



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

David J. Naelon
GCFW Practical v3.0
Submitted on May 2, 2004

Protecting the Family Business: The DMZ Guide for GIAC Enterprises

Overview.....	4
Brief GIAC History.....	4
Assignment 1 – Security Architecture.....	7
The Task at Hand: the New Business Operations	7
Customers	7
Suppliers	8
Partners.....	9
GIAC On-Site Personnel	9
GIAC Mobile Personnel.....	10
General Public.....	10
Considerations	11
Architecture and Component Review.....	11
Internet Router	13
Firewall Components Standards	15
Web Archicture.....	15
Load Balancers	17
SMTP Relays	19
Web Proxy.....	21
Client to Site VPN.....	23
Network IDS	24
Administrative Components.....	27
Admin Support Staff Net	28
Perimeter Services Net.....	28
Assignment 2 – Security Policy and Component Configuration.....	30
Border Router	30
Overview	30
Global Configuration Commands	30
Interface Level Configuration Commands	35
Basic Filtering.....	36
Border Router Summary.....	38
Primary Firewalls	38
Primary Firewall Hardening	39
Nokia IP 530 Appliance.....	39
Global Firewall Settings	43
Summary	46
Security Policy for Primary Firewalls	46
Web Networks Security Policy	47
Service Networks Security Policy.....	48
Web Proxy Security Policy	49
SMTP Relay Security Policy.....	49
VPN Configuration and Security Policy	50
Summary	54
Assignment 3 – Design Under Fire.....	55
Assignment 4 – Work Procedure	63
Nokia IP 530	63

Checkpoint Firewall-1 Management.....	65
Web Firewall Rule Creation	68
Appendix A - Bibliography	71

© SANS Institute 2004, Author retains full rights.

Overview

In accordance with the design request from GIAC Enterprises, the following design proposal shall be submitted for review.

GIAC Enterprises is a new player in e-business processes dealing in the online sale of fortune cookie sayings. They are venturing into the expansion of their brick and mortar business to include a robust internet presence. The GIAC business model must account for the following core components:

- Customers must be able to place new orders and verify the status of existing orders through the GIAC corporate web presence.
- Suppliers must be able to submit materials for use and check on payment status through the GIAC corporate web presence.
- Partner companies are granted both Customer and Supplier status and must be able to operate as such.
- Internal Employees must have a vehicle for support of the web presence and online functions, while maintaining a consistent state of protection from outside threat.
- Mobile Sales Force and Telecommuters must have reasonable access to corporate applications and sales functions.
- General Public must have the ability to learn about GIAC Enterprises through the web presence.

Brief GIAC History

Beginning in late 1812, Giuseppe Giac was moved to tears after hearing the Overture of 1812. In fact, he was so moved and so emotional, he began writing brief sayings and words of encouragement. As time went on, he began placing the sayings in his favorite deserts when serving them at the family restaurant. However, Giuseppe became quickly disheartened that the paper would not hold the ink he used when the slips were sunk into the cream filling of a cannoli or placed between the layers of a tiramisu. Furthermore, Giuseppe's father Rocco became enraged when customers began choking on the linen and papyrus he tried to use as he began to hone his craft.

Not wanting to deter his son's spirit, Rocco Giac began to make hollow cookies that his son could place his tiny words of wisdom into. The new cookies became an instant success in the city. Soon afterward, customers from all over creation began making requests of the father and son combination for dozens upon dozens of the cookies. GIAC Enterprises was born.

As the years past, Giuseppe could not keep up with the demand for new and creative fortunes. Also, as the family business flourished, Giuseppe was unable to attend college as he was desperately needed at home. This limited the number of languages

into which the sayings could be translated. Scrambling to keep up with demand, the business expanded operations and began hiring linguists and writers to maintain the creativity and variations of the sayings.

Eventually, the cookie craze caught on throughout the country and the largest corporations in the world began packaging and reselling the product. Upon his death in 1898, GIAC's products were being repackaged and sold all over the world. The company tried to keep up with various technologies in order to maintain their market. During the early days, GIAC really prided itself as a corporation that tried to stay on the cutting edge of technology in order to meet their customer's needs.

During the Depression, hard times hit GIAC the same as it hit the rest of the country. As generations passed and the business stayed in the family, the cynicism of the times made its way into the corporate culture. Non-family employees and business partners were cut loose one by one and eventually the company began to falter. Sensing this weakness, other companies began producing the same types of products and hired many of the people that GIAC let go. The competition became tighter and tighter through the late 30's and early 40's. But somehow, GIAC survived.

In late 1944, GIAC elected a new company president and great-grandson of Giuseppe. Domenic Giac took the reigns of the family business and set out to re-establish GIAC Enterprises as the industry leader. Domenic had the idea of combining the sayings on the front of the slips of paper with various number series on the back of the paper. The sayings, when correlated with the numbers would produce coded messages for troops overseas. The government, ecstatic with a way of both feeding the troops a special treat and sending secret messages began exclusively purchasing all their snacks from GIAC Enterprises. To this day, that single move is credited with saving GIAC from bankruptcy.

Through the next 60 years, using updated printing presses and re-establishing their relationships with creative minds throughout the world, GIAC flourished as the largest producer of sayings in the world. They have maintained this market presence until the middle of 2003. Production stagnation, a sharp rise in travel costs and a rise in real-estate costs started to sink into the bottom line of the company. Like all major corporations, layoffs and cutbacks hit hard. Domenic's grandson Mario, placed in charge in October of 2003, knew that a new corporate direction was needed.

