Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW) Practical Assignment

The Future of Network Intrusion Prevention Systems
GIAC Enterprises' Network Security Architecture

Version 4.0

By
Diane Johnson

Submitted August 6, 2004

Abstract Summary

Network Intrusion Prevention Systems are discussed in assignment one of this paper. The question is whether these systems have matured sufficiently to improve the posture of an organizations security without overwhelming the System Administrator. The topics include some analysis of the technologies strengths and weaknesses as well as future needs that Network Intrusion Prevention Systems might help to fill.

Assignment two addresses the Network Security Architecture Design for GIAC Enterprises. This design looks into the business requirements and considerations of GIAC Enterprises and addresses them through building a secure perimeter to protect the e-business focus of the organization.

Assignment three defines the Checkpoint Firewall 1 policy for GIAC Enterprises based on the business and access requirements detailed in the Network Security Architecture.

Table of Contents

Assignment 1: Future of Network Intrusion Prevention Systems— Friend or Foe?

Introduction

At every layer of security there is a System Administrator completing tasks, automating updates, and improving the organizations overall security posture through their diligence. But System Administrators today are spending more time keeping their systems current and secure than in years past. The challenge is that the window to apply updates grows shorter for each vulnerability and the release of associated exploits. The bad guys have become faster and more efficient in writing and releasing new malware code.

Gregg Keizer's article Gartner: Worms Jack Up the Total Cost of Windows brings out some excellent points about dealing with widespread worms. Keizer cites Gartner research director Mark Nicolett "The appearance of Sasser makes the shortest time ever -- just 18 days -- between the appearance of a vulnerability and the beginning of an attack." [1] The article goes on to note MSBlast, which took only 25 days to get to market, held the previous record. Given this short timeline between vulnerability and exploit, System Administrators cannot afford to combine patches and updates in quarterly or even monthly cycles anymore. When a new vulnerability is announced, everyone must stop everything and secure their systems.

While the issue is similar in every layer of information security defense, the future direction of various technologies will bring different impacts to an organization and their security architecture. Keizer recounts that Nicolett "recommended that enterprises boost spending on patch management and intrusion prevention software to keep ahead of worms." Mark Nicolett is quoted to have said: "Intrusion prevention gives enterprises some breathing room. . . .They don't have to panic when the vulnerability clock starts ticking." If we focus our attention on Network Intrusion Prevention defenses, we can explore the problem, understand future implications and determine if this defense mechanism is our friend or our foe.

Historical Relationship

Intrusion Prevention Systems (IPS) have grown out of Intrusion Detection Systems (IDS). It is valuable to understand the strengths and weaknesses of IDS so that we can analyze the current and future state of IPS. The IDS passively listens to network traffic and uses a library of signatures to detect suspicious activity or events. The signatures include strings of expected conditions within traffic that look like a particular exploit. When an event is detected the system will record the event in a log and send alerts about the event. The System Administrator receives the alert and then evaluates if the event is legitimate traffic or an actual attack. If the event is an attack, identified systems are investigated for compromises and cleaned.

There are significant weaknesses to the IDS process. Most obvious is the reactive and manual nature of the response activities. Specific weaknesses of IDS include:

1. IDS only detect attacks. This means that they are a reactive tool and not a

proactive tool.

2. IDS are signature-based systems. A signature must be written and applied before an IDS can detect an attack. Most signatures are based on exploits instead of vulnerabilities. The exploit must be in the wild before a signature is written and applied leaving windows of opportunities for attackers.
3. IDS generate a large number of false positive alerts. Many alerts turn out to be legitimate traffic that looked similar to an attack signature. To reduce false positives, extensive fine-tuning by administrators is necessary before the alert information is useful. In some cases, the fine-tuning may cause the IDS to miss the real attacks.
4. IDS use rudimentary blocking mechanisms. Because these devices are not in-line of the traffic, they must send commands to routers or firewalls and depend on these other devices to do the actual blocking. This means that the ability to block an attack once it is detected is not efficient. Many IDS are never set to block because of the lack of confidence in the detection capabilities and the lack of confidence in the blocking mechanisms.
5. IDS cannot stand up to the higher volumes of traffic that the internal network pushes through. Many IDS stop recording information or stop working completely when subjected to multi-gigabits of data.

The strength of IDS is that it is an excellent tool to use to identify compromised systems within a network once an outbreak has occurred. These devices can be placed at the perimeter or access layers of the network and will provide useful information to be used to clean up a compromised network.

The Network Intrusion Detection system seems to be a friend to the System Administrator at first glance. But it certainly comes with extra baggage. The IDS is a labor-intensive tool, it keeps the System Administrator working in reactive mode, and it does not provide sufficient protection to be a viable strategic investment.

Current State of Network IPS Technology

The Network Intrusion Prevention System (NIPS) is a system that is placed directly in the path of the traffic, or referred to as in-line. This placement allows the device to analyze all data and react by blocking malicious packets. NIPS technology has significantly matured over the last year. This improvement in technology has raised the level of confidence in the products. Gartner analyst John Pescatore identifies three criteria for an intrusion prevention system: "It must not disrupt normal operations. . . It must block malicious actions using multiple algorithms. . . It must have the wisdom to know the difference (between attack events and normal events)." [2] Several vendors now offer adequate NIPS solutions that meet Gartner's minimum criteria and offer other obvious benefits:

- There are NIPS products that do not disrupt business operations. These devices have been placed in-line of network traffic, even gigabit speed networks, and the inspection process latency is acceptable. The key to the success is that the hardware is built to handle the high speed. Vendors have used ASIC-based components and multi-gigabit backplanes to improve the throughput and meet

the high-speed performance needs.

- There are NIPS products that use multiple algorithms to inspect the traffic and make prevention decisions. Instead of simply depending on exploit-based signatures, IPS rules may be based on the underlying vulnerability, protocol deviations, or unusual behavior on the network. Much of this is due to improved ability of the IPS to comprehensively inspect traffic at the application layer. Some vendors may still rely heavily on signatures, but the signatures are based on the vulnerability and not the exploit. Behavior- and anomaly-based prevention techniques are available and are being heavily marketed.
- There are NIPS products that can distinguish between malicious traffic and legitimate traffic. The technique used to distinguish malicious traffic is the behavior- or anomaly-based algorithm. The baseline traffic pattern information of the network is used to determine what is normal and what is not normal. These baselines profile information such as thresholds for specific traffic that once reached can be accurately identified as an attack versus legitimate traffic. Tracking connection state helps with this concern, as the device understands more about the communication for each session. Other products will remember reconnaissance attempts to fictitious addresses and mimic the expected response. When suspicious attack actions are taken on these fictitious addresses, the device will alert and prevent the attack to the rest of the network.
- Labor investment to fine-tune profiles and signatures to the organization's environment as well as to monitor logs and update filters adds significant value to the security provided by the device. This work may be lessened with these newer NIPS; however, devoting the resources to this activity will allow the NIPS to do more blocking and improve the security posture of the organization.

