patch management, automated log analysis and alerting, centralized and out-of-band backups, SAN technology as well as centralized authentication with 2-factor

verification. Furthermore, the solution provided to GIAC Enterprise will segment their network based upon security needs as well as performance and technological considerations.

There will be in-dept explanations of the choices available to GIAC including some pros and cons and why the final solution was selected. In addition, a security policy that implements the earlier select design will be presented.

Network Intrusion Prevention System

Today's interconnected society is highly dependent upon communications on demand. From online transactions to personal entertainment, users' desire around the clock access to a variety of services. To provide an acceptable service level to users requires a highly reliable and available infrastructure. Couple this requirement with the ever increasing discovery and exploitation of system vulnerabilities and one realizes that the information security industry has been presented with a huge challenge. Various concepts and strategies have been proposed and implemented to address the need to provide highly available and secured services. Network Intrusion Prevention Systems (NIPS) is one of the newer technologies being evaluated to proactively provide highly available and secured services. Below I will discuss the problem NIPS seeks to address, how the technology works including some vendor implementations and what affect the technology might have on the Information Technology Industry including operational information security engineers.

Why the need for NIPS?

Network Intrusion Prevention System was birth out of the desire to leverage the current strengths of the Intrusion Detection System (IDS) technology by providing the capability to not only alert on suspicious traffic, but also act upon these alerts based upon predefined actions. Intrusion detection systems (IDS) are software or hardware based systems, which are used to inspect, monitor and inform about the occurrence of activities, which are pre-classified as abnormal or suspicious. Most IDS are signature based in that they inspect traffic or activities and compare the header and/or payload to commonly know signatures for malicious or interesting traffic. Additionally, IDS can alert on protocol abnormalities such as invalid IP or TCP options, addresses or other header info. IDS can inspect each packet separately or they can inspect traffic based upon the entire conversation (A.K.A stateful-inspection), which includes reassembling fragments and tracking the conversation in both directions to determine if any part of the message seems abnormal. For network-based intrusion technologies (NIDS/NIPS etc.) to inspect traffic, it must have a connection to a path off a switched port analyzer (SPAN) port, a hub, a tap or in-line. This allows the intrusion technologies to see all the traffic along that path and then perform its

function. Depending upon where you deploy your intrusion technology that will influence to method used to access the path example - if the environment is fully switched then a SPAN on that switch is needed or using a tap of the switch uplink connection would suffice.

NIDS has the ability to reliable alert on known signatures such as common viruses and works which have static header and/or payload data. Additionally, NIDS is effective at providing information to identify abusive and/or compromised systems by alerting administrators of the alleged behavior. IDS can also, we classified as non-intrusive because it only inspects the networks communications and this is where the clear distinction is between NIPS and NIDS. Network Intrusion Prevention proponents such as Richard Stiennon of Gartner recommend stopping large scale investment in IDS implementations because “they offered after the fact assurance that network and system integrity was intact” and also that “Intrusion Detection Systems have proven to be market failures”.

Another contributing reason for the NIPS technology research is the problem of “false positives” with IDS. An IDS false positive occurs when a communications flow has similar header and/or payload data to a known signature and the IDS alerts on the communications even though the traffic may be legitimate. This problem has frustrated many security engineers and has caused a lot of “searching for ghost(s)”. Network Intrusion Prevention seeks to minimize false positives by using not only signature based inspection but a combination of several methods with the alert critically based upon the level of certainty that the traffic is suspicious. Some of the combined methods used are signature based, protocol anomalies, throughput or content variations versus previous content baselines and flow-based approaches which alert on significant changes in specific connection types or host(s).

NIPS technology offers the ability to dramatically reduce not only false positives, but also the need for 24x7 monitoring. Many security environments don’t have the staff, desire or skill set to rigorously interrogate the aggregated logs from all the devices on the network. Thus, some environments use automated scripts and tools to perform this function while others just pay someone else to do it for them. NIPS promises to dramatically reduce the level of analysis needed due to the its combined technique flow analysis which will result in less alerts, more blocked attempted intrusions and more rest for security administrators.

How does the technology work?

Network Intrusion Prevention System was created to leverage the strengths of IDS by taking the technology to greater heights and not only alerting on infractions or interesting communication, but also taking predefined actions to mitigate and or block the traffic in question. NIPS uses several mechanisms to classify its traffic as either acceptable, bad, suspicious etc. Some of these include behavior-based threat detection, policy enforcements, network intelligence etc. The implementation of this technology varies and sometimes integrates several other technologies as well. Some NIPS

implementations add deep packet inspection or content filtering capability to existing firewall technology. Others use honey-pots to attract prying eyes, network based virus protection technology, rate-based controls and various combinations of some or all these technologies.

Solutions which add features to existing firewall technology such as TOP Layer's 5500, Onesecure by Netscreen, Intruvert by NAI and IPolicy's Enforcer allows for more intelligent firewalls which not only controls access with IP or TCP header information but also evaluates the payload of communications to verify that the communications adheres to defined allowable traffic. This essentially provides firewall content filtering for all communications. Thus, not only will this firewall allow only inbound TCP port 80 to your corporate HTTP server, but it can verify the payload of the traffic to allow access to only certain web pages, directories and provide bound checking against buffer overflows or rule base verification against known attacks.

Other NIPS implementations use honey-pot based technology such as ForeScout Technologies' ActiveScout to masquerade as a vulnerable device and entice someone performing reconnaissance to attack the seeming susceptible device. When the elated attacker communicated with the NIPS device all future communications from this device to the network is denied. In addition, some implementations use the NIPS to send bogus NETBIOS information and if any system systems attempts to communicate with the bogus host it will also be "black-holed". Some IPS solutions combine networked based virus checking to existing security device such as firewalls or even have the systems as standalone inline network virus protection systems. These implementations can be very similar NIDS with the added benefit that now they block known virus signatures. Still other implementations combine a detection engine along with intelligence gathering technology to provide rate and flow analysis, monitoring, alerting, throttling and resetting. These implementations gather data on "normal" host and/or network usage and provide NIPS services based upon predefined QOS like parameters. This can be done to individual suspicious host, a group of hosts, port numbers or other characteristics.

How might this affect Information Security Industry and the "Defense in Depth" model?

For some time now, the Information Security Industry has preached the model of "Defense in Depth" which essentially promotes using a layered approach to security. With this approach, there are several security zones and different technologies/vendors are used at each zone to leverage the collective strengths of all the various systems. Different technologies and vendors have their strengths and the premise is to use the device best suited to protect the assets located at the different zones and applying a mixture of vendors will reduce the likelihood of network compromise due to exploiting security vulnerabilities in a specific vendor's implementations. With the changing face of information security and the increase in vulnerability exploitation some have started to re-evaluate the current model to determine

whether there should be more consolidation of the depth of security zones or “pack more punch” at each layer. NIPS implementations blur the line by usually aggregating previously dispersed functions into single devices. This approach has both its advantages and disadvantages with respect to network speed and possible latency issues. Also, what about all the managed services, which surfaced due to the demand for 24x7 monitoring, event correlation, analysis and remediation?

The aggregation of functions which NIPS technologies offers might be attractive to some organizations, but this aggregation doesn’t come cheaply. Most IPS based solutions are currently much more costly that buying individual devices with some of the same functions but there are many hidden benefits to consolidation. With a firewall based NIPS and no IDS there will no longer be a need for a SPAN or tap etc, because the device is now in-line and can see the traffic as it flows through the separate interfaces. This implementation will also provide a more reliable alerting mechanism because hub or SPAN based feeds will discard packets or limit SPAN data if traffic volume is very high which can cause the traffic not to seen by the intrusion technology and thus malicious communications can be go unnoticed. In addition, the aggregation allows more detailed checks to be performed before sessions are allowed to their destination such as virus scans, protocol anomaly validation etc.