Mario attended a SANS conference in New Orleans later that year. He knew the company's paranoia of the Internet, fueled mostly by their intricate dealings with the government as well as way too many X-Files episodes, needed to be set aside. Hearing that many of the great minds in the community attended these conferences, he felt it would be a good place to begin learning about what his company needed to do in order to continue to grow and regain their position atop the world market.

Many of the business processes internally would remain the same as they had for generations. However, Mario needed to find ways of bringing in revenue, maintain

better control of raw materials and cut down the cost of working with partner companies and suppliers.

Mario looked hard at what the key components of his new business model were and identified the six key components mentioned earlier: customers, suppliers, partners, internal employees, teleworkers and the general public. After consulting with the board of directors and various internal technical experts, GIAC made a request for design architecture in support of their new e-business.

Assignment 1 – Security Architecture

The Task at Hand: the New Business Operations

Working from the six key components as specified by GIAC Enterprises, the six key components will have specific access requirements. Based on those access requirements, the business operations of GIAC Enterprises can be implemented.

Customers

Customers are the core of the GIAC business as they generate well over fifty-percent of the revenue. In years past sales personnel had to manually enter orders into the order entry system on behalf of the customers. This led to a number of problems with data entry, order timing and service. Customers were at the mercy of the sales personnel. Also, since the customer base was spread throughout the world, telecommunications costs were skyrocketing out of control as inbound toll-free access charges mounted. The widely dispersed customer based also created a need for near 24X7 staffing of the on-site call center.

Perhaps, however, the biggest of the problems was the defect rate. Every order placed by a customer had to be recorded by sales personnel then entered into the order entry system. This non-value added step put the chance for error at multiple places in the order process. Since the entire order entry process was at the hand of GIAC employees, defects and mistakes (along with the associated costs) were also eaten up by GIAC.

Mistakes also effected the customers who were expecting orders. Since there was no on-line presence, customers had no way of obtaining order status unless they made calls to the call center. Customers were feeling helpless in the order process.

Customers can purchase fortunes in two forms: electronic and paper. The paper orders are printed on-site at GIAC headquarters and subsequently shipped. Electronic orders are filled via electronic files. In today's environment, the electronic files are burned to CD and shipped.

GIAC wants to continue to use their existing order entry system as it interfaces well on the back side with their printing, file generation and shipping systems. However, they would like for customers to securely enter their own orders via an on-line web order entry system. This entry system must also allow customers to view existing orders, track order status and view billing. As orders are entered by customers on the web interface, information must regularly reflect in both the printing and file generation systems.

Since the files generate rather quickly, and they are typically not very large in size, it is acceptable (and preferable) that this function be available for near immediate fulfillment. The files must be available for download from the same front end system that order entry is accomplished through.

Paper orders are more time consuming. The backend database and mainframe systems automatically run the printing system with some supervision from GIAC staff. As specific automatic milestones are hit (i.e. begin order printing, twenty-five, fifty, seventy-five and one hundred percent completion and shipped) the order system is updated.

When orders complete, they are boxed and labeled for shipping. Shipping vendors pickup orders from the GIAC warehouse and interface with the internal shipping system which houses tracking information. The tracking information is added to the order information in the system. This tracking information must also be available to customers.

Since customers will be accessing the on-line system via the world wide web, a web server farm is required for access. All customer access is accomplished via HTTPS (TCP 443) to a load balanced web farm. RSA/SecurID tokens will be issued to customers for access to the system. Applications will be provided to customers based on the user id specified.

Suppliers

Suppliers come in a number of flavors. Intellectual suppliers submit sayings for use. Translators take recently submitted sayings and port them to a number of different languages. Office supply companies fulfill stationary type products (pads, pens, etc) as well as paper and ink products for the presses.

The cost of the intellectual capital is skyrocketing. Since GIAC has no on-line presence in their current environment, they must incur the cost of bringing in writers and translators on a regular basis. These expenses include all travel expenses as well as the actual cost of the sayings themselves.

GIAC also ends up at the mercy of the writer and translator schedules. In addition, last minute needs and emergencies are difficult to meet. A need for some form of remote entry for these suppliers is a must.

Suppliers of hard goods and office products also would like an electronic way of pulling orders. Since GIAC currently does not have a web presence, they are unable to submit orders to other companies without making lengthy long distance phone calls. As most of GIAC's suppliers all have expansive on-line ordering capabilities this becomes a nuisance.

Upon completion of the new environment, GIAC wants an online entry system for their saying suppliers. Entry can be done one of two ways: either line by line into the entry system or via a flat text file. Once entries are submitted, GIAC staff must be able to review and proofread them. This process utilizes the same backend system as the order entry system and has the same reporting features. Due to the intellectual property concerns, saying suppliers need to be able to securely view entry status and payment status.

Translators will require similar functions to suppliers in terms of billing, however, they must have the ability to view the saying database. Translators are paid by translation and they must also have the ability to view payment status.

GIAC's hard product suppliers need the ability to view inventory and order requests. The printing system inventory supply is kept up-to-date by GIAC personnel. In addition, approved requests for office supplies are kept in an internal database that was used by support personnel to phone in orders. GIAC would like their office product supplier to access this database to keep products in stock.

The supplier access is very similar to the customer access and will be done via HTTPS to a load balanced web farm. As with customers, RSA/SecurID tokens will be given to appropriate contacts for system authorization. Only authorized applications will be available to suppliers.