The weaknesses of the current NIPS offerings are:

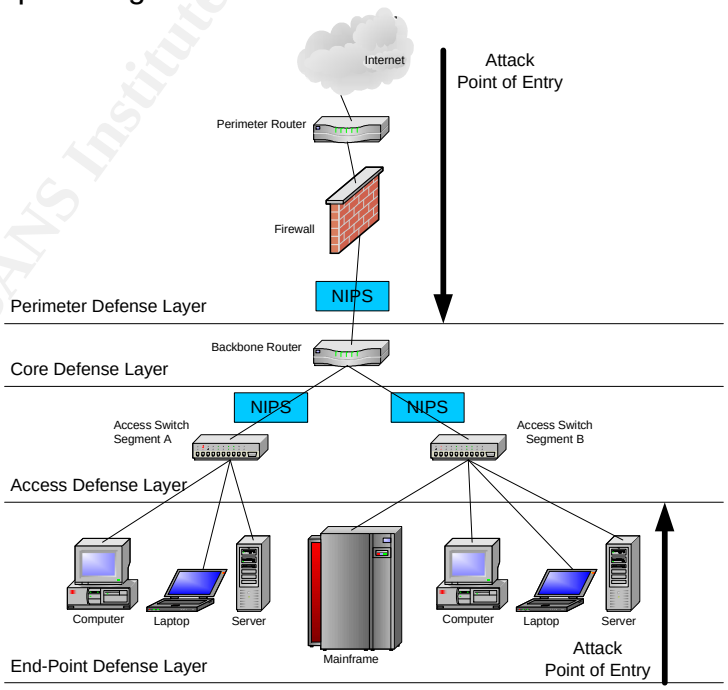
- Price point for gigabit speeds is very high, particularly for small to medium businesses.
- The most effective placement strategy is at all perimeter points as well as all access layer points of the network. This increases the price point.
- NIPS vendors have an Information Technology focus and do not provide for protections when an application is using a proprietary protocol riding on TCP/IP. This weakness has a limited scope and does not apply to GIAC Enterprises.
- "Zero-day" is touted as prevented by most of these NIPS. That claim depends on the definition used for "zero-day". One definition would be zero-day exploit is released for an already published vulnerability. A totally different definition would be zero-day exploit is released for an unpublished and unknown vulnerability. The second zero day scenario may be more difficult to prevent by the NIPS if the worm writer is particularly careful to disguise the traffic as legit.
- Many NIPS cannot inspect encrypted traffic. This issue still leaves SSL, SSH, and VPN traffic uninspected.
- Placement can leave holes in the defenses and the end-point layer of the network. Architects need to understand the risks that are being accepted based on NIPS placement within the network.

System Administrators can be relieved of many tasks associated with successful compromises because a great number of attacks are prevented by the NIPS. The extra baggage our friend Network Intrusion Prevention Systems brings in the current state of technology is mostly budgetary baggage. The products can do an adequate job of prevention in most scenarios as long as your budget is sufficient to deploy at perimeter and access layer points enterprise wide. Even with full network coverage, there is a tendency to be lulled into a false sense of security. These devices still leave holes such as potential for zero day issues, end-point local subnet compromises, or issues from encrypted sessions.

Defense In-Depth and Network Architecture

Defense In-Depth is defined by the SANS Institute as "the approach of using multiple layers of security to guard against failure of a single security component." [3] These multiple layers include a wide range of design elements and components. The diagram below shows typical network layers of defense. The most common points of entry for attacks are the network perimeter connections such as Internet or partner connections and the network end point connections such as laptops that walk around to other networks. These points of entry are where the Network Intrusion Prevention Systems will be most effectively placed. If you can secure each access point, then you can significantly contain the damage of a compromise that enters your network.

In this scenario, the NIPS can protect your core routers from a compromise that enters from either direction; the hosts on Segment A can be protected from a compromise that enters via Segment B; as well as the backbone routers and both Segment A & B can be protected from a compromise that enters via the perimeter. This compromise containment means that the System Administrators will only need to investigate and clean devices on Segment B, instead of the entire network if the compromise enters from a walk-in laptop on Segment B.



In addition to using multiple layers of the network to provide protection, Enterprises use diverse components to strengthen their defenses. The Perimeter Router, Firewall, Network Intrusion Prevention Systems all perform different functions yet work together to protect the network's information systems. Paul Criscuolo gave the definition for firewall versus IPS use during the SANS Institute hosted webcast on July 28, 2004, as: the Firewall is used to enforce policy and the IPS is used to verify traffic that does get through is legitimate. [4]

For the Network Security Architecture designed for GIAC Enterprises, dedicated Network Intrusion Prevention Systems do not yet play a role due to the high price point for these devices. GIAC will take advantage of the Primary Firewall's IPS features to prevent malicious attacks. At the Regional Offices, the Firewall/VPN servers include IPS features that will be used to protect these offices. GIAC will also install an Intrusion Detection System at the Internet perimeter. This device is more reasonably priced at this time and the next code revision should bring significant prevention capabilities. This diverse approach allows GIAC to keep their options open as the market continues to mature. Many experts believe that IPS will become an integral part of firewalls while others believe that putting all your protections in one device is asking for disaster. As GIAC Enterprises grows, IPS technology matures, and IPS prices are lowered, a project should be undertaken to evaluate, design, and deploy IPS technology through GIAC Enterprises infrastructure.

The Future of Network IPS Technology

The Information System Industry is shifting from the ideal that data, all of it, must be transmitted across the network as quickly as possible—to the ideal that only the legitimate data should be allowed to be transferred across the network as quickly as possible. Many crazy figures about the amount of malicious traffic on networks have been reported. The key fact is that there is malicious traffic that is impeding transmission of legitimate traffic and compromising information systems. Network Intrusion Prevention Systems play an important role in stopping this malicious traffic today and hopefully an even stronger role in the future.

Sales Engineers from at least seven major Network Intrusion Prevention System vendors have emphasized the latest buzz phrases that describe the future of NIPS technologies in terms of "embedded at every level," "evolution that will leverage your current investments," "virtually in-line," and "self-protecting networks." While these phrases evoke wonderful images of a more secure future, the focus of this discussion about the NIPS future will center around the effect developments may have on business needs and network security day-to-day operations.

Vendors have monetary motivation to continue to improve the NIPS product lines and mature the protection capabilities associated with traditional Information Technology systems. By improving this technology and by widespread adoption of the technology:

- NIPS will help the Information Technology industry to stay viable. The cycle of continuous patches, attacks, and compromises is giving the industry a bad name and reducing credibility for any application running on the currently preferred or

easy malware target. People at work and home are disillusioned and tired of the cycle.

- NIPS can buy time for organizations to properly QA and rollout patches, as many attacks will be effectively stopped. Business applications need to be tested with patches to properly identify and mitigate any incompatibilities the patch may introduce.
- NIPS will return the time System Administrators now spent on the stop, drop, and roll update fire drill to the System Administrator. This will allow them to do the other parts of their jobs.

In addition to protecting the traditional IT systems, there is a real need for information security technology to understand and protect the odd systems that are becoming part of every TCP/IP network. HVAC, phone switches, security cameras, physical entrance controls, and SCADA plant control systems are examples of devices that are interconnecting with Corporate networks. As noted in the March, 2004, GAO Report to Congressional Requestors, *CRITICAL INFRASTRUCTURE PROTECTION Challenges and Efforts to Secure Control Systems,*

> Information security organizations have noted that a gap exists between currently available security technologies and the need for additional research and development to secure control systems. Research and development in a wide range of areas could lead to more effective technologies. For example, although technologies such as robust firewalls and strong authentication can be employed to better segment control systems from external networks, research and development could help to address the application of security technologies to the control systems themselves. Other areas that have been noted for possible research and development include identifying the types of security technologies needed for different control system applications, determining acceptable performance trade-offs, and recognizing attack patterns for use in intrusion detection systems. [5]

Of the seven companies I spoke with regarding NIPS research, only two vendors were able to confirm that their company was spending research funds in this area.

Improved Intrusion Prevention Systems for non-IT specific systems is an important part of NIPS future. With these types of protection tools, air gaps between networks would be less necessary; the amount of duplication of effort and resources would go away; and the amount of tedious packet analysis to build custom signatures would be reduced. The effect on the organization would be a real cost savings and a stronger security posture for these sensitive devices. If NIPS could effectively prevent targeted attacks to these odd systems along with the normal IT systems, they would truly be a friend to the System Administrator.

Assignment 2: Network Security Architecture for GIAC Enterprises

GIAC Enterprises provides fortune cookie sayings to bakeries worldwide. The Corporate office is located in the United States with four regional satellite offices geographically distributed around the world. Our products include custom fortunes for those special occasions, quotes from famous historical entities, and traditional sayings from philosophical tenets. GIAC Enterprises operates most business transactions with customers, suppliers, and partners through Internet communication channels. This e-commerce focus creates security challenges that need to be met while still providing for specific business requirements. This section defines the network security architecture and the considerations and accommodations necessary to meet business requirements.