However, all this analysis can introduce latency to communication flows, which can disrupt business and negatively impact revenue streams. Most NIPS vendors tout impressive speeds, which usually reflect performance is, simulated cases and usually don’t live up to the hype. Thus, careful customized analysis of current bandwidth utilization and test needs to occur before these devices are implemented in production networks. The possibility of network issues may also be increased because the NIPS devices are performing so many functions that isolating a malfunctions rule, component, signature etc will be more difficult. Furthermore, now if your NIPS device fails there is a greater impact to the network infrastructure than if an individual IDS etc failed because not only is the firewall possible affected but no content filtering is occurring, no traffic monitoring is occurring and maybe even the entire network access might be negatively affected.

Additionally, the intrusive nature of most NIPS implementations can cause packet loss, data corruption and self inflicted DOS attacks. In addition, with less vendor variations the infrastructure is more susceptible to a single exploit for the NIPS of your choice. Before an attack on an internal device might traverse several security devices and be caught by at least one of them, but with a “silver bullet” approach that single device is now the weakest link. For NIPS implementations which leverage “honey-pot” based technologies they will only catch the probing attacker while the single purpose mass propagating worms which continuously cripple networks will go unnoticed. Also, for NIPS which rely on network intelligence there will minimal effectiveness until the network baselines have truly been discovered or these systems will generate more false positives and headaches that any NIDS. While NIPS is suppose to minimize the need for 24x7 monitoring and manages services someone will still be needed to decipher the NIPS alerts which will grow as

threats and exploits continue to rise in number. Thus, manages services are not going away, at least not right now. However, as network intelligence based systems mature the need for these services might slowly diminish.

Currently, the Information security market seems to be taking it slow with NIPS implementations and I believe this is an appropriate approach. The major advantages, which NIPS is supposed to offer, are over hyped. While, I believe that NIPS is here to stay, I don't believe it is the great savior. Implementations, which carefully combine complementary technologies such as firewalls and deep packet inspection, will eventually replace the firewalls of today. The combined analysis approach of flow inspection is great as well as many of the ideas NIPS has brought to the table, but as the hype over NIPS has grown, so has the response from NIDS vendors. Many NIDS vendors have begun to add behavior-based threat detection, policy enforcements, network intelligence and a host of other features to NIDS. Thus, the battle lines have been drawn and only time will tell if Richard Stiennon's assertion that "IDS is Dead" is true or not.

GIAC Enterprise Introduction

GIAC Enterprise started its online fortune cookie sayings business in the mid 90's when the Internet was gaining popularity and as the Internet grew, so did GIAC Enterprise. Their original presence on the Internet was via a managed service solution that housed their web content, provided electronic transaction processing as well as their 28k dialup access to the Internet. As GIAC Ent experienced business success and the related growth, their operational model changed and they required a greater computing infrastructure as well as having greater control of their Internet presence. In conjunction with their computing infrastructural growth, there arose a greater dependence by GIAC Enterprise upon their infrastructure to be highly available. Thus, GIAC Enterprise hired a management-consulting firm to analyze their computing environment and provide recommendations for increasing its stability and availability. The consulting firm performed several assessment measures including a vulnerability assessment as well as some penetration tests and informed GIAC Enterprise of how easy it was to remotely map their network and the services that were offered as well as exploit some known security issues with various versions of components they were utilizing in their infrastructure. The consultants recommended to GIAC Enterprise that their security posture is the weakness that could undermine their efforts to provide stable and highly available services. Upon reviewing the findings, GIAC Enterprise's management decided to make changes in their security posture by allocating the resources to have their security infrastructure upgraded to minimize their attractiveness to would-be attackers as well as having systems that would assist in post-mortem information gathering if an attack is ever launched against the company's assets.

Determining the right security design for any organization requires first a proper understanding of resources the organization possesses and the value levels placed upon the various classes of resources. In addition, there needs to be an understanding of potential use and user's of these resources and possible abusers of your resources. Furthermore when designing an appropriate security infrastructure, their needs to be a determination of the possible cost, political, performance and other business-related implications of the design choices. This information will facilitate the implementation of proper access control and mitigation procedures where it is feasible without negatively impacting the operations. After interviewing several key decision makers from GIAC Enterprise as well as some operational personnel, a list of highly valued information system resources and the possible abusers of these resources were aggregated. The possible abusers were separated into two classes, insider and outside. From the interviews and research it was evident that the database housing the fortune-cookie sayings, the payment transaction processing system, which stores customer information and payment data and the communication channels/infrastructure (including switches, internet, servers etc.) over which these resources travel or are temporarily resident were the most valued resources. Additionally, during the previous information gathering procedure GIAC Ent's management and employees also learned that though some resources are considered more valuable than others, the security of the organization is dependent on the strengths and weaknesses of all the components collectively.

Currently, GIAC provides at least some access to the following groups/classes of users; customers, suppliers, partners, local employees, remote employees and the public. Consequently, the potential "inside" abusers are defined as disgruntled current or past employees with at minimum cursory, but possibly intimate knowledge of at least some portions of the network infrastructure (such as server names/IP-addresses, passwords, type of services on various devices and physical location). Other "inside" abusers are uninformed or naive local or remote users as well as deliberate or unintentional spillover network traffic from shared partner or customer connections. Conversely, "outside" attackers ranged from competitors, novices playing with security or security-evading tools, to improperly configured systems, to experimental probing, automated tools, script kiddies and malicious destructive offenders. GIAC Enterprise has grown considerable since its humble beginnings and as a mid-sized company its management has stressed that the security design implemented should provide the organization with a good current security posture without financially restricting future changes. Thus, they decided to use a healthy dose of open source where applicable and invest wisely in core components. Additionally, GIAC Enterprise management would like the design to utilize economies of scale to get better prices from vendors where possible. The design to follow will consider how to best provide GIAC Enterprise's customers, suppliers, partners, employees and the public with uninterrupted and uncompromised access to the services each user class requires.

Security Architecture

1.1 "What is Information Security and how is it provided?"

Before the GIAC Enterprise security architecture can be explained, we will formally define information security and what it seeks to provide. Information security can be defined as "The confidence that information and services available on a network cannot be accessed by unauthorized users", Comer, pg.582. This confidence can be provided via data integrity, which is protecting against unauthorized changes to data, including either intentional or accidental by ensuring that changes are detectable. Common methods utilize MD5 or SHA hashing. Next there is Data availability, which is guaranteeing that legitimate access to data, is not prevented. This can be accomplished by leveraging fault tolerant and redundant systems as well as implementing additional anti denial of service (DOS) features within services and networking equipment. Additionally, information security confidence can be achieved by providing confidentiality which is protecting data against unauthorized disclosure to unauthorized individuals or processes. Encryption is commonly used to achieve confidentiality. Then there is authorization, which is allowing only selected entities to view selected data and this is commonly done via access control procedures and permissions. Next, there is authentication, which is used to verify an identity claim by or for an entity. Authentication is normally achieved via a username password challenge, a digital certificate presentation, biometric means such as finger print recognition etc. Finally, there is replay avoidance, which seeks to prevent unauthorized capturing of packets and using them later to emulate a previous communication session. Utilizing encryption technologies and securing communication channels are common vehicles used to prevent replay attacks.