Partners

In a few instances, companies provide and perform both Customer and Supplier functions. These partner companies are located around the globe. Partners can supply sayings, translate sayings, resell electronic forms of sayings or resell printed fortunes. For a company to be considered a partner, they must perform at least one customer function and one supplier function. The system must account for this type of access.

Since partners function like both customers and suppliers, they will need access to a larger number of applications. However, they will access the applications via the same HTTPS site. The RSA/SecurID system will authorize the appropriate applications for view by the partner.

GIAC On-Site Personnel

On-site personnel have networked PCs and an internal e-mail system. However, they have not had any external access to date. As the corporation attempts to conduct business in an electronic world, the Board has decided to open up the corporate network.

As part of the new environment, GIAC would like to provide external email services and web browsing access to their employees. Of course, this access must be secured and locked down as much as possible. GIAC management wants logging of all accessed websites in accordance with generally accepted usage practices. They also want e-mail scanned for viruses and SPAM before it hits the internal mail server.

Outbound web traffic (TCP 80, 8080 and 443) will be required for employee web browsing. This is accomplished using an outbound load balanced proxy server farm. Internal employees already utilize a mail system for internal e-Mail. The extension of the internal email system to the Internet will require both inbound and outbound SMTP (TCP 25) traffic. An SMTP relay channel will proxy mail in a bi-directional manner for the internal email system. The internal mail servers will never have direct external access. Externally placed DNS servers are located in the outbound proxy channel. For the DNS servers to function, inbound and outbound TCP 53 is required.

GIAC Mobile Personnel

Traditionally, traveling sales personnel would spend the day calling on customers gather orders and other information. Orders taken throughout the day were then called into the GIAC call center at night. As previously stated, many of GIAC's customers are global entities. Long distance charges were skyrocketing as business boomed. However, the downtime between when orders were taken and subsequently fulfilled was becoming unacceptable. In addition, the error rates were problematic as well. Orders were written down by the sales personnel, subsequently written down via phone conversation at the call center and finally entered into the system.

Many of GIAC's long standing employees also have been departing due to the inflexibility of the workplace. As urban sprawl took its toll, the commute to and from work for those employees living outside the city limits made for intolerable days. A large population of employees lobbied for some type of work at home procedure. However, since GIAC did not have any semblance of an online presence, this was not possible.

Domenic, like the successful Giac's before him, valued the employee and valued the personnel that worked so long for his company. He also saw the need for the mobile sales people to cut down on phone expenses and the order entry error rate.

To that end, GIAC must have some form of VPN connectivity. The connectivity should be limited to approved personnel only and also limited to approved applications. Since internally, GIAC locked down desktops and controlled them tightly, it is also required that some level of control be given to computers given VPN access.

General Public

All though the general public typically wouldn't be interested in the day to day business functions of GIAC, they may be interested in learning about the company's storied

history and philanthropy. Investors also may want to obtain certain information about the company for making financial decisions. To solve this issue, a web presence will be required.

Considerations

Careful review of the GIAC requirements shows a desire for increased levels of customer service, accuracy and availability. While attention must be paid to the internal requirements of e-mail and web browsing access, the overriding focus is on customer access.

Since GIAC is a worldwide power in this market with a strong customer base and a strong flow of capital, expenditures on equipment will have great flexibility. However, cost cutting measures and a desire for efficiency are concerns. Internally, GIAC has invested time, money and effort to various systems in efforts to streamline business operations. This is apparent in the discussions around the internal sales entry and tracking applications currently in use.

Staffing considerations must be taken into account. In any business, the largest expense is usually human capital and payroll. Security personnel typically command higher salaries than most networking related engineers. As such, GIAC desires to minimize the number of support personnel needed to maintain operations.

GIAC also understands that success in this endeavor could potentially lead to expansion of operations. As such, their design must be modular and easily repeatable. Should GIAC decide to build additional datacenters for redundancy or increased capacity, there should be standards defined for hardware and software purchases within their DMZ.

IP Addressing Scheme

The networking scheme used by GIAC is in the following chart. 100.100.10.X space is used for the public segments. This space is not currently allocated.

Network	Mask	Function
100.100.10.0	/27	Non-secure web farm / Internet facing
100.100.10.32	/27	Secure web farm / Internet facing
100.100.10.64	/27	Citrix VPN Farm
100.100.10.96	/27	SMTP Relay Farm / Internet facing
100.100.10.128	/27	Web Proxy Farm / Internet facing
172.18.10.0	/27	Non-secure web farm / Core facing
172.18.10.32	/27	Secure web farm / App network facing
172.18.10.64	/27	Secure application server farm
172.18.10.96	/27	SMTP Core connectivity farm
172.18.10.128	/27	Web proxy Core access farm

172.18.10.11.0	/25	DMZ support services network
172.18.10.11.128	/25	DMZ support staff secured subnet
192.168.10.0	/24	Assigned in /30 blocks for router links

Architecture and Component Review

To support the design requirements, the GIAC architecture is approached from a modular perspective. Each module within the design can be reproduced as needed. This modular design allows for the greatest flexibility. The full DMZ design contains four modules:

1. Internet Common (Internet Router)
2. Web Module
 - a. Secure Web
 - b. Generic Web
3. Service Module
 - a. VPN Channel
 - b. Mail Relay
 - c. Web Proxy
4. Administrative Network

For all DMZ implementations, the Internet Common module will be required. Once the DMZ common implementation is complete, other modules are added to complete the build. A fully built GIAC DMZ is represented in Figure 1.