Business Requirements

Business requirements identified for GIAC Enterprises customers include availability of services at all hours of the day. Established customers need to have the ability to conduct transactions via the Internet including placement and status tracking of orders, payment processing, statements, order history, and catalog searches for traditional and modern theme fortune cookie sayings. One-time customers need the ability to order via the Internet from our catalog or custom sayings and complete the transaction including payment, printing, shipping, and integration of cookie orders with partner bakeries.

GIAC Enterprises requires on-going business relationships with vendors and suppliers such as shipping agencies, office and paper suppliers, information technology equipment and services vendors, and facilities management providers.

GIAC Enterprises depends on strong business partnerships for financial, sales, marketing, human resources, legal, and information technology integration services. We also partner with several bakeries to provide our customers streamlined shopping. These partnerships, while overseen by experienced internal staff, add complexity to our security architecture because of the need to protect transactions and communications.

In business, face-to-face relationships and human interactions are important. For our regional satellite offices, we need to provide the ability to conduct meetings with customers and staff over distances using video or web conferencing, email, and voice communications. The sales force requires the ability to interact with enterprise systems to provide appropriate assistance to their customers.

GIAC Enterprises staff is positioned internally and externally to the network. Historians and writers of fortune cookie sayings are contracted employees and are usually accessing resources from external locations. We also require that employees be given the opportunity to work from home regularly. All staff interacts with partners, suppliers, customers and other employees as needed for their respective area of responsibility. The Internet is an important part of this interaction as well as an important part of our ongoing fortune cooking saying research.

General information about GIAC Enterprises products, services, support, and history of

fortune cookies and the sayings needs to be available to the public without providing access to privileged information.

Access Requirements

Customers are provided access through GIAC Enterprises' secure web portal services to applications and systems. This service has the following requirements:

- The service secures connections from external networks with SSL encryption to protect the data of our customers as it traverses the hostile Internet.
- No other protocols are open to this server or listening on this server. Hardening of the system minimizes the exposure risk and potential infection vectors available to compromise the system.
- The portal server is logically located in the Demilitarized zone (DMZ) of the network separated from the internal network by a stateful inspection firewall. Firewall rule set restricts this server to communicate only with necessary systems. This design reduces the potential of compromise to systems within the internal network.
- Authentication and authorization parameters are stored within the database serving the portal. Access is granted to only the applications and data for which the individual authenticated is given permissions, which protects the data from inadvertent exposure to other customers and competitors.
- Traffic flow to the DMZ Customer WebPortal from the external network are restricted to port 443/SSL only. Traffic from the internal network to the DMZ is also restricted to port 443/SSL. Wherever possible, traffic flow from the internal network to the DMZ by an application that asks the DMZ server if it has any new requests for data. This restricts flows from the DMZ to the internal servers down to established flows only and enhances the security of the flow to the internal network.
- Weekly vulnerability audits of externally facing servers are conducted by 3rd party auditors and compared against the baseline to provide continued assurances that the security policy is still in effect.
- All other protocols and services are explicitly denied.

Our staff would need access to communication with vendors and suppliers via:

- Internet email, SMTP, smime.
- Internet browsing, ftp, ssl, dns, vpn.

No back-door dial-in capabilities are provided to vendors or suppliers. Dial-in access bypasses the security monitoring available at the perimeter. All other protocols and services are explicitly denied.

GIAC Enterprises partners with companies that have already enhanced their systems to provide sufficient security to our network using the following guidelines:

- All connections with partners' networks use Virtual Private Network (VPN) architecture. VPN provides high levels of encryption to protect sensitive data and secure authentication to identify entities prior to granting access to GIAC Enterprises network.
- Virtual Private Network interoperability is key to all partnerships. Interoperability

of systems allows us to reduce costs by working with existing infrastructure for new partnerships.

- We require a minimum level of encryption of DES and prefer to establish VPN tunnels using 3DES or AES encryption algorithms whenever available. It is important that the level of encryption used be secure enough to protect sensitive data for the life of that data. Since some of our communications involve financial information, we want to protect that long living data appropriately.
- Vestibule Zone Architecture is used for all VPN servers. The concept here is to bring the tunnel through the external firewall and terminate them in a fortified Vestibule Zone. Communications from this Vestibule Zone are then limited by a stateful inspection firewall to the internal network to identified services necessary for partnerships. This architecture allows for monitoring by Intrusion Detection Systems as well as the vpn and firewall logs.
- Services identified as necessary to conduct business should be limited to specific ports and protocols traversing from the Vestibule Zone to the internal network. SQL, FTP, SSH, SSL, and DNS are all allowed services. Each service is enabled as needed for specific partners.
- Hosts within the internal network, which need to be accessed by partners, will be specifically identified. This allows system administrators for those hosts to properly manage the host-based security.
- No services utilizing all dynamic ports or large port ranges will be allowed. No connections requiring access via Microsoft RPC ports are allowed. Limiting the ports allowed to communicate with the internal network provides for stronger firewall rule sets and minimizes opportunities for circumventing these measures.
- All connections between the Vestibule Zone and external networks use the standard vpn ports, which will minimize exposure of the hostile Internet.
- No back-door dial-in capabilities are provided to partners. Dial-in access bypasses the security monitoring available at the Vestibule Zone.
- Communication between staff and partners should use secure Internet e-mail as the first choice. SMTP Internet e-mail is optionally available as not all partners are setup to work with secured e-mail. Staff is expected to not send sensitive information through unsecured email.
- All other protocols and services are explicitly denied.

The regional satellite offices use the same architecture established for customers and partners following these restrictions:

- For customer account tasks the sales forces uses the web portal. This strategy allows staff to gain familiarity with the tools we ask our customers to use as well as utilizing the same infrastructure and thereby reducing costs.
- For other tasks requiring access to systems within the Enterprise, the satellite office uses a VPN site-to-site connection to the Vestibule Zone. This strategy again reduces costs associated with infrastructure and support as well as providing central locations for ingress to the network.
- Services identified as necessary to conduct business should be limited to specific ports and protocols traversing from the Vestibule Zone to the internal network. SQL, FTP, SSH, SSL, and DNS are all allowed services. In addition, ICA clients

may be used to access MetaFrame servers on the internal network.

- Services are procured through a 3rd party for web conferencing and video conferencing. This decision allows GIAC Enterprises to use the conference server without opening additional protocols and ports to or from our network.
- No back-door dial-in capabilities are provided to sales force. Dial-in access bypasses the security monitoring available at the perimeter and Vestibule Zone.
- Communication from and to sales staff should use secure Internet e-mail as the first choice. SMTP Internet e-mail is optionally available as not all customers are setup to work with secured e-mail. Staff is expected to not send sensitive information through unsecured email. Staff is not provided with POP or IMAP e-mail download capabilities.

GIAC Enterprises egress communications from the network are restricted where it is possible to identify the requirements. Our staff would need access to communication as outlined below:

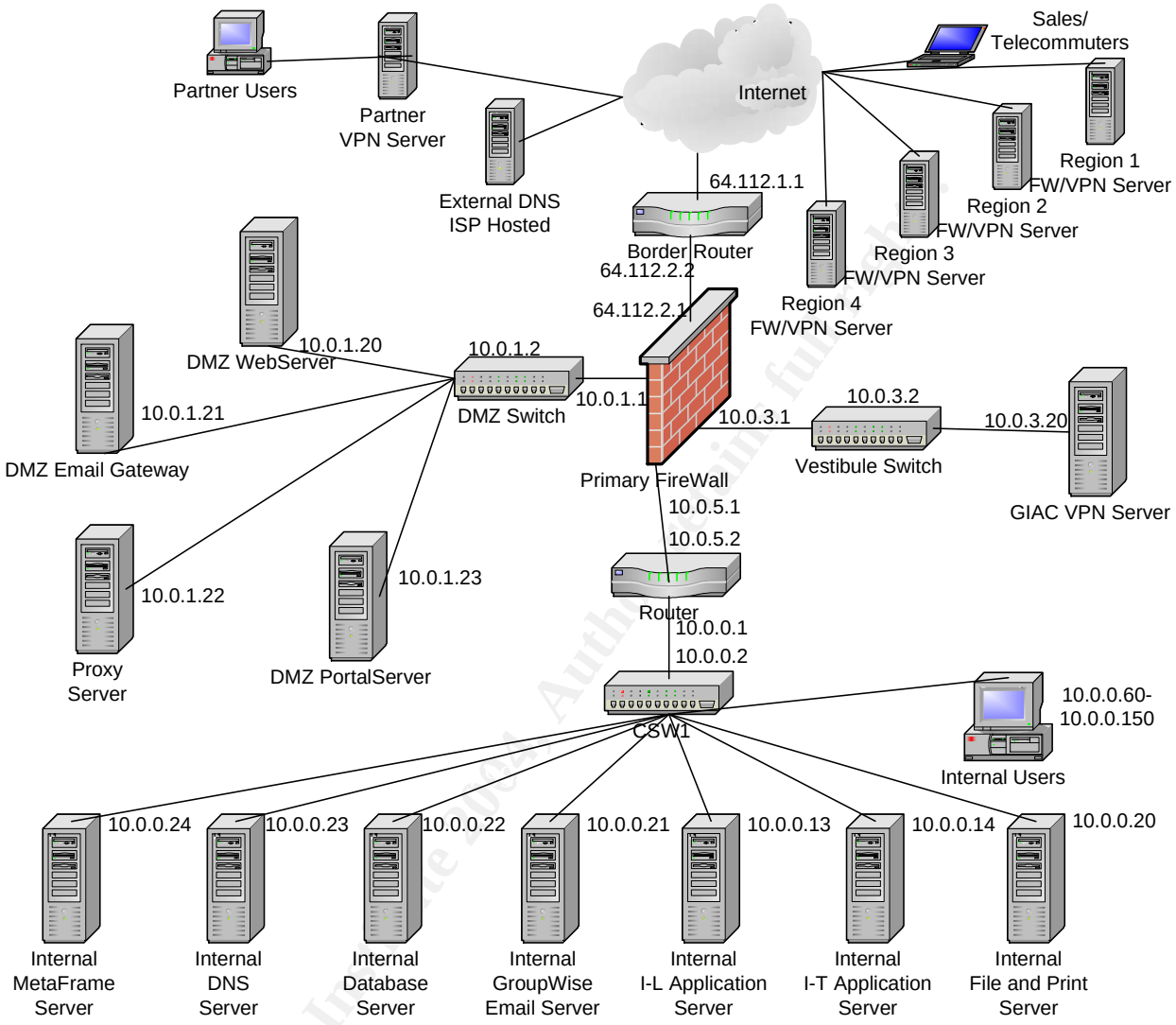
- Internet e-mail through use of SMTP or smime is allowed egress services and protocols. Communication from and to staff should use secure Internet e-mail as the first choice. SMTP Internet e-mail is optionally available as not all contacts are setup to work with secured e-mail. Staff is expected to not send sensitive information through unsecured email. Staff is not provided with POP or IMAP e-mail download capabilities.
- Email gateways scan for malicious content within all inbound and outbound Internet e-mail. E-mail communication is the top infection vector used by worms, viruses, and Trojans. Locking down the protocol types allowed and scanning for malicious content with an up-to-date signature product provides a healthier computing environment.
- Internet browsing, ftp, ssl, dns, and vpn are all allowed egress services, applications, and protocols. These are common services we know that staff need to use to conduct business. Web and ftp traffic will be configured to pass through the proxy server.
- Internet browsing and other external access from internal servers, switches, and routers is explicitly locked down, as these devices do not have a need for this access. Disallowing outbound connections from servers reduces exposure potential for many exploits.
- Web and ftp traffic is scanned at the proxy server for malicious content. Many zero-day exploits use web browsing as its infection vector and scanning for malicious content with an up-to-date signature product provides a healthier computing environment.
- DNS is setup in a split DNS configuration. The internal and external DNS are hosted on different servers with different domains hosted on each server.
- All other protocols and services are explicitly denied.
- Administration of devices will be secured as much as possible.
- Logging of security events for crucial components will be two-prong to enable off-system consolidated security information management database. This provides extra security of log files as many hackers and exploits cover their tracks by deleting pertinent log entries. Off-system logging makes erasing evidence more

difficult for the hacker.

Public access to our Network Architecture includes the following restrictions:

- Web browsing access to the public web server is permitted. This allows connections using port 80/http from external networks. That service port is the standard application used over the Internet.
- Any transactional activities are processed by links to the SSL transaction portal for one-time orders.
- No other protocols are open to the web server or listening on the web server. Hardening of the system minimizes the exposure risk and potential infection vectors available to compromise the system.
- The web server is logically located in the DMZ separated from the internal network by a stateful inspection firewall. Firewall rule set restricts this server to communication only with necessary systems. This design reduces the potential of compromise to systems within the internal network.
- Weekly vulnerability audits of externally facing servers are conducted by 3rd party auditors and compared against the baseline to provide continued assurances that the security policy is still in effect.
- All other protocols and services are explicitly denied at the firewall positioned prior to the DMZ.
- Known source ip addresses and ports that are used as attack points will be filtered at the border router prior to the firewall. These lists are available from various security sources. This filtering rarely impedes legitimate traffic and it does ease the impact to the firewall for suspicious activity such as large-scale port scans and current worm activity. Recommendations for changes will be reviewed weekly and as needed for hot activity.
- Ingress filtering for spoofed addresses, such as the net block of addresses that we own will be filtered at the border router.

Diagram of GIAC Enterprise Network



Security Architecture Components

Border Router

Brand:	Cisco Systems 7200
Version:	Cisco IOS 12.2(24)
Purpose:	The filter router provides connectivity to the Internet Service provider (ISP).
Security Function:	The security function of the Border Router is to block the simple ip addresses known to cause massive disruption or instability on the Internet. This reduces the amount of traffic that the firewall needs to interpret and process.

Placement:	The filter router is placed at the edge of the Enterprise perimeter. It is the connection to the ISP. It is the first level of defense against the hostile Internet.
Strength/Weakness:	The router moves traffic very efficiently. This device is not designed to act as the main filtering device; therefore, limiting the access control list rules to basic overarching restrictions is best.
Mitigation Techniques:	Using the router filtering to work at the ip address level of communication allows the router to efficiently move traffic while blocking traffic the network never needs to see such as spoofed sources from our own net block. Use other layers of defense such as intrusion prevention sensors to alert and act on attack conditions and firewalls to filter traffic.
Decision Factors:	Technical factors that influenced the decision for this device's use are that there is a strong body of knowledge available for support of the device within the IT support services. This device fits well within budgetary guidelines.

Primary Firewall

Brand:	Nokia IP530 hardware running Check Point FW-1 software
Version:	IPSO version 3.8 build 34; Check Point FW-1 version NG with AI R55 with all hot fixes
Purpose:	Controls and audits access to security zones.
Security Function:	The firewall inspects traffic packets destined between security zones and allows or denies the traffic based on defined rule sets and policies. The firewall chosen is a stateful inspection firewall that looks beyond just the destination/source address and ports and evaluates the packets through application layers. The firewall maintains a dynamic state table related to current traffic and evaluates subsequent connections with this information. This firewall also has intrusion prevention capabilities that will be utilized to prevent malicious traffic.
Placement:	The firewall is placed in-line just inside the perimeter after the ISP router. The firewall has four interfaces for different security zones and rule sets. • First interface connects to the external network • Second interface connects to the DMZ network • Third interface connects to the Vestibule Zone network • Fourth interface connects to the internal network
Strength/Weakness:	Firewalls filter traffic very well at port and protocol levels. When deep packet inspection at the application layers of the OSI model is necessary, traffic through a firewall may be slowed if the firewall is not designed to handle this added load.
Mitigation Techniques:	Use the firewall to filter for the basic malicious traffic as available from the vendor. Use other layers of defense such as

	the proxy server to analyze and restrict malicious http and ftp requests and the webshield to analyze and restrict malicious smtp content.
Decision Factors:	Technical factors influencing this choice include: the product is rated highly within the industry, the IP530 model can expand to provide gig interfaces, the day-to-day operation tasks are easily managed through the management station, and it is one of the firewalls that is inspecting traffic at the application layer. The 50-user license for the firewall did not push out the budget appreciably and no political factors influenced the decision. Any internal firewalls should be from a different vendor to provide appropriate protection.