1.2 "How we do, what we do & who is looking at what stuff" – Access Requirements, Justification and Business Operations

GIAC Enterprise's sole source of operating revenue is based upon the sale of their fortune cookie sayings worldwide. They package these "bits of wisdom and humor" from various sources including suppliers as well as via partnerships with other similar organizations around the world. The true benefits of their partnerships are received from the cross-cultural and multi-lingual translations which are shared and which allow each partner to spend less time attempting to be experts of all cultures and languages. This security architecture will elaborate on how GIAC Ent provides its computing services to the various entities.

1.2.1 Customer Access and Operations

Perspective or repeat customers access GIAC Ent's home page via HTTP and follow the link to "Products" which displays the product categories as well as an assortment of options. When a customer desires to make a purchase, then

the customer selects the “Buy Now” option, which redirects the user to the secure customer portal site. The customer portal is only accessible via HTTPS because this access mechanism can provide customer’s some sense of reliability that the server being contacted is a GIAC Enterprise authorized server as well as securing communication between client and server via encryption. HTTPS provides this reliability by verifying that the client’s trust the issuer of the digital certificate (called Certificate Authority) the server is presenting and that the current host information matches the information on the digital certificate being presented. Following the digital certificate verification, there will be a negotiation of some security parameters including the encryption algorithm to be used etc. The reliability offered by HTTPS though not full proof because of vulnerabilities such as “man in the middle attacks”, uses a certificate presentation and verification mechanism to validate the server being accessed and then hides the client server communication which is better that the anonymous and blind trusting nature of the normal HTTP access. In addition, if there are discrepancies discovered during the verification process, depending upon the customer’s Internet browser settings the customer might be notified and offered the opportunity to see the variations. The customer has to then choose to continue the product purchase process as GIAC Ent’s customer portal as a new or an existing customer, which will determine how the customer proceeds. If the customer is new, then the customer proceeds as a new user and will have to enter some profile data later in the process. If the customer is a repeat buyer then the customer must be authenticated using the company id and the pass-code supplied after the first purchase. This pass-code is a combination of the company ID and the current pseudo random token-code on the supplied SecurID key fob. This registration procedure is required for two reasons. Firstly, because the fortune cookie sayings cannot be returned, the customer and the payment procedure must be validated before the purchase can be finalized. In addition to the pre-purchase payment validation, the customer registration provides an additional layer of security for GIAC Enterprise by permitting only registered customer’s access to the “GIAC Enterprise Customer Portal”, which has access to GIAC Ent’s customer info including links to previous purchases.

After the server and customer authentication process, the customer is then presented with an array of options to purchase fortune cookie sayings by theme, mood, assorted etc. After a product is selected, the customer is requested to enter some profile data such as company name, size, type of business, contact information and finally what mode of payment will be used for this transaction. After the transaction is submitted, the customer will immediately receive a confirmation email and the GIAC Enterprise sales team will also be notified via email of the pending purchase which initiates the validation of the payment method process. In addition, a customer profile is created in the customer database and a new order will be created with a status of pending and assigned to a sales support representative based upon the company name and location. After the validity of the payment method is verified which can range from minutes for credit card transactions to a couple of days for purchase orders payments or checks, then a GIAC Enterprise sales support representative will access the particular customer’s profile. This will be followed by a change to the status of the order to

an approved status, which will send an email to the customer inclusive of a billing statement, customer ID, a one-time password and a confirmation that they can now retrieve their product from GIAC Ent's Customer Portal via a hyperlink provided. When the customer visits the customer portal, they will retrieve a text file of their sayings, which is unique per transaction and customer id. The fact that the customer portal is access by HTTPS, the retrieval of the sayings can be hidden from other Internet users thus protecting GIAC Ent's valued asset. In addition to the customer notification, the billing system will alert an accounts payable representative of the transaction and the collection process will begin. Upon receipt of payment for an order, that customer's account and order status is changed to reflect the completed transaction.

1.2.2 Supplier Access and Operations

GIAC Enterprise obtains most of its fortune cookie sayings from various suppliers who are required to make deliveries via one of GIAC Ent's VPN solutions as well as use GIAC Enterprise provided 2-factor SecurID authentication for accessing the https delivered "GIAC Enterprise Supplier Portal" to deposit the fortune cookie sayings into the "Blessings Box". Each supplier has an account at the supplier portal, which corresponds to an individual storage area used to deliver the suppliers sayings. The individual supplier repositories are polled routinely to extract sayings as well as notifying accounts payable (AP) and the AP transaction system of any new deliveries. The receipt of a notification indicating a supplier delivery will cause both a manual inspection of the deposited file and a subsequent export of the file into the "Blessings Box" which is name of the GIAC Enterprise's fortune cookie sayings repository. This will be followed by an email confirmation being sent to the particular supplier affirming the receipts of a certain number of sayings as well as the modification of the AP transaction record to reflect the affirmed receipt. The supplier will then access the GIAC Enterprise supplier portal to submit an invoice and subsequently, query the payment status.

1.2.3 Partner Access and Operations

Another avenue that GIAC Enterprise uses to obtain its "words of humor and wisdom" is via partnerships with similar businesses globally. With the increasing travel and migration of people from numerous nations and cultures, the need to provide fortune cookie sayings that are multicultural and multilingual has increased. Thus, these partnerships allow similar business's in different geographical, cultural and linguistic regions to share sayings that are relevant to many customers without having to each be masters of many cultures and languages. The agreement between the partners is predefined related to the quantity and intervals when exchanges will occur. Therefore, at the pre defined interval GIAC Enterprise places the sayings in the partnership deposit folder of their ftp server. Partners will visit the GIAC Ent. Partner's portal and enter their SecurID credentials and extract a copy of the shared sayings as well as deliver their shared sayings.

GIAC Ent processes shared sayings in a similar fashion to purchased sayings except for this transaction being categorized to not initiate a payment to a supplier.

1.2.4 Local Employee Access and Operations

GIAC Ent's local employees interact with various key services to perform their daily activities depending upon their particular department and job function. The services that all or at least most local employees utilize will be discussed firstly and then there will be a discussion of how various departments use some of these services as well as other specific departmental services. All GIAC Enterprise local employees access the active directory (AD) domain for centralized authentication as well as SMB file storage and printing services. Indirectly the local employees utilize the AD domain for access to Intranet web application access, employee directory access (location and public employee information), email access and the transaction process systems, which houses the sales, order processing, accounts payable, accounts receivable and purchasing systems. The SecurID service is accessed either directly for local/console authentication or indirectly when AD is accessed. With a new feature in the SecurID implementation, AD domain authentication request are redirected to the ACE server to leverage the benefits of 2-factor authentication. Internal and External email and web access are also necessary for varying types of communication and information retrieval. Internally most organizational communications and services such as time reporting, vacation request, benefits enrollment, reimbursements and current happenings are available via HTTP (Intranet) for easy access. In addition, internal email is the most common way of business communication and this is provided via commercial SENDMAIL, which integrates Internet Message Access Protocol (IMAP) using STARTTLS and Internal Simple Mail Transfer Protocol (SMTP) service. External www access is provided via a proxy service on the DMZ and external mail is transferred via the internal SENDMAIL SMTP service to the gateway SENDMAIL SMTP service also located on the DMZ.