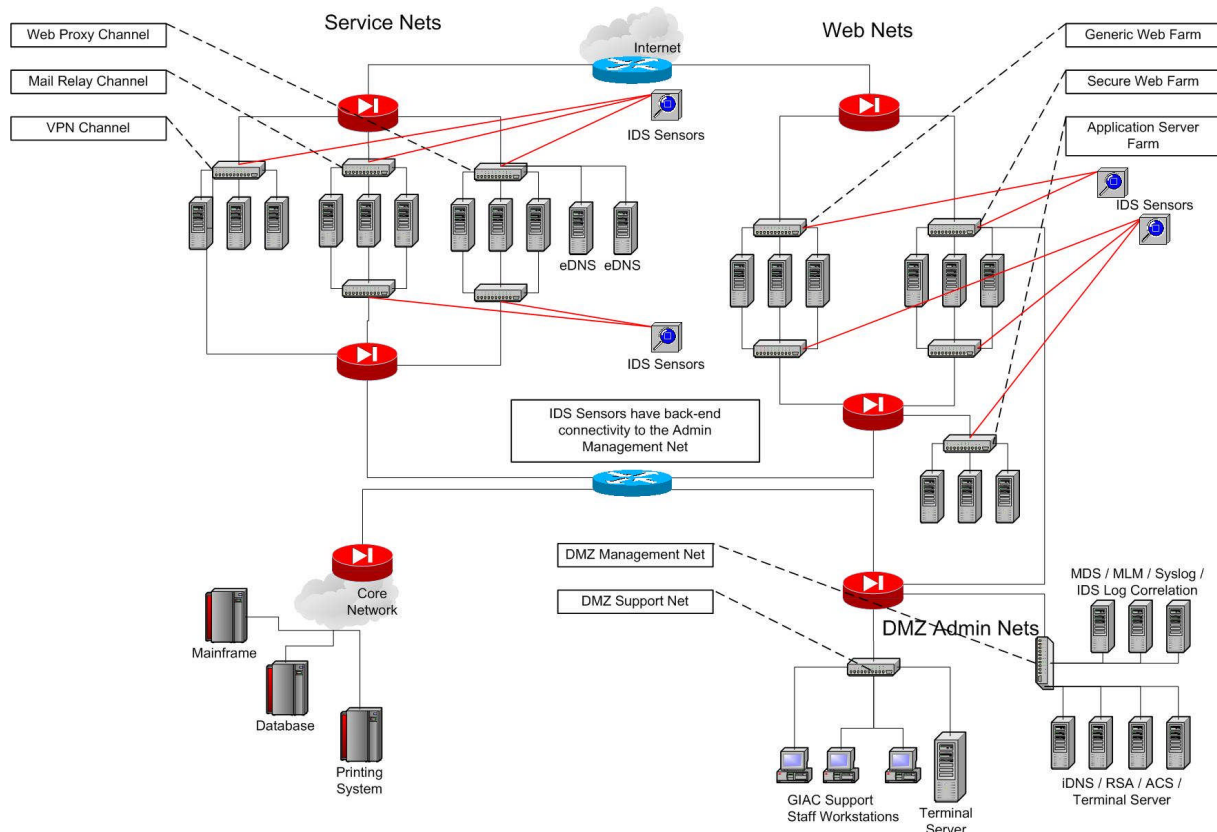


Figure 1 : Fully Built GIAC DMZ

Internet Router

To solve the issue of customer access, an access point must be established. In the GIAC DMZ, that access point is the DMZ router. BGP peering will not be done on the router as the ISP will host all DMZ services. This will help harden the router and reduce the amount of information available during attack reconnaissance.

For the Internet Router, a Cisco 7600 series device will be used. A single, channelized fractional DS-3 will provide internet access to the DMZ environment. Since the DS-3 is channelized, additional bandwidth can be added as needed as usage dictates. The 7600 provides enough flexibility to deploy the DMZ in the modular aspect proposed, as well as enough throughput to handle the bandwidth. The 7600 series is offered in a variety of different chassis sizes, all of which share the same subset of FlexWAN cards and expansion modules. This flexibility will allow for the greatest growth potential should operations require greater throughput in the future. For this deployment, a 7603 will suffice.

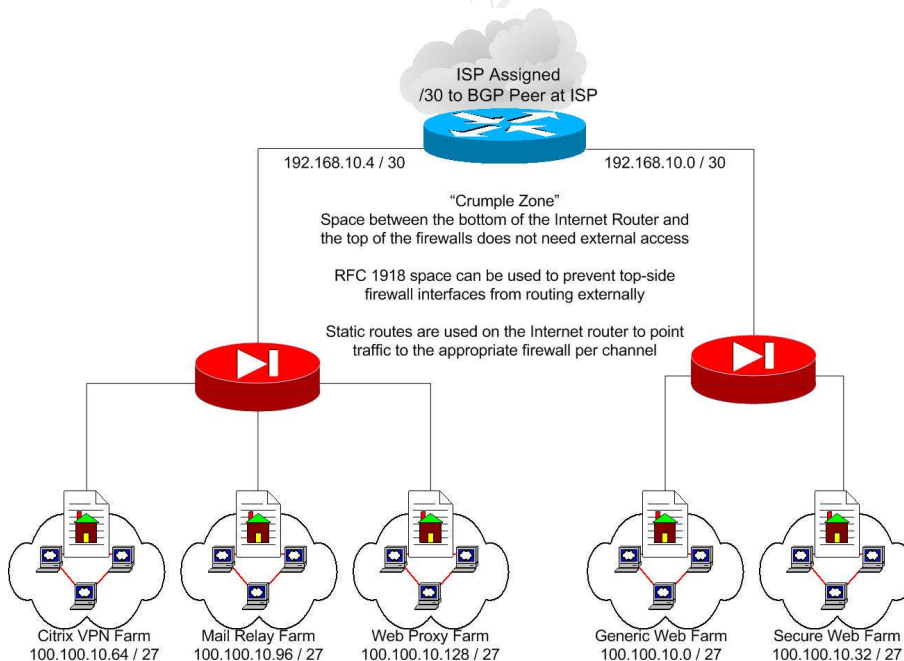
Clear text administration of devices in the DMZ is not allowed, therefore SSH will be needed to remotely administer the router. Based on that requirement, IOS version