Virtual Private Network Server

Brand:	Checkpoint VPN1
Version:	SecurePlatform R55 with all hot fixes
Purpose:	The VPN Server acts as the termination point for Virtual Private Network tunnels.
Security Function:	Its security function is to provide encryption of data across the untrusted Internet, to act as the authentication and authorization service for connections with partners' networks as well as to secure connections used by regional satellite offices and staff across the untrusted Internet.
Placement:	The VPN server is placed inside the firewall in the Vestibule Zone network segment. This design allows the VPN sessions to be terminated within a controlled environment while still giving us the opportunity to monitor and restrict traffic flows that continue to the internal network.
Strength/Weakness:	The VPN server provides strong authentication and a means of more granular authorization and access to network resources once authenticated. This system also allows us to build audit trails and monitor usage. The downside to VPN service is that once the tunnel has been established, it is an extension of the network.
Mitigation Techniques:	Configure the VPN community to require user authentication, restrict access where possible, and validate security policy requirements across the tunnels such as current patches and anti-virus signatures.
Decision Factors:	Technical factors influencing this purchasing decision are that the same management server and interface is used to manage both the firewall and vpn gateways. This reduces support costs like training and number of servers necessary to support security components.

Network Based Intrusion Detection System Sensors

Brand:	Cisco 4235 Intrusion Detection Sensors
Version:	4.1(4) S106
Purpose:	IDS sensors passively listen to network traffic and detect malicious content.
Security Function:	Its security function is to analyze traffic flows at critical network points and identify, correlate, and alert on potential security breaches and other suspicious activities.
Placement:	Sensors are most useful when placed on the inside of new security zones. This placement allows monitoring of traffic for suspicious activity as it leaves or enters new zones. Sensors are also useful when placed at strategic backbone locations to monitor activities within the network. This appliance can be quickly relocated based on ever-changing needs of the network.
Strength/Weakness:	This device is an easy to install appliance that can be quickly moved to other logical locations if suspicious activity is suspected. Many normal activities can produce false positive readings, which make the information less useful until tuned. The database of signatures is quite useful in pointing out benign triggers.
Mitigation Techniques:	IDS information requires tuning to the specific computing environment. Once tuned, these sensors provide valuable information.
Decision Factors:	This investment should be considered a tactical purchase at this point. The dollars invested will bring value to the security of the Enterprise and help as noted above. The long-term strategy should be to replace this device with Intrusion Prevention technology. This may involve moving to a different vendor if Cisco continues to be slow with this service. Current Intrusion Prevention technologies are quite expensive for smaller organizations.

Network Segmentation Security Zone Scheme

Segmenting networks into security zones gives an enterprise opportunities to manage network traffic between zones.

External Addresses: 64.112.1.0/24 (This address space is randomly picked for the purposes of this assignment and has not officially been assigned for my use. IP addresses are assigned by ARIN to organizations or provided through the enterprises ISP.)

External Segment Purpose: To provide publicly addressable faces to services hidden in other security zones. This protects the internal addressing scheme and makes it a little more difficult for an attacker.

Demilitarized Zone (DMZ) Addresses: 10.0.1.0/24

DMZ Segment Purpose: To provide public and customer access to services in a controlled environment while minimizing the risk to Enterprise Corporate systems housed on the Internal network.

Vestibule Zone Addresses: 10.0.3.0/24 for VZ; 172.16.250.0/24 & 172.17.0.0/24 for VPN Address Pool.

VZ Segment Purpose: To terminate business-to-business VPN sessions as well as client-to-server VPN sessions within a controlled environment while still giving us the opportunity to monitor and restrict traffic flows that continue on into the internal network.

Internal Addresses: 10.0.5.0/24 Connecting Segment; 10.0.0.0/24 Internal Segment; others will be defined as needed.

Internal Segment Purpose: To house the computing environment necessary to GIAC Enterprises business functions. This is the general-purpose corporate network.

Defense In-Depth

A powerful and effective security strategy is commonly referred to as defense in-depth. This strategy uses multiple layers of security to deter, protect, defend, and recover from the expanding breadth of threats. The security architecture in this paper adheres to the defense in-depth principle by allowing different network elements to manage the threats for which they are most suited; by designing a network cordoned off for function and access theology; and by giving inner layers granular access control and data filtering support.

Elements of the Defense in-Depth strategy pinpoint threats at various layers for which they are responsible and apply appropriate security measures at that point. Defense layers and their respective values are listed below.

- Perimeter Router protects itself and the firewall directly behind it by dropping traffic that one should never accept into their network based on simple protocol rules. This is our first line of defense.
- The firewall controls and audits access to the network by permitting and denying traffic flows based on ports and protocols or services. This device filters traffic that is traversing between security zones.
- VPN systems protect data traversing untrusted networks by encrypting communication sessions that have passed some form of authentication test. This provides for secure use of less expensive communications channels instead of maintaining isdn or T1 connections to satellite offices, partners, and service providers.
- Intrusion Detection Systems watch the network or host for suspicious activity. A network IDS can be deployed at strategic locations across the infrastructure to detect intrusions. A host IDS can be deployed on strategic servers to detect intrusions. These sensors can be integrated with analysis and alerting systems to correlate results and enable administrators or systems to react accordingly.
- Virus Protection actively scans for new threats on servers, workstations, email gateways, and web proxy gateways which inhibits the ability for malware to enter and spread within your environment.

- Patch Management is a process that all system administrators undertake to install vendor recommended security patches when they become available. This process mitigates risk associated with known vulnerabilities that can and will be turned into active exploits used to compromise systems.
- System Security Assessments performed on a regular basis help to point out security holes or changes from a baseline state such as missing patches, unnecessary services, and insecure accounts or disk shares.
- Building a homogenous and diversified environment has been shown to be more secure. This architecture design takes the approach of using different equipment for different functions instead of relying on one security device and/or one security vendor to do it all.
- Internal security zones demarcated with firewalls and IDS sensors further enhance protection for critical data or systems within an enterprise. They also provide easy segmentation for internal business continuity of critical systems in the event of a major cyber event.

This architecture document does not address the entire security strategy necessary for an organization; but, rather, the basic plumbing needed to start protecting access and to define a perimeter of the network. The implementation of these perimeter fortification devices frames the external security zones to act as the first layers of GIAC Enterprises cyber defenses.

Assignment 3: Primary Firewall Policy

The information contained in the following section will detail the security policy needed for the key component of GIAC Enterprises' perimeter network security: Primary Firewall. This policy is based on the business and access requirements and considerations defined in the Network Security Architecture section of this document.

Firewall Access Rule Set Requirements

The Primary firewall rule set policy supports the security stance of the organization through the specific requirements detailed below.