Additionally, all non-server devices access the Dynamic Host Configuration Protocol (DHCP) service to obtain an IP address to able to function on the network and all devices access the Domain Name System (DNS) service to be able to communication with other device via hostnames instead of IP addresses. All devices also send log information to the centralized log service such as authentication data, administrator required device changes, critical errors etc. The information sent to the log service from service devices is greater in volume and more detailed than the data sent by user stations. All devices also, access the patch management services to retrieve service updates and patches. Windows servers and Linux devices access the Patchlink service while windows clients use the System Update Service (SUS) service freely provide by Microsoft. This solution facilitates having vendor service updates being supplied to all resources using that service in a timely and organized manner. GIAC Enterprise company policy requires all users to save company data to network drives. This policy is enforced by allowing file creation access to only the user's profile "temp" and

"temporary internet files" directories, which limits where new files can be saved. In addition, the profile directories are cleaned by a script when users log into the network. For laptop users they are allowed to save files to their "My Documents" directory, which is synchronized with each user's network drive whenever that user logs onto the local network (Not via dial-in where SMB is prohibited). The reason for the scrutiny of file saving locations is to facilitate centralized backup of designated data servers as well as providing high availability of company data via Storage Area Network (SAN) technology. Finally, all windows host use the centralized virus protection management service and windows laptops use the centralized personal firewall management service to maintain uniform and current configuration information to defend against viruses, worms and trojans. The personal firewall service will restrict what services can be accessed as well as the services permitted to interact with the network on the laptops. These centralized solutions allow global changes to occur simultaneously during regular maintenance or in response to threats.

The sales and marketing team perform a major role in acquiring, soliciting and facilitating new and continuous business for GIAC Enterprise. They interact with the email servers to send messages to solicit new business, to inform current customers of promotions etc., to facilitate the customer purchase process as explained earlier as well as just daily communication internally and externally. The local finance and accounting team performs certain EDI transactions and E-Payment transactions such as tax filings, electronic payments, banking transactions etc, which require an elevated level of communications integrity and/or confidentiality that are gained by utilizing VPN services. The legal team also depends upon services, which provide an elevated level of communications integrity and/or confidentiality provided by certain email functionality as well as VPN technology. The receiving and shipping department utilizes vendor provided web capabilities for tracking items as well as a local component stored in the enterprise transaction processing system. All the other departments generally use the common services in many general ways.

1.2.5 Remote Employee Access and Operations

GIAC Enterprise has many sales and marketing representatives who travel extensively to all parts of the globe to seek business for them. In addition, they also have many permanently remote employees as well as the typical local employee who access corporate resource off-hours. This additional access extends GIAC Enterprise's network perimeter to all corners of the world and over many communication facilities. Thus, the service offering to this class of users is less than the services offered to local employees. GIAC Ent provides remote access via an outsourced remote access provider in combination with it own VPN implementation. The outsource solution provided by IPASS Corp is very cost effective because long distance charges are virtually eliminated via the vast network of local access point that IPASS offers in most parts of the world. IPASS not only provides the traditional dialup service, but there is also wireless LAN access to wireless hotspots as well as other emerging access technologies.

The extension of GIAC Enterprise's perimeter to provide remote employees access to local resources is a balancing act. Although remote employees need certain access to be productive, providing this access allows the vulnerabilities of each system to become points of weakness for all the resources they access and in the end, the entire network could become vulnerable without careful planning and some tough decisions. GIAC Enterprise decided to offer most of the services to its remote users as it offers to its local employees except for SMB based services such as the file and print services because these are usually the targets of many remote attacks. In addition, remote users only have access to commonly defined service ports as well as the service and security networks and this strategy reduces GIAC Enterprise's exposure from remote users to only the more fortified devices on the service and security networks. For most of the travelers, they will be using company provided laptops, which provides restricted local access (non admin) via cached credentials along with the SecurID authentication feature, which allows token codes for up to a predefined period. This capability provided by SecurID would prevent unauthorized access to GIAC Enterprise laptops if they were stolen or lost. In addition enforcing Encrypted File System (EFS) on windows laptop data directories provides additional physical security if a laptop is lost or stolen because only the encrypting user or a domain administrator can access files protected by EFS.

1.2.6 Public Access and Operations

Finally, GIAC Enterprise provides www access for the public to view its home page, product offerings, employment opportunities, company history as well as information about contacting the organization.

1.3 "Intended function of security devices & justification of placement"

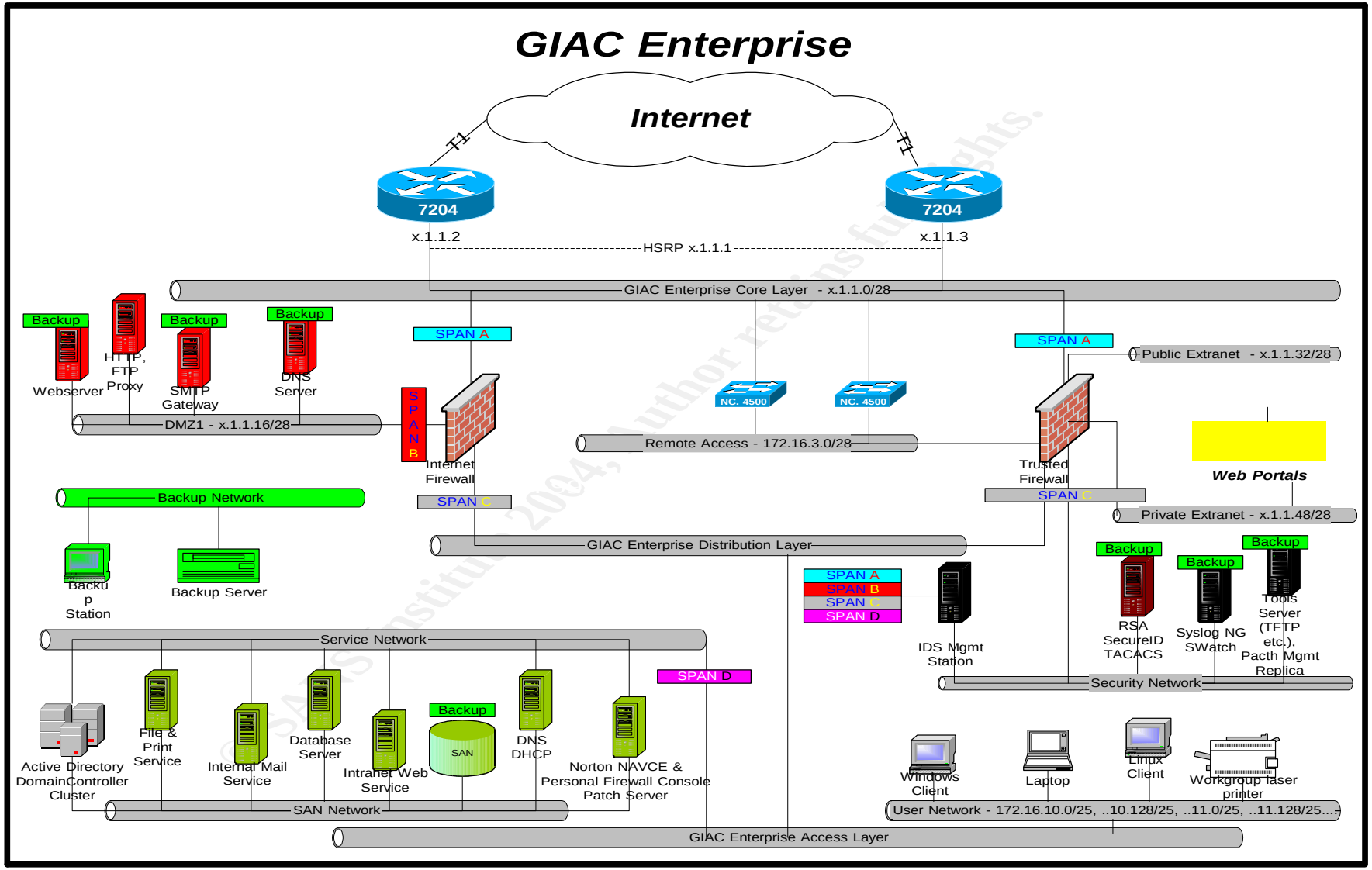
GIAC Enterprise's network design consists of array technologies, which are complementary and as a whole, the design provides "Defense in Depth" to the organizations resources. Following will be explanations of the components of the design including the intended function, justification for the placement of the component and how does the component contribute to providing a layered approach to securing resources.