12.1(3)T or later that supports encryption is necessary. For this deployment, IOS version 12.2.17d-SXB will be used. This version supports 3DES and SSH on the 7600 series router.

In the GIAC design, the Internet Router acts as a border or edge router. Its primary focus is passing traffic and not to act as a security device. It is important however, to take precautions to harden the router due to its vulnerable location within the network. Steps to harden the router will be discussed later in this document within the “Security Policy and Component Configuration” section.

While the web and service network firewalls are not considered part of the internet common, they need to be mentioned as they are partnered. Again, the firewalls and internet router do not exchange routing information. They do however, protect the registered space owned by GIAC Enterprises. A crumple zone is deployed between the Internet Router and the topside firewall interfaces. Using RFC 1918 address space, a small border is erected before the firewalls. This will provide added protection for the firewall interfaces. There is not a need for the topside firewall interfaces to route externally. They simply provide a routing mechanism for inbound and return traffic to hit the appropriate channels. Using a 30-bit mask also limits the address space available on the subnets to only the directly connected interfaces. The firewalls themselves have some routing capability once they receive packets. They can make a decision as to which farm to send the traffic.

Many of the advanced filtering, firewalling and IDS features of the new Cisco IOS versions will not be a factor in this deployment. As previously stated, the function of the Internet router is as an edge access device, and not a full blown security device. This points the focus for the choice of IOS from feature list to stability.



Firewall Components Standards

To secure connectivity to the outside world from the Corporate Network, firewalls are used. A stateful inspection firewall provides high performance firewalling capabilities and rule bases that are easy to manage and configure. Allowable traffic needs only to be specified in one direction. Return traffic is allowed via state table that manages IP session information.

Firewall components have two major factors: physical hardware and firewall software. For the physical hardware component, all firewalls purchased will be Nokia IP 530 series appliances. All appliances will run Checkpoint Firewall-1 NG r55.

Standardization is key for a new deployment. Ease of management is also key. As GIAC is new to the DMZ world, there will be a learning curve for system support. Nokia appliances running Checkpoint software are very common. Training is readily available as are reference materials. From a support perspective, using the Nokia appliances also makes support of the network intrusion detection systems easier. Nokia supports ISS Real Secure on their appliances. Network intrusion detection will be discussed more in depth later in this document.

Perhaps more important than hardware standardization, the Nokia has a built in OS that is hardened and optimized for both the hardware and for Firewall 1. This operating system is called "IPSO" and is a FreeBSD Unix variant supported by Nokia. GIAC will deploy IPSO version 3.7.0 build 32 as the standard for all firewall implementations. While the 530 series appliance has had its share of problems early in 2003, many of the hardware issues have been resolved. Specifically, the harddisks have been upgraded from the micro-drives used initially to full size and the problematic power supplies have been upgraded.

Firewall 1 in the NG r55 version (as in versions since NG) supports the implementation of a Multi Domain Server (MDS) for the purpose of management. This allows for centralized management of all firewalls, rule bases and logs. The MDS allows for the creation of containers within the management system which allows for the logical grouping of firewall modules and log locations. Also, virtual management stations and log servers can be defined local to the MDS (or to a separate physical Multi Log Manager – MLM). This allows for decreased hardware costs and support. Although r56 has been released to production by Checkpoint, r55 is known to be stable and has been in production for some time.

Web Architecture

To provide customers, suppliers and partners access to services a web presence is needed. In the GIAC architecture, this presence is multi-tiered to provide for the

greatest security. Customer traffic is separated from general traffic to provide the greatest performance.

The firewall components represent the central security focus of the implementation. Referring back to Figure 1, a layered approach to design is deployed. Working from the top down, the front line of defense begins with the two top-side firewalls. The top side firewalls protect the registered space in the GIAC network. Only access absolutely required should pass the firewall. Since hosts in this portion of the DMZ are more susceptible to attack, careful implementation of the firewall rule base is imperative.

A second tier of firewalls is present to protect application server access. Bastion hosts in the upper tier of the DMZ are dual homed, but they do not route. Web access is allowed from the top through the firewall.

Figure 2 shows the general architecture of a web channel for GIAC. Through the top side firewall either 80 or 443 traffic is allowed to flow down to hit the web server. This uses registered space and is freely routable. The use of a load balancer in this part of the module will be discussed later.

Inbound requests are processed by the web servers and any application calls that are required are passed to a secondary process on the server. The secondary process can make an application call down through the application firewall. These multi-tiered approach completely separates the presentation layer from the application layer. Also, since the application layer servers are not routable, they are more difficult targets.