- Firewall is to be dedicated to filtering traffic. No general purpose computing services are to be hosted on the device.
- Data should not be allowed to flow between security zones except through the firewall.
- Firewall and operating system should be updated with security patches in a timely manner.
- Administration of the system will be conducted over encrypted sessions authenticated with individual named user accounts from the internal network only and by dedicated administration staff.
- Logging of security events will be captured on separate logging server for correlation and security of information.
- Filters should be set to block ip spoofing attacks and hide internal addresses.
- Malicious traffic rules will be set to filter specific known attacks.
  - ❖ Denial of Service: Teardrop, Ping of Death, LAND.
  - ❖ IP and ICMP: Max Ping Size at 69,Packet Sanity.
  - ❖ Application Intelligence—Web: General Http Worm Catcher
  - ❖ Application Intelligence—Web: Http ascii only request headers
  - ❖ Application Intelligence—Web: Http ascii only response headers
  - ❖ Application Intelligence—Web: Peer to peer turned off all types
  - ❖ Application Intelligence—Web: Cross site scripting protection on
  - ❖ Application Intelligence—Mail: SMTP Content
  - ❖ Application Intelligence—Mail: Mail and Recipient Content
  - ❖ Application Intelligence—FTP: Bounce
  - ❖ Application Intelligence—MS Networks: File and Print Sharing CIFS Worms
  - ❖ Successive Events Alerting
  - ❖ Others as identified
- Filters will be set for the following traffic flows

Host	Flow	Host	Service	Action
External	→	DMZ Web	http	Allow
External	← →	DMZ Email Gateway	Smtp	Allow
External	←	DMZ Proxy	http, 443, ftp, DNS	Allow
External	→	DMZ Portal	SSL	Allow
External	← →	VPN	VPN Ports	Allow
External	→	All others	All	Deny

DMZ Email GW	← →	Internal Email Server	Smtp	Allow
DMZ Proxy	←	All Internal hosts	80, ftp, 443, DNS	Allow
DMZ Portal	←	Internal Database	Sqlnet2	Allow
DMZ Switch	←	Internal Switch	Ssh2	Allow
VZ VPN/Natted	← →	Internal DNS	Dns	Allow
VZ VPN Natted	← →	Internal MetaFrame	MF ICA ports	Allow
VZ VPN Natted	← →	Internal Database	Sqlnet2	Allow
VZ VPN Natted	← →	Internal email	SSL	Allow
VZ VPN Natted	← →	DMZ Portal	SSL	Allow
VZ Switch	←	Internal Switch	SSH2	Allow
Internal Servers	← →	Anything else	All	Deny
Internal Wkstns	→	DMZ Web and Portal	ftp, http, https, ssl3, dns, icmp requests.	Allow
Internal Wkstns	← →	Anything else	All	Deny
Internal Router	← →	Anything else	All	Deny
FW Admin wkst	→	Firewall	Ssh, ftp, ssl, checkpoint specific	Allow
Anything else	→	Firewall	All	Deny

Importance of Firewall Rule Order

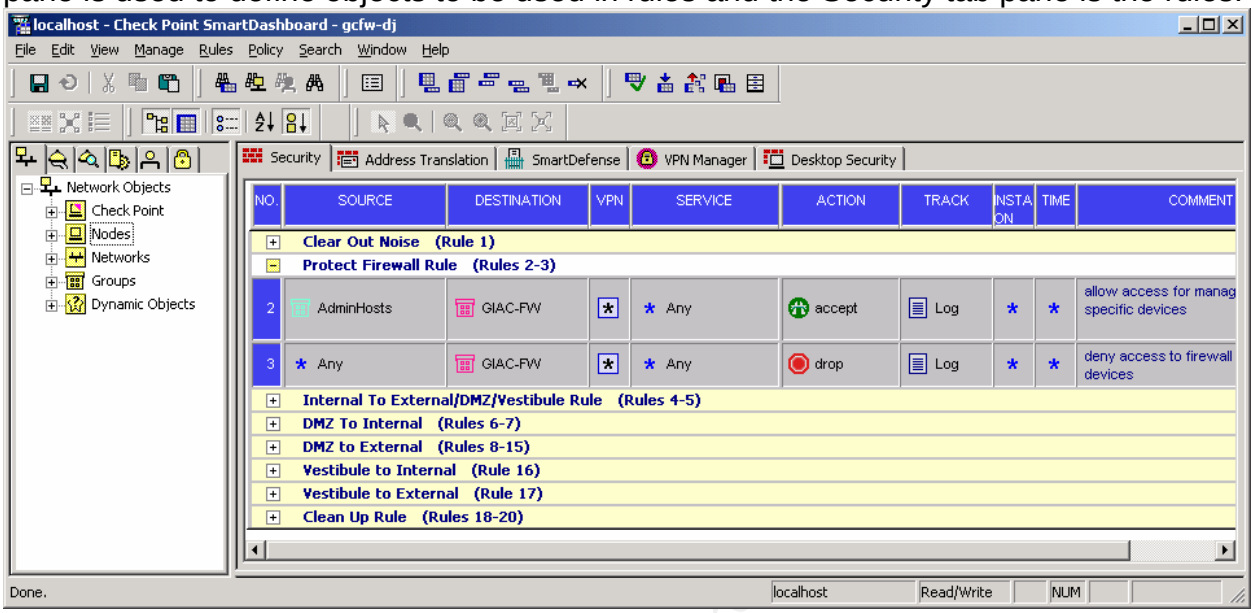
Checkpoint describes their Security Rule Base Fundamental Concept as "That which is not explicitly permitted is prohibited."[6] Rules are applied sequentially such that packets are tested against each rule in the order that the statement is listed in the configuration. Once a match is made, the rule is applied to that packet and no further checking against the rule set is conducted. If a lenient permit rule is listed before a specific deny rule, the packet passes right on through without ever being tested against the deny rule. The best practice of rule set order is:

- Place more specific rules first.
- Place more general rules last.
- Include a stealth rule to prevent any direct access to the firewall and a cleanup rule to drop all traffic that is not explicitly permitted and log those attempts.
- Checkpoint Firewall-1 has a set of implied rules that intermix within your defined rule base as applied first, before last, or last. These implied rules must be reviewed and evaluated for the proper order and usage based on GIAC Enterprises environment.
- Anti spoofing is not set as a rule, but is defined based on the interface and networks associated with each interface at the gateway topology properties.
- Several application layer services are inspected for content and rules can be refined for this feature using the smart defense rules.

Firewall Objects, Rules, Elements, and Syntax

Smart Dashboard is the application used to define Checkpoint objects used in firewall rules and policies.

The diagram below shows the main screen of SmartDashboard. The Network Objects pane is used to define objects to be used in rules and the Security tab pane is the rules.

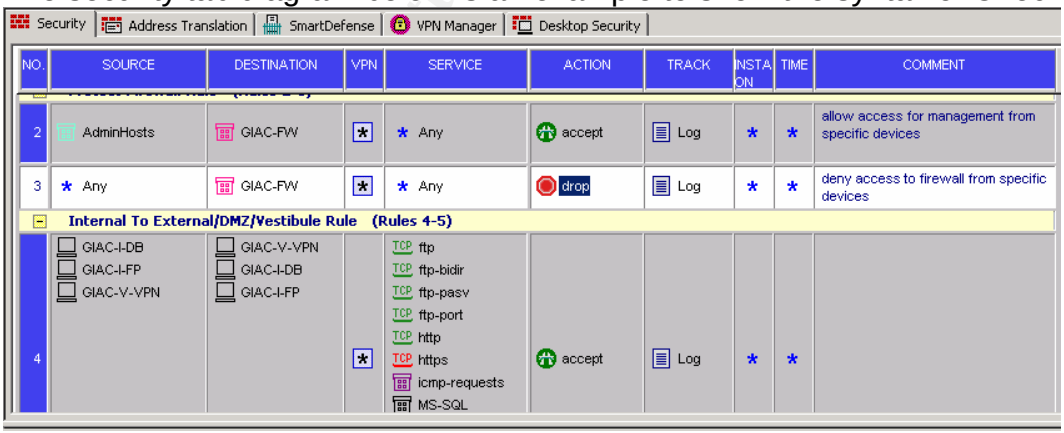


The table below lists the initial objects to be included in the Firewall Policy.