1.3.1 "Network Design"

Before describing the GIAC Enterprise network design there are a few general statements and points that need to be made that will usually hold true about some general purpose networking devices. GIAC Enterprise uses Cisco catalyst switches 4500 and 2950 throughout their network with mostly 10/100 ports and GIG ports for the server networks. In addition, Cisco MSFC modules cards are used for distribution layer routing and 7204's for border routers. All Cisco switches and routers use IOS version 12.3 and most recent patches. Most current Cisco products has enhance web

administration access via SSL but GIAC Ent currently will not utilize these features especially until a currently know SSL vulnerability[1] is addressed.

[1] http://www.cisco.com/en/US/products/products_security_advisory09186a0080207d5f.shtml



1.3.2 "Filtering Border Routers"

This network design uses filtering border routers for inspecting traffic entering (ingress) GIAC Ent's network for filtering of private addresses as well as packets with local source addresses. The main purpose of this device is to provide connectivity to the Internet via its ISP's as well as routing traffic to the appropriate destinations. As a security device, the border routers are used to perform functions such as ingress filtering and high availability. Performing ingress filtering on private addresses (10.0.0.0/8, 192.168.0.0/16…etc) will eliminate invalid Internet traffic from entering the network. Private addresses aka (RFC 1918 addresses) were designed to be valid only within an organization, thus a message coming from the Internet with a source of a private address can never be valid traffic because a response will usually not get back to the original sender unless source-routing is utilized and the real sender is specified in the source-route path. One might say, "UDP traffic might not illicit as response, so what's the big deal?" Yes, a UPD datagrams might not illicit a response, but if there was an error along the path of a UDP datagram an ICMP error might have to be returned to the original sender to inform them of the problem. When the original sender's address is invalid on the Internet, then ICMP messages or any message for that fact cannot be returned to the original sender except for source-routed packets because RFC 1918 states that Internet routers should discard message to this destination address. Ingress filtering on source addresses that are designated to GIAC Enterprise will eliminate attempts to exploit access that is granted to local GIAC Enterprise addresses because it's not possible for valid traffic from the Internet to have a source address owned by GIAC Enterprise. Additionally, as with private addresses, responses to these spoofed addresses usually will not be returned to the "real" original sender unless the message is source-routed. Additionally, if the sender doesn't care about a response from his message it is possible that the message contains commands that when processed by the destination service will then allow the "real" sender to verify the receipt of the message as is common in some payload based buffer overflow attacks. If the message never gets past the border, it cannot accomplish its purpose. To eliminate source-routed spoofed messages to or from GIAC Enterprise, source routing will be disabled on its routers. Therefore, the ingress filtering utilized reduces traffic from misrepresented or invalid Internet sources aka (spoofed sources). Reducing spoofed traffic at your border routers provides layered coverage by not allowing invalid traffic to even enter the network since this device will be the first layer 3 or above device that packets will attempt to traverse. The basic internet address based ingress filtering being utilized also doesn't add much additional overhead to the router since it has to process the IP layer information for routing purposes. One might ask, since the border routers can filter ports as well why not perform ingress port blocking and never let unwanted traffic to enter the network. While it is true that GIAC Ent's routers can use extended ACL's to perform such functions this will require the router to inspect another layer of the "encapsulated onion" and thus increase resource utilization. GIAC Enterprise will use its firewalls to perform those functions.

The border routers are also configured for HSRP (Hot Standby Routing Protocol), which provides redundancy and high-availability for Internet connectivity by creating a virtual router from two or more routers. If the primary router fails then the router with the next highest priority within the HSRP group will assume both the layer2 (hardware address) and layer3 (internet address) information for the group. In addition, redundancy is also provided by using two Internet connections from different providers in conjunction with BGP (Border Gateway Protocol) for synchronization of routing information between our possible routes. Using multiple Internet service providers (ISP) reduces the likelihood of Internet connectivity downtime due to problems at an individual ISP, which is important for an E-Business such as GIAC Enterprise.

1.3.3 "Stateful Firewalls"

At the next layer of the GIAC Enterprise network infrastructure are two firewall pairs, which statefully inspect all ingress and egress (exiting) data flows. These firewalls are used to restrict access to GIAC Enterprise's resources either by host or by port. The statefulness functionality enhances security by implicitly denying traffic from lesser-secured interfaces (e.g. Internet facing interface) to more secured interfaces via its state table or checking for an explicitly defined action. By using a state table, this device will permit or deny if an entry for this connection exist in the connection table or the access is explicitly allowed. Additionally, this stateful inspection device can use special functionality to check for protocol adherence such as http, ftp, SMTP etc. Furthermore, this device will reassemble fragmented traffic to validate the entire message when determining whether to allow or deny a communications flow. These firewalls are strategically placed below the border routers to receive the ingress filtering coverage provided by the border routers, to protect the Internet accessible devices as well as controlling egress Internet access. Without some filtering device, GIAC Ent's connection to the Internet would be a open door for Internet host to exploit vulnerabilities in services, crack weak password, perform denial of service attacks against resources, use GIAC Ent's host to launch anonymous or distributed attacks on other networks etc. In addition, these routers will perform egress (exiting traffic) filtering to allow only the addresses that are designated for their network. This measure will prevent the spoofing of non-GIAC Ent addresses from within the GIAC Enterprise local network and protect other Internet hosts.

One pair of firewalls is used for public access to the organization as well as for internal devices to access external email, http, ftp etc to the Internet. While the other firewall pair, houses employee and customer VPN access, in addition to the GIAC Ent's customer, partner and supplier portal sites (Extranet) as well as the security network. Using a parallel firewall infrastructure allows ingress policy implementation to be segmented into a more trusted and less trusted domain as well as allowing the division of connection workload across devices, which can reduce possible bottlenecks. GIAC Enterprise selected to use Cisco Pix 525's (v6.3) in a failover configuration because it could negotiate better pricing and

maintenance to couple the firewalls with the existing Cisco equipment it already possesses. Additionally, GIAC Ent's knows that most engineers have worked with Cisco IOS products thus, current and future engineers will have a shorter learning curve for understanding and implementing its security policy. The Pix device has the appropriate bandwidth and NIC slots available to meet current needs as well as providing room for growth. The parallel firewall infrastructure is ideally placed, because routers usually have more horsepower than firewalls, and thus they can process a greater volume of messages. With the filtering performed at GIAC Ent's border routers the traffic processed by the Internet and Extranet firewalls will be less than if a firewall was the first device encountered on their network.