The weakness of this design lies in the complexity of the server management. Ip forwarding must be turned off on the bastion web servers or else a web server compromise could potentially lead to an application server compromise. A second weakness is one common to all stateful inspection firewalls: load. Stateful inspection is known to be fast, however, if enough traffic bombards an interface, they are known to pass packets that do meet inspection criteria. This is mitigated by limiting the pipe size coming into the internet router. A DS-3 will cap out at 45MB, hardly enough to overload the Nokia interface.

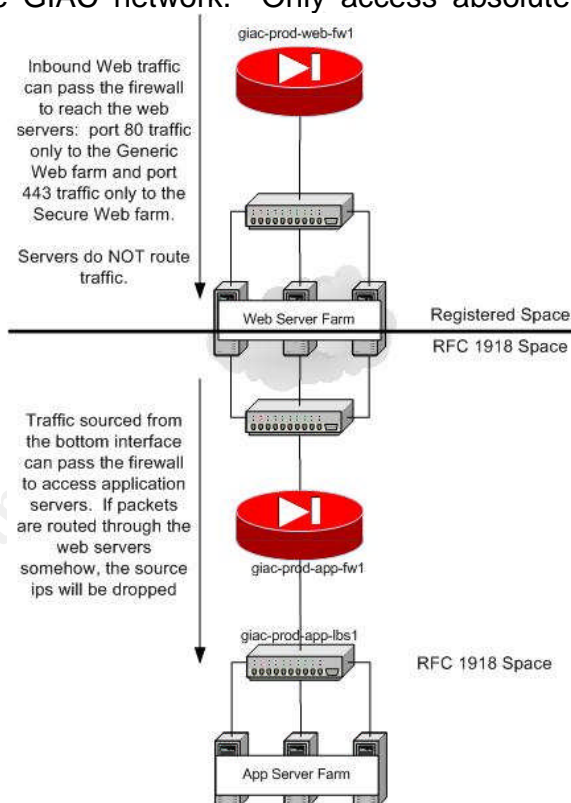


Figure 2 : Web/App Data Flow

This tiered architecture extends down further when access to the mainframe, database and printing systems are needed. The bastion application servers pass data to the web servers. The data has to come from somewhere. This design calls for the data stores to be located on the GIAC Core network. GIAC employees access these systems every day. Most of the traffic that passes to these systems is sourced from internal employees. While internal threats are real and need to be addressed, that is outside the scope of this document.

Figure 3 focuses on the main scope, customer access to their data. The GIAC

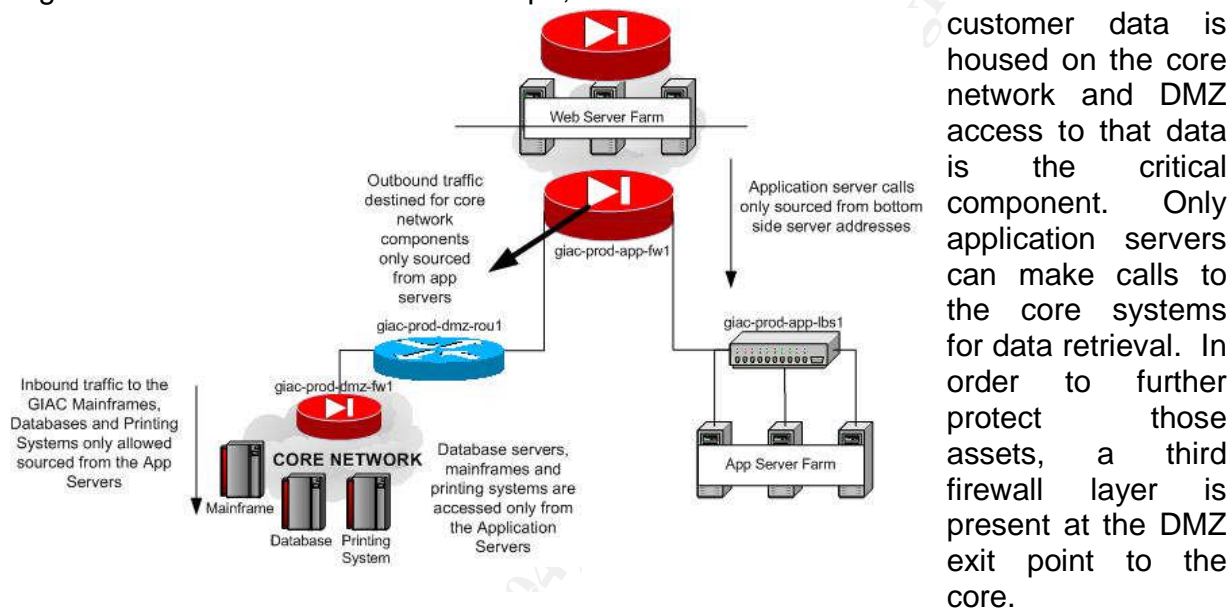


Figure 3 : Web/App/Core Data Flow

Malicious traffic has a very difficult time getting to the main data stores. Any inbound threats will need to pass the topside web firewall, through the web server farm, through the application firewall and finally through the DMZ exit firewall. While this is certainly a possibility, the chances are unlikely. This third layer now provides separation at all major access points for an application: web presentation, application logic and data store.

Load Balancers

Server availability is a critical component to the GIAC Enterprises design. Server maintenance and upgrade is an inevitable component of a web presence. The trick is to create a situation where servers can be removed from service for maintenance, without completely taking down the application.