Object Type	Object Name	Detail Information
Gateway	GIAC-FW	IP Address: 10.0.5.1 Version: NG with AI Products: FW-1 Topology: Automatic Fill
Nodes	GIAC-D-CSW2	IP Address: 10.0.1.2
	GIAC-D-Portal	IP Address: 10.0.1.23 NAT Addr: 64.112.2.241
	GIAC-D-Proxy	IP Address: 10.0.1.22 NAT Add: 64.112.2.242
	GIAC-D-SMTP	IP Address: 10.0.1.21 NAT Add: 64.112.2.243
	GIAC-D-Web	IP Address: 10.0.1.20 NAT Add: 64.112.2.214
	GIAC-V-VPN	IP Address: 10.0.3.20 NAT Add: 64.112.2.244
	GIAC-V-CSW-3	IP Address: 10.0.3.2
	GIAC-I-DB	IP Address: 10.0.0 22
	GIAC-I-DNS	IP Address: 10.0.0.23
	GIAC-I-MF	IP Address: 10.0.0.24
	GIAC-I-SMTP	IP Address: 10.0.0.21
	GIAC-I-FP	IP Address: 10.0.0 35
	GIAC-I-CSW1	IP Address: 10.0.0.2
	GIAC-I-R1	IP Address: 10.0.5.2
	GIAC-I-T	IP Address: 10.0.0.14

Object Type	Object Name	Detail Information
	GIAC-I-AdmPC	IP Address: 10.0.0.60
	GIAC-I-L	IP Address: 10.0.0.13
Networks	GIAC-External	Address: 64.112.2.0 Mask: 255.255.255.0 NAT: empty
	GIAC-Vest	Address: 10.0.3.0 Mask: 255.255.255.0 NAT: empty
	GIAC-DMZ	Address: 10.0.1.2 Mask: 255.255.255.0 NAT: empty
	GIAC-V-NAT	Address: 172.16.0.0 Mask: 255.255.255.0 NAT: empty
	GIAC-Internal5	Address: 10.0.5.0 Mask: 255.255.255.0 NAT: Hide behind gateway
	GIAC-Internal0	Address: 10.0.0.0 Mask: 255.255.255.0 NAT: Hide behind gateway
Groups	GIAC-ProtectedNet	Include: GIAC-Internal5 GIAC-Internal0
	AdminHosts	AdminPC MgmtStation
	GIAC-VPN-NATTED	GIAC-V-NAT

The security tab diagram below is an example to show the syntax of Checkpoint rules.

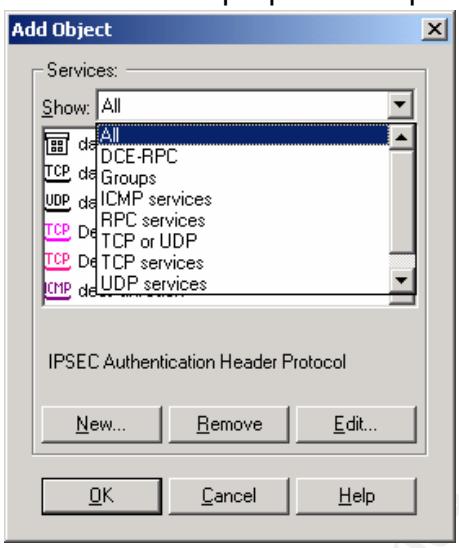


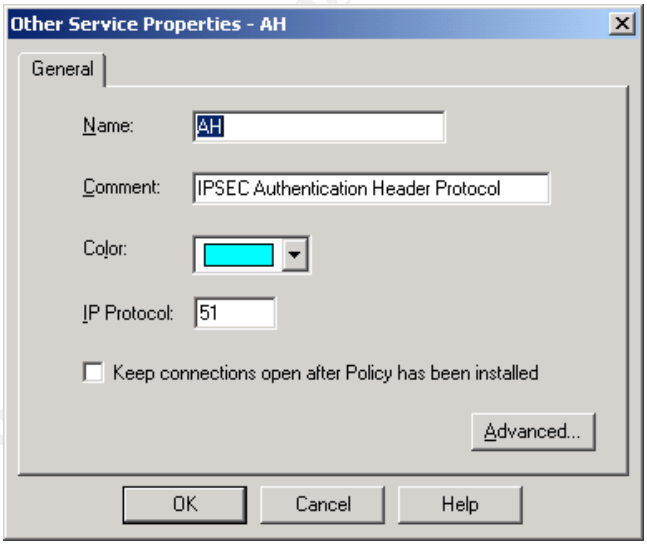
Check Point firewall rule number three says that traffic from any source whose destination is the GIAC Firewall using any service will be dropped and logged. This rule is positioned just below rule number two that accepts traffic from the firewall administration workstations and management server sources defined in AdminHosts group. Take note that rule number two allows “any” service from these management

stations. This is how the initial rule set for testing was defined. The service will be refined and tightened down prior to implementation.

The elements we will use for building GIAC Enterprises firewall policy are:

- Source and Destination: This can be any object such as a host, gateway, network, or group. These fields can be negated to define that the source or destination is not a particular object.
- VPN: We will not be using this element.
- Service: This includes the ports and protocols that will be defined to narrow down access. Many services are predefined. You can create your own custom services or edit properties of predefined services.





- Action: The actions that can be taken by the firewall are accept, drop, or reject. With reject as reset packet is sent and the connection is closed.
- Track: This sets the logging or alerting options.

Firewall Rule Set Defined for GIAC Enterprises

The following screen prints display the Checkpoint Rule Set defined for GIAC Enterprises. The comment column includes a description of what each rule accomplishes.

I have used rule headers to describe the basic grouping of the rules. The rules pictured below clear out noise the network does not need and protects the firewall itself.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Clear Out Noise (Rule 1)								
1	* Any	* Any	*	UDP bootp UDP rip	drop	- None	*	*	Drop all rip and dhcp requests. do not log
	Protect Firewall Rule (Rules 2-3)								
2	AdminHosts	GIAC-FW	*	* Any	accept	Log	*	*	allow access for management from specific devices
3	* Any	GIAC-FW	*	* Any	drop	Log	*	*	deny access to firewall from specific devices

The rules pictured below are those necessary for traffic between the internal network and the External, DMZ and Vestibule security zones as well as the DMZ to Internal.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Clear Out Noise (Rule 1)								
	Protect Firewall Rule (Rules 2-3)								
	Internal To External/DMZ/Vestibule Rule (Rules 4-9)								
4	GIAC-I-DB GIAC-VPN-NATTED	GIAC-I-DB GIAC-VPN-NATTED	*	sqlnet2	accept	Log	*	*	VZ-VPN access to Internal Database
5	GIAC-V-VPN GIAC-I-DNS GIAC-VPN-NATTED	GIAC-V-VPN GIAC-I-DNS GIAC-VPN-NATTED	*	dns	accept	Log	*	*	VZ-VPN access to Internal DNS Server
6	GIAC-I-MF GIAC-VPN-NATTED	GIAC-I-MF GIAC-VPN-NATTED	*	TCP http TCP https TCP Citrix_ICA UDP Citrix_ICA_Browsing	accept	Log	*	*	VZ-VPN access to Internal MetaFrame server
7	GIAC-I-SMTP GIAC-VPN-NATTED	GIAC-I-SMTP GIAC-VPN-NATTED	*	TCP https	accept	Log	*	*	VZ-VPN access to Internal Email Web Client
8	GIAC-D-Portal GIAC-VPN-NATTED	GIAC-D-Portal GIAC-VPN-NATTED	*	TCP https	accept	Log	*	*	VZ-VPN access to Internal DMZ Portal
9	GIAC-I-CSW1	GIAC-D-CSW2 GIAC-V-CSW3	*	TCP ssh_version_2	accept	Log	*	*	Access between internal switches and DMZ/VZ switches defined to ssh version 2
	DMZ To Internal (Rules 10-11)								
10	GIAC-D-Portal GIAC-I-DB	GIAC-I-DB GIAC-D-Portal	*	sqlnet2	accept	Log	*	*	Access between DMZ Portal and Internal Database defined to sqlnet2
11	GIAC-D-SMTP GIAC-I-SMTP	GIAC-I-SMTP GIAC-D-SMTP	*	TCP smtp	accept	Log	*	*	Access between DMZ Email Gateway and Internal Email defined to smtp

The rules pictured below are those necessary to traverse between the DMZ and Vestibule zones to the External Internet zone.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	DMZ & Vestibule to External (Rules 12-18)								
12	GIAC-D-Proxy	GIAC-ProtectedNet	*	TCP http TCP https TCP ftp TCP ftp-bidir TCP ftp-pasv TCP ftp-port	accept	Log	*	*	DMZ Proxy Server access definition for specific services
13	* Any	GIAC-D-Web	*	TCP http dns	accept	Log	*	*	Any access to DMZ Web on www. DNS access is for the isolated testing only
14	* Any	GIAC-D-Portal	*	TCP https	accept	Log	*	*	Any access to DMZ Portal on https
15	GIAC-D-SMTP	* Any	*	TCP smtp dns	accept	Log	*	*	DMZ Email Gateway access definition for smtp and dns only
16	* Any	GIAC-D-SMTP	*	TCP smtp	accept	Log	*	*	Any access to DMZ Email Gateway on smtp
17	GIAC-V-VPN	GIAC-ProtectedNet	*	AH ESP	accept	Log	*	*	VZ VPN server access definition for vpn services
18	GIAC-ProtectedNet	GIAC-V-VPN	*	AH ESP	accept	- None	*	*	VZ VPN server access definition for vpn services

The rules pictured below are those that are necessary to lock down internal devices access as well as cleaning up anything else not explicitly defined.