1.3.3.1 "Internet Firewalls and the services it protects"

The Internet firewall processes ingress connection request to the DMZ segment and egress connection request to Internet services. Additionally, the Internet firewall allows only certain services to be reached from the Internet as well as statefully managing communications to and from other services. This network is one of the greatest deliberate exposure points to GIAC Ent's security posture because all valid Internet host can initiate communicates with this network and most services it offers. However, these hosts are probably the most fortified and monitored devices due to their exposure. This segment houses the BIND DNS, Commercial SENDMAIL SMTP gateway, Squid Proxy Service and the public Apache Web service.

When services are offered to internal users under a single administrative domain, the intent of users connecting to these services is usually viewed as non-harmful even though repeatedly many system compromises have originated from within an organization's border. Conversely, when devices can be reached by any Internet host, the intent of the connection cannot be naively trusted, thus protective measures provided by a single solution or a combination of different tools can provide a "Host base Intrusion Detection System" (HIDS). Leveraging HIDS on certain devices can provide an additional layer of protection for services especially those that are known to produce periodic vulnerabilities. All of GIAC Enterprises externally accessible servers are housed on Red Hat Enterprise Linux 3.1 servers in a clustered configuration. Linux machines have a treasure of HIDS tools by default, along with many open source additions, which GIAC Ent has chosen to use so that they don't have to be tied to a particular vendors HIDS approach. By utilizing tripwire, syslog, swatch, iptables and portsentry, GIAC Enterprise can monitor and proactively defend its Linux devices against various attacks or malicious activity. How the various tools are used to achieve a HIDS solution will be discussed later in this document when focusing of protecting specific services.

During the initial design stages there was consideration being given to subdividing the DMZ segment to have the DNS service on its own segment because the external DNS service is viewed as one of the crown jewels of the organization and if this service is compromised, GIAC Enterprise can be severely hampered. What if the DNS service was

on the same network segment as the web service and one of the web servers was compromised. The attacker could configure the DNS service on the compromised device and perform ARP poisoning techniques to masquerade as the authentic DNS server. Thus, when valid DNS request are sent to the GIAC Enterprise DNS service the compromised device could give false information pointing users away from GIAC Enterprise's web sites causing a Denial of Service (DOS) attack or even pointing users to malicious sites or offensive sites. Someone might ask a follow-up question "What about the web service being compromised and used to redirect web site visitors to the sites mentioned above?" While this is true, compromising the DNS service could compromise all externally available services offered by GIAC Enterprise as well as all services employees are accessing on the Internet. However, though the scenarios were insightful and thought provoking the Cisco switches which provide the physical connectivity for all GIAC Enterprise devices has a sweet feature which can thwart ARP spoofing called "Port Security". This feature when enabled on an individual port will remember what MAC address it has seen sending traffic from the port and if any other MAC addresses is seen transmitting from this port, the port is automatically disabled which, can lead to a DOS attack, which is easier to remedy than the alternative already discussed.

For Internet users to conveniently communicate with GIAC Enterprise's service offerings (Web sites, email etc) a DNS server is needed to translate the user friendly domain names to the IP address of the devices that houses the particular service of interest. GIAC Enterprise provides a DNS service that employs a split brain DNS scheme where the external DNS servers have knowledge of the DMZ hosts and other external DNS servers. In addition, the external servers provide proxy DNS service for Internet host resolutions on behalf of the internal DNS servers. Meanwhile, the internal DNS service has knowledge of GIAC Ent's internal host and forwards request for Internet host to the external DNS service. Internal DNS servers are synchronized, but this local resolution information is never forwarded to the external DNS service. The DMZ is a safe place to locate the external DNS server because it doesn't allow direct traffic into the internal network and the firewall interface can provide access to only the DNS service port and protocol required. The DNS service could have been placed between the border router and the outside of the Internet firewall interface, but that position would have exposed the device to DOS attacks, scanning etc. Despite the fact that this host is hardened and only allows inbound DNS-queries and zone transfers from its cluster partner the exposure would have been minimized. However, "allowing the firewall to do its filtering thing" and reduce the likelihood of DOS attacks from distributed scanning is reason enough not to place the service outside the firewall interface. Why not place the DNS service inside the corporate network or why not just have one DNS solution on the service network? Well, although the DNS service doesn't fully utilize a high degree of the server resources and may seem like a waste to use a split brain scheme, allowing Internet hosts to directly connect to a device inside the LAN would allow a user free reign in the corporate network if the DNS service was compromised.

GIAC Enterprise's dependence upon its Internet presence cannot be overstated thus, its public web service, which is the gateway for customers, must be accessible to any Internet host. Placing this service on the DMZ off-loads network filtering to the firewalls allowing the host to focus on providing its service as well as providing other security benefits mentioned earlier in discussing other DMZ services. In addition, the fact that this service houses mostly static information its internal access is very limited, thus reducing its direct vulnerability exposure to internal services and hosts.

For email to flow from domain to domain throughout the Internet, each domain has to have a point of contact to receive these messages similar to a city, state or zip code distinction. The SMTP gateway acts as intermediate post office for messages destined to or addressed from users within GIAG Enterprise's domain. Without allowing access to the SMTP gateway from Internet host, then others wishing to send messages to the GIAC Ent domain would have to use "snail mail" which is another name for your trusted local postal system. Placing the SMTP gateway on the DMZ has the same rational as placing the DNS service in the same location. However, this concession for email can expose an infrastructure to many issues such as controlling mail relaying and validating service request. Improperly configured corporate SMTP gateways can be abused to relay Unsolicited Bulk Email (SPAM) if the service is not configured to authenticate the submission of messages to users outside the GIAC Enterprise domain as well as implementing the recommendations found in RFC 2505[2]. This authentication will include validating that the message is destined for an address within GIAC Ent's domain as well as verifying that outgoing messages were originated from an internal system.

GIAC Enterprise's business necessitates only certain Internet usage for internal employees such as http, https, SMTP and ftp. Thus, to better utilize Internet bandwidth via caching, provide anonymous http usage as well as filtering ActiveX, Java and other such possible harmful technologies a proxy service is used. The Squid proxy service with squid-filter add-on modules provides the security benefits of hiding internal system addresses as well as filtering web components that can be used to compromise systems browsing the web. GIAC Ent chose this product because it was not convinced that it wanted to invest in proxy firewall or did it want just a vanilla web proxy with filtering. The solution chosen gives them more flexibility so that if other business related Internet requirements arise they can adjust as well as they are still financially able to procure a enterprise solution in the future because they didn't really invest much into this solution as the software is free.

1.3.3.2 "Extranet Firewalls and the services it protects"

The main purpose of the extranet firewalls is to facilitate access to GIAC Enterprise's customer, supplier and partner portals, employee and partner VPN services as well as the security network services. In addition, the

[2] RFC 2505 "Anti-Spam Recommendations for SMTP MTAs" Best Current Practice – G. Lindberg

segmentation of traffic between the Internet and the extranet firewalls, allows most customer, supplier and partner interactions to be facilitated by the extranet firewalls. This fact simplifies access policy implementation versus providing all these services on a single firewall pair. These firewalls restrict what VPN users are able to access based upon the access requirements detailed earlier in this document.

All extranet devices are dual-honed with connections to the private and public extranet networks. External access is provided via the public extranet network and internal access for administration is provided via the private extranet network. This separation allows the firewall to use separate interfaces to process internal and external communication, thus if a extranet host is compromised only its private extranet access can be used to access internal systems which only has filtered access at the firewall. In addition, the host NIC on private extranet has only static routes to certain internal hosts to provide additional host hiding. The customer portal is the only accessible service on the public extranet network that can traverse the outside interface of these firewalls. The extranet public network allows only supplier and partner VPN connections to access the supplier and partner portals respectfully with the exception being internal users via the proxy service.