Load balancers provide this functionality. A load balancer is a switch that provides OSI Layer 4-7 capabilities. Virtual IP addresses (VIP) are configured on the switch. Web servers connected to the layer 2 segment are configured to respond to the VIP. The

switch maintains a traffic table and session table for the servers and selects which server to pass the request to.

Inbound firewall rules only allow traffic destined for the VIP, and not to the real server addresses. As IP traffic flows, the return traffic is sourced from the VIP and not from the real servers. The user will have no idea which server they are connected to when they make the request. The example below demonstrates the process for <https://customer.giac.com>.

For the GIAC DMZ implementation, Foundry Networks Server Iron 100 devices are deployed. The Server Iron 100 (SI100) are modular switches allowing for growth. Each

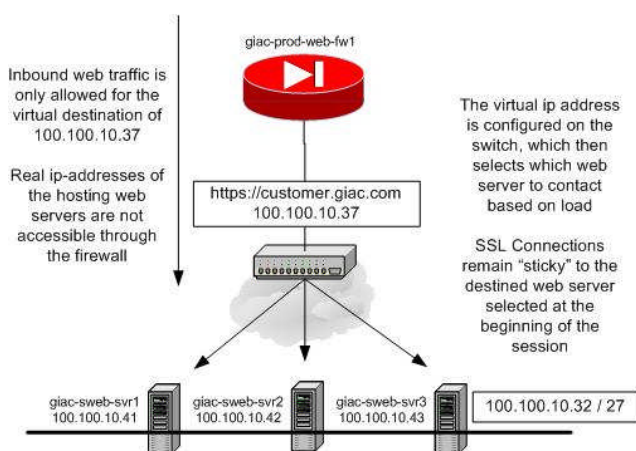


Figure 4 : Load Balancing Overview

chassis can hold up to four blades containing fast Ethernet or Gigabit Ethernet (copper or fiber) ports. Blades are hot swappable and can be added without taking down the box. This allows for the greatest uptime during upgrades and maintenance.

GIAC implemented SI100 code 8.1.00dT22. This code allows for advanced load balancing functions, private VLANs and SynDefender (SynDef). The SI100 has the capability with other versions of code to also perform firewall load balancing. However, that function will not be

necessary in this implementation. It is available for future upgrades.

Another interesting feature is the ability to have the Foundry listen on one port, then pass the traffic to the server on another port. This is particularly useful in a bastion host environment. Inbound traffic to the VIP will come in on port 443. However, when the Foundry makes a load balance decision, it can pass the traffic to the server on any port specified, provided the server is listening. Attackers may know the port the application runs on (i.e. 443) however the servers themselves can be listening on a redirected port, leaving 443 off. This adds a layer of confusion to attacks.

The weakness in this scenario is specific to the load balancer functionality. The switch determines which servers are up and functioning through a process called a health check. The health check is a packet sourced from the management ip address of the switch destined for the real server ip address. It is never a full session, however. The load balancer sends a "syn" to the server. The server responds with a "syn-ack." This process occurs about every 2-3 seconds. Network based IDS systems will see this as a possible syn-flood attack. Also, if host based IDS is deployed on the server, it could trigger a DOS alert and block the packets. If the packets are blocked at the server, the load balancer never receives the syn-ack during the health check. Once a health check

fails, the server is removed from rotation. IDS sensors and host based intrusion must be configured properly to account for this functionality.

SMTP Relays

GIAC Enterprises requires inbound and outbound email in order to communicate more effectively with their customers. Internally, email had been used for some time, however it was never extended to the outside world.

The mail channel is comprised of a multi-process dual homed mail relay running Solaris 9. GIAC has chosen to use the commercial version of Sendmail called Sendmail Mailstream Manager version 3.05. As support is an important consideration for GIAC Enterprises, the management team felt more comfortable with a supported version of the product. Mailstream Manager contains plug-in support for anti-spam, anti-virus and corporate policy enforcement. Very much like the

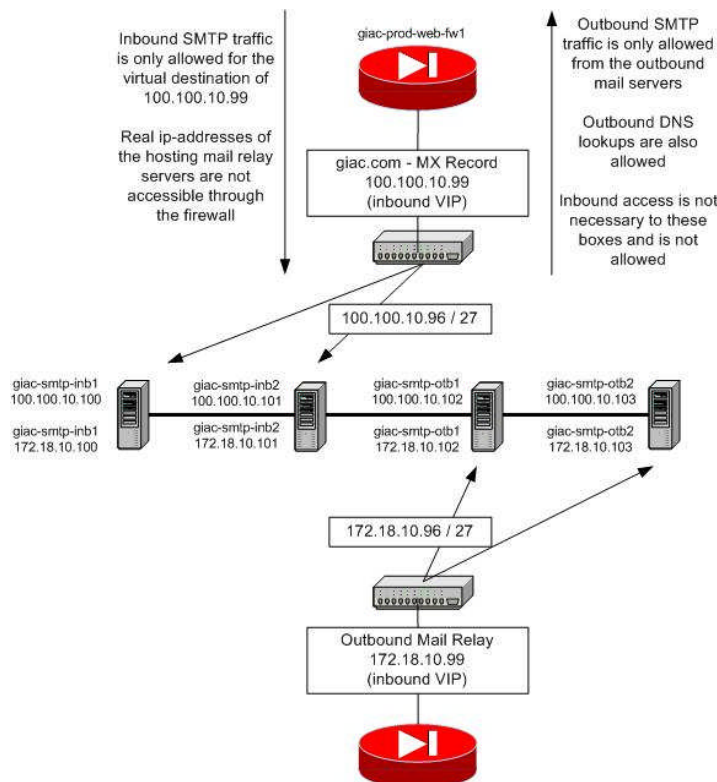


Figure 5 : SMTP Data Flow

centralized management capabilities of Checkpoint Firewall 1 NG, Mailstream Manager has a console for single point management of multiple servers.

SMTP traffic is divided up into Inbound and Outbound relay farms. The inbound farm services mail entering the GIAC DMZ. The GIAC MX record is load balanced among the inbound mail relays. Traffic passes to the top interface of the relay. Mail messages are checked against the corporate mail policy, scanned for viruses and processed for spam. The inbound process then hands off the traffic to the bottom interface for passage into the DMZ and down into the GIAC core mail servers. The outbound farm works in much the same way. GIAC mail servers contact a load balanced VIP on the bottom side of the channel for passage out. Mail is checked for viruses and any company policies are applied by Mailstream.

The bottom side firewalls provide another layer of security in keeping the Core network protected from the outside world. Even if a box is compromised, there are other components in place to mitigate risk. Figure 6 shows greater detail on the traffic flow from the outside world into the Core network through the SMTP Relays.

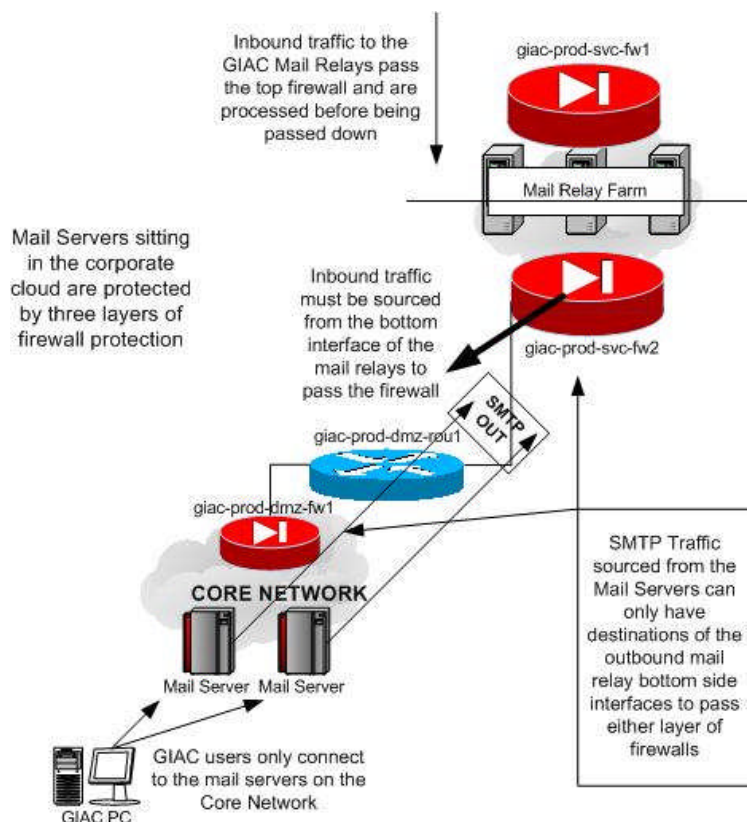


Figure 6 : SMTP Detail

As mail comes into the channel, the top side firewall passes it to an inbound relay VIP which then processes the information and passes it down. The bottom side firewall will only allow packets sourced from the bottom interface to pass. Packets must be destined for the internal mail servers to pass the firewall. All other traffic is dropped.

Once through the bottom service firewall, the DMZ core router makes a routing decision and passes the packets to the DMZ firewall protecting the core network. Packets destined for the mail servers are NATed, then passed to the Core network for delivery.

Outbound SMTP traffic works much the same way. The mail servers on the core network have queued mail to send out. The MTA contacts a NATed address on the DMZ firewall. The packet is translated and passed up to the DMZ core router then to the service firewall. On the outbound passage, only the bottom side outbound VIP is accessible, and it is only accessible from the NATed address on the DMZ firewall.

The weakness of this deployment is the reliance on the underlying Solaris operating system. Care must be taken to lock down the OS as tight as possible in order to mitigate risk of attack or compromise. The Center for Internet Security, <http://www.cisecurity.org/> has references for best practices and procedures for securing Solaris. Although using a supported version of Sendmail provides a support mechanism, the underlying application has a history of vulnerabilities and exploits. Subscribing to bug track and monitoring the Internet Storm Center will be key in keeping the SMTP traffic secured.

A GIAC requirement for employee web browsing is met through the use of a proxy channel. Trojans, worms, viruses and various other attacks are easily downloaded to corporate PCs through normal web browsing. In most cases, users have no idea what has happened and while the infections run rampant throughout the network, it goes undetected by support personnel. The challenge then becomes providing a safe and secure mechanism for web browsing that is easily supported and transparent to a technically unskilled employee.

Figure 7 : Web Proxy Overview

Blue Coat proxies also interoperate with a number of third party vendors for the purpose of virus scanning and web content filtering. The Blue Coat family also has a centralized management console to enforce corporate wide policies at multiple connection points. This centralized management system fits well into the other product choices made by GIAC. Having a centralized management point for all major DMZ components allows for the most efficient methods of device configuration and policy enforcement.

Users in the GIAC core network configure their browser proxy settings to the outbound proxy VIP address shown in Figure 7. This can be done either directly via IP address