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	Clear Out Noise (Rule 1)								
	Protect Firewall Rule (Rules 2-3)								
	Internal To External/DMZ/Vestibule Rule (Rules 4-9)								
	DMZ To Internal (Rules 10-11)								
	DMZ & Vestibule to External (Rules 12-18)								
	Clean Up Rules (Rules 19-21)								
19	GIAC-I-DB GIAC-I-FP GIAC-I-CSW1 GIAC-I-DNS GIAC-I-L GIAC-I-MF GIAC-I-R1 GIAC-I-SMTP GIAC-I-T	* Any	*	* Any	drop	Log	*	*	Locked down internal servers and routers to not allow access outside of the network
20	GIAC-ProtectedNet	* Any	*	TCP ftp TCP ftp-bidir TCP ftp-pasv TCP ftp-port TCP http TCP https TCP ssh TCP ssh_version_2 TCP ssl_v3 dns icmp-requests	accept	Log	*	*	Locked down internal networks to allow access via specific services
21	* Any	* Any	*	* Any	drop	Log	*	*	cleanup rule--drop everything that is not explicitly defined and log

Security Architecture Depth Revisited

It has been proven to me that no matter what port, protocol, ip address, anti-virus, signature filtering, alerting, or rate-limiting strategies are used, an overly motivated trained individual with sufficient resources and sufficient time can get in. The hackers today have a tool that can bypass our best efforts given sufficient motivation or they simply social engineer access to achieve their goals.

Given that overwhelming challenge, it does not mean that security professionals should simply wash their hands, open the door, and invite hackers in. When using a layered defense, we can minimize the risks to the data and services this architecture is designed to protect. We can keep our networks, and the data within them, safe by being vigilant at all levels of our defense in-depth strategy.

Keep on patching
Keep on updating signatures
Keep on reviewing alerts and logs
Keep on training staff to be aware of the security challenges
Keep on improving our defenses as the technology advances

Elements of the Defense in-Depth strategy that have been detailed in this document will go a long way in providing protection at the various layers for which they are responsible. The Border Router, Primary Firewall, IDS sensors, and VPN Servers together form a strong-tiered perimeter defense.

End Notes and List of References

End Notes

[1] Keizer, page 2.

[2] Pescatore, page 2.

[3] SANS, page 6.

[4] Criscuolo.

[5] United States General Accounting Office, page 19

[6] Check Point Systems, help page.

List of References

Brenton, Chris, Baccam, Tanya, Northcutt, Stephen. Track 2 Firewall Perimeter Protection and VPNs; 2.2 Packet Filters. SANS Institute. 2003.

Brenton, Chris, Spitzer, Lance, Baccam, Tanya, Winters, Scott, Northcutt, Stephen. Track 2 Firewall Perimeter Protection and VPNs; 2.3 Firewalls. SANS Institute. 2003.

Brenton, Chris, Baccam, Tanya, Northcutt, Stephen. Track 2 Firewall Perimeter Protection and VPNs; 2.4 Defense In-Depth. SANS Institute. 2003.

Brenton, Chris, Elfering, David, Baccam, Tanya, Northcutt, Stephen. Track 2 Firewall Perimeter Protection and VPNs; 2.5 VPNs. SANS Institute. 2003.

Brenton, Chris, Stearns, William, Baccam, Tanya, Northcutt, Stephen. Track 2 Firewall Perimeter Protection and VPNs; 2.6 Network Design and Assessment. SANS Institute. 2003.

Chappel, Laura A. White Hat Tool Box: Tools, Tricks, and Traces. Saratoga: Podbooks, Inc. 2003.

Check Point Systems. "Security Rule Base." Help page. (2003). August19, 2003.

Cisco Systems. "Cisco Threat Response: An Intrusion Protection Security Solution." http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/thret_wp.pdf (July 16, 2004)

Criscuolo, Paul. Paller, Alan. "Los Alamos National Laboratory on Intrusion Prevention Systems: A Real World Case Study." SANS Webcast. Wednesday, July 28 at 1:00 PM EDT (1700 UTC). http://www.sans.org/webcasts/show.php?webcastid=90514**,** , (July 28, 2004)

Forescout Technologies. "The First 15 Minutes." 2003.

Keizer, Gregg. "Gartner: Worms jack Up the Total Cost of Windows." May 02, 2004. URL: http://www.securitypipeline.com/news/showArticle.jhtml?articleId=19502393&printableArticle=true (July 24, 2004).

McAfee Security. " Host and Network Intrusion Prevention Competitors or Partners?" June, 2004. URL: http://www.networkassociates.com/us/_tier2/products/_media/mcafee/wp_host_nip.pdf (July 21, 2004)

McAfee Security. "McAfee IntruShield Netowrk IPS Sensor Data Sheet." URL: http://www.networkassociates.com/us/_tier2/products/_media/mcafee/ds_intrushielddidssensor.pdf (July 21, 2004).

McClure, Stuart, Scambray, Joel, and Kurtz, George. Hacking Exposed, 3rd Edition. Berkeley: Osborne/McGraw-Hill. 2001.

Mirage Networks. "Combating Rapidly Propagation Threats From the Internal Network." URL: http://www.miragenetworks.com/wp_Combating_RPTs.pdf (August 4, 2004).

Novak, Judy (primary author). Track 2 Firewall Perimeter Protection and VPNs; 2.1 TCP/IP for firewalls. SANS Institute. 2003.

Pescatore, John. "Enterprise Security Moves Toward Intrusion Prevention." Analyst Reports. September 25, 2003. URL: http://www.csoonline.com/analyst/report1771.html (August 6, 2004).

Pescatore, J and Stiennon, R. "CIO Update: Enterprise Security Moves Toward Intrusion Prevention." Gartner Article IGG-06042003-03. June 4, 2003.

Pescatore, J and Stiennon, R. "Defining Intrusion Prevention." Gartner Research Note TU-20-0149. may 29, 2003.

"SANS Glossary of Terms Used in Security and Intrusion Detection." The SANS Institute. May 2003. URL: **http://www.sans.org/resources/glossary.php#D** (August 6, 2004).

SC Magazine for IT security professionals. "TippingPoint UnityOne-1200 (Special

report Intrusion prevention." Product Details. March 25, 2004. URL: http://www.scmagazine.com/products/index.cfm?fuseaction=productDetails&productID=6344&type=review (July 28, 2004).

Stiennon, Richard D. "Magic Quadrant for Intrusion Detection Systems, 2H03." Gartner Research Note M-22-0693. April 13, 2004.

Stiennon, Richard D and Nicolett, Mark. "Next-Generation Firewalls Will Include Intrusion Prevention." Gartner Article Top View AV-23-2253. June 25, 2004.

Sturdevant, Cameron. "UnityOne Foils Attacks." March 29, 2004. URL: http://www.eweek.com/article2/0,1759,1557583,00.asp (July 28, 2004)

Tipping Point Technologies. "UnityOne: Intrusion Prevention Systems: The Platform for Unrivaled Security and Performance." URL: http://www.tippingpoint.com/pdf/resources/datasheets/U1001.pdf (July 23, 2004).

United States General Accounting Office. "Report to Congressional Requesters; Critical Infrastructure Protection; Challenges and Efforts to Secure Control Systems." GAO-04-354. URL: http://www.gao.gov/new.items/d04354.pdf (March 2004)