The security network is used to provide specific access to resources such as TACACS for network device login (ex. router, switches, routers and firewalls), SecurID for 2-factor authentication, Syslog, TFTP for configuration and IOS management, IDS analysis etc. It was placed off this firewall to provide centralized filtering for services and from certain DOS and network mapping/reconnaissance techniques. In addition, this network allows externally reachable devices to access certain services such as patch management, virus signatures management and logging, without direct access into the internal network. If this network was provided anywhere, except directly off a firewall interface, service filtering on a per host basis could be cumbersome and difficult to maintain as well as DMZ and other external devices would have to get certain services manually or have direct access into the internal network.

1.3.4 "IDS"

The IDS solution provided by GIAC Enterprise utilizes SourceFire Management sensor (v3.0), a NS3000 (to handle Gig Service network) and NS2100 sensors (v3.0) as well Shadow IDS (v1.8). The Shadow IDS is an open source IDS solution which GIAC Ent uses to capture snippets of its external traffic to report to its management the correlation between attempted attacks versus what the firewall filter SNORT IDS will view. It is used for trend analysis, future signature creation via post-mortems of compromised devices or suspicious activity. Placing this device outside the firewall is necessary for the comparative analysis previously mentioned can be done. In addition, GIAC Ent uses a commercial version of the popular static SNORT IDS for other perimeter and internal analysis. The management station securely communicates configuration, signature data and aggregates sensor data from each senor. Alerts generated are forwarded

to the central syslog server for coordinated analysis. The main purpose of the IDS attached to SPAN (B-D) is to obtain data on intrusion attempts that traverse the Internet or Extranet firewalls and alert GIAC security team to research and resolve the issue. Positioning the network spans at the location listed on the diagram allows the important intrusion points to be monitored. There is no monitoring on the remote access segment because the extranet, security and inside segments are monitored and the remote access network is not accessible from the outside interface, thus there is need to directly monitor this interface.

1.3.5 "Host and Other security measures"

Previously the primary perimeter security devices were discussed; this discussion will now focuses on various host specific security techniques as well as some other general security measures implemented both internally and on the perimeter of GIAC Enterprise's network. GIAC Enterprise's disaster recovery policy requires backup of critical systems and data. This is implemented on a separate network that backed up host access directly via another NIC. No services listen on this interface except the backup client as a security precaution. In the network diagram some hosts are identified as backup host, these hosts have their system state and data backed up. The fact that most host and all client data is stored on the SAN using EMC storage this data is highly available and is easier to backup than if all data was on every individual host. Port security will be enabled on all external device port as well as some critical internal servers. As mentioned before centralized logging will be done via SyslogNG and all server as well as network device will forward their logs. To allow for proper analysis, a NTP server will be used to synchronize time of these devices.

1.3.5.1 "General rules Linux servers"

All of GIAC Enterprises Linux host run Red Hat Enterprise Linux 3.1 with the latest patches for the services offered. Linux machines have a treasure of HIDS tools by default, along with many open source additions, which they have chosen to use so that they don't have to be tied to a particular vendors HIDS approach. By utilizing tripwire (v2.3.47), SyslogNG (v2.25), swatch (v3.1) and portsentry (v1.1), GIAC Enterprise can monitor and proactively alert any activity deemed as malicious or suspicious. Their HIDS solution uses tripwire to monitor changes in file hash, syslogNG for centralized storing of log files, swatch for monitoring and alerting on log activity that is defined as suspicious as well as portsentry for sending alerts on scanning activity. Their solution also, have the option of using portsentry to perform prevention techniques at the network layer by inserting rules via iptables to deny access to scanning host. However, their security team is cause about using this functionality until extensive testing and management approval is received. Additionally, general hardening rules such as changing the umask for default directories, remove unused setuid applications, put programs in a chroot jail, restricting local console login to root, using ssh only for remote login, using

SecurID for all pam service authentication as well as other recommendations in sources such as “Hacking Linux Exposed”.

1.3.5.2 ”General rules for Windows servers”

All of GIAC Enterprises Windows servers run Windows 2000 Server or Advance Server with the latest patches for the services offered. Windows servers are usually the most attacked devices and thus GIAC Ent invested in the Symantec’s Client Security product to secure the windows servers on the service and security network. This product provides antivirus, firewall and intrusion detection and integrates with the other Symantec products into the Symantec management console. All severs can get updates of policy changes and signatures simultaneously. In addition, the logging provided augments the non-existent network logging provided by the OS. The firewall functionality is used to limit access to and from the servers based upon their profile (ex. Web server, domain controller, Ace Server etc). All windows devices also, have SNARE agent (v2.3.5), which converts event log messages to syslog format so that certain event activity can be sent to the central syslog server for analysis such as admin local logins, password failures etc. In addition, the devices are hardened as prescribed by the “Securing Windows 2000 Step by Step”.

1.3.5.3 ”General rules for workstations and laptops”

GIAC Enterprise’s internal users mostly use windows XP machines with a few exceptions of administrators with Linux machines. All users’ have non-administrative accounts to limit the damage they or someone impersonating them can do to local a host. As mentioned before all windows host get patches from the local PatchLink patch management server and virus signatures from the Symantec antivirus server. Windows laptops have Symantec Client security just as the servers do, but their client profile differs allow no inbound connection initiation and only certain outbound connections.

Security Policy

Pix firewall access-list rules are order specific other items are not. Permit statements usually should be put before deny statements. If allowing specific host use permit, otherwise use the deny statement. Permits allow the access-list to continue to be processed while denies will cause the packet to be dropped if the criteria matches. However, to deny few host and allow everything else then place deny of specific host first then allow the others.

PIX Version 6.3(3)
interface ethernet0 100full **– *Sets the Interface speed to 100 & duplex to Full.***

interface ethernet1 100full ***– Sets the Interface speed to 100 & duplex to Full.***
interface ethernet2 100full ***– Sets the Interface speed to 100 & duplex to Full.***
interface ethernet3 auto shutdown ***– Default disables the Interface and sets speed & duplex to auto***
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 intf3 security10

Nameif sets interface security levels with sec0 being the least secure zone and sec100 being the most trusted zone. This affects how data flows from interface to interface with explicit access-list required for flows origination from higher security zones to lower security zones.

enable password VUFzWR2xbd0OWXZ7 encrypted ***– Sets enable mode local password***
passwd VUFzWR2xbd0OWXZ7 encrypted ***– Sets local password for admin user as encrypted***
hostname seclabpix1 ***– Sets device hostname***
domain-name giacenterprise.net ***– Sets device domain name***
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25

Fixup protocol instructs pix to reassemble fragmented packets and evaluate the message as the destination host would see it. This feature will catch attempts to use fragmentation to bypass rules if the port field will be spread across multiple fragments.

names
access-list acl-outside permit udp any host 223.1.1.19 eq domain ***– Allows internet DNS request to DMZ DNS server***
access-list acl-outside permit tcp any host 223.1.1.21 eq smtp ***– Allows internet smtp services to allow receipt of internet mail***
access-list acl-outside permit tcp any host 223.1.1.23 eq www ***– Allows http access to company public web server.***
access-list acl-dmz deny udp host x.1.1.19 10.0.0.0 255.0.0.0 eq domain ***– Denies DNS request to internal servers.***
access-list acl-dmz deny tcp host x.1.1.19 10.0.0.0 255.0.0.0 eq domain ***– Denies DNS request to internal servers.***
access-list acl-dmz deny tcp host x.1.1.23 10.0.0.0 255.0.0.0 eq 80 - ***Denies http request to internal servers.***
access-list acl-dmz deny tcp host x.1.1.23 10.0.0.0 255.0.0.0 eq 443 - ***Denies https request to internal servers.***
access-list acl-dmz permit tcp host 223.1.1.19 any eq domain ***– Allows DNS request to all servers except internal servers.***
access-list acl-dmz permit udp host x.1.1.19 any eq domain ***– Allows DNS request to all servers except internal internal servers.***

access-list acl-dmz permit tcp host x.1.1.23 any eq 80 ***– Allows proxy server to request http pages for internal users from the internet.***
access-list acl-dmz permit tcp host x.1.1.23 any eq 443 ***– Allows proxy server to request https pages for internal users to the internet.***
access-list acl-dmz permit tcp host x.1.1.21 host Inside-Smtp-Server eq smtp ***– Allows SMTP gateway server to connect to internal SMTP servers to transfer mail messages.***
access-list acl-dmz permit tcp host x.1.1.21 any eq smtp ***– Allows SMTP gateway server to connect to other SMTP servers to transfer mail messages.***
access-list acl-inside permit tcp 172.16.0.0 255.255.0.0 host x.1.1.23 eq www
access-list acl-inside permit tcp 172.16.0.0 255.255.0.0 host x.1.1.23 eq https
access-list acl-inside permit tcp 172.16.0.0 255.255.0.0 host x.1.1.23 eq ftp
Allows internal host to connect to only the proxy server for external Internet access. This hides internal clients from exposure to Internet abuse and allows proxy server to verify url and perform filtering as needed.
access-list acl-inside permit udp 172.16.0.0 255.255.0.0 host x.1.1.19 eq dns - ***Allows dns request to dmz DNS host***
access-list acl-inside permit tcp host internal-smtp-server host x.1.1.21 eq smtp – ***Allows external email to smtp gateway server.***
access-list acl-inside permit tcp host internal-patchlink-server host x.1.1.0 255.255.255.224 eq www ***– Allows Patchlink updates***
access-list acl-inside permit tcp Security-net Border-routers eq ssh ***– Allows remote admin to border routers etc.***
pager lines 40
logging on
logging host inside security-log-server ***– Set syslog server***
logging monitor errors
logging buffered errors
logging trap errors
mtu outside 1500 ***- Sets MTU for interfaces***
mtu inside 1500
mtu dmz 1500
ip address outside x.1.1.4 255.255.255.240 - ***Sets interface ip address for devices.***
ip address inside 10.33.145.1 255.255.255.224 - ***Sets interface ip address for devices.***
ip address dmz x.1.1.17 255.255.255.240 - ***Sets interface ip address for devices.***
ip audit info action alarm

ip audit attack action alarm
failover
failover timeout 0:00:00
failover poll 15
failover ip address outside x.1.1.5
failover ip address inside 10.33.145.2
failover ip address dmz x.1.1.18

Sets failover ip address. In normal state the secondary device lays dormant until the primary fails then the secondary assumes the ip info of the primary.

pdm history enable
arp timeout 14400
global (outside) 1 x.1.1.64-223.1.1.250 ***- Sets one–to-one nat***
global (outside) 1 x.1.1.251 ***– Sets PAT (one-to-many NAT) to be used if other nat pool is exhausted.***
nat (outside) 0 x.1.1.0 255.255.255.240 0 0 ***– Disables NAT for outside addresses***
nat (inside) 1 10.33.145.0 255.255.255.224 0 0 ***– Enables NAT for inside addresses***
nat (dmz) 0 x.1.1.16 255.255.255.240 0 0 ***– Disables NAT for address on local dmz net***
nat (dmz) 0 10.0.0.0 255.0.0.0 0 0 ***– Disables NAT for address on local dmz net***
static (inside,dmz) 10.0.0.0 10.0.0.0 netmask 255.0.0.0 0 0 ***– Allows internal devices to accessible from DMZ.***
access-group acl-outside in interface outside - ***Binds acess-list to individual interface.***
access-group acl-dmz in interface dmz
access-group acl-inside in interface inside
route outside 0.0.0.0 0.0.0.0 x.1.1.1 1 ***- Default route points to internet.***
route outside x.1.1.0 255.255.255.224 223.1.1.4 1
route inside 10.0.0.0 255.0.0.0 10.33.145.41 1
route dmz x.1.1.16 255.255.255.224 223.1.1.17 1
timeout xlate 3:00:00 - ***Session and xlate etc timeouts.***
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ (outside) host x.33.145.63 1sth1sr3allyy0u timeout 5 ***– Sets TACACS+ host and key***

aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa authentication ssh console TACACS+
aaa authentication telnet console TACACS+
aaa authentication serial console TACACS+
Sets remote admin authentication to use TACACS+ for centralized authentication control.
no snmp-server location
no snmp-server contact
no snmp-server community giacsecent
no snmp-server enable traps - ***Disabled snmp services. Snmp has many security issues with early versions.***
floodguard enable ***– Allows pix firewall TCP resources to be reclaimed if the user auth subsystem is out of mem.***
sysopt noproxyarp inside ***- Disables proxyarping on active interfaces.***
sysopt noproxyarp outside
sysopt noproxyarp dmz
telnet timeout 5
ssh security-net 255.255.255.0 inside ***– Limits ssh access to the security network, thus no other network host except hosts on the security network can remotely administer this device. This limits the use of clear text via telnet and uses ssh which encrypts administration communications.***
ssh timeout 10 ***– Sets ssh timeout to reduce risk of exploiting a vacant ssh session.***
console timeout 0 ***– Disables console timeout***
terminal width 80

References

BorderGuard
http://www.stillsecure.com/products/bg/?rf=google&rfdetail=intrusion_prevention

Garfinkel, Simson & Spafford, Gene - “Web Security, Privacy & Commerce”

Hatch, Brian & Lee, James – “Hacking Linux Exposed Second Edition”..

HIDS
URL: http://www.linuxjournal.com/article.php?sid=5616

McQuerry, Steve – “Interconnecting Cisco Network Devices”

Messmer, Ellen, “Don’t dis’ my IDS” – Network World Fusion 06/16/03
http://napps.nwfusion.com/cgi-bin/forum/gforum.cgi?post=529

Network Intrusion Prevention Systems
http://www.nwfusion.com/reviews/2004/0216ips.html

Northcutt, Stephen Et al. - “Inside Perimeter Security”, New Readers, 2003

Northcutt, Novak, “Network Intrusion Detection Third Edition”, New Readers, 2003

RFC Editor Database (1733, 1939, 2195, 2505, 2821, 2979, 3013, 3365, 3501)
http://www.rfc-editor.org/rfcsearch.html

SANS Institute – “Track 2 Courseware Firewalls, Perimeter Protection and VPNs” 2003

SANS Institute, “Securing Windows 2000 Step by Step”

Scambray, Joel & McClure Stuart – “Hacking Windows Exposed”..

Shadow IDS
URL: http://www.nswc.navy.mil/ISSEC/CID/Install3-MS.htm

Snyder, Joel, Burns Christine **– “**ForeScout pitches honeypot technology as IPS”
http://www.nwfusion.com/reviews/2004/0216ipshoneypot.html

SyslogNG
http://www.balabit.com/products/syslog_ng/

Symantec Host IDS
URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&EID=0

Symantec Client Security
URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=154&EID=0

Tripwire
URL: http://www.tripwire.org/ganda/index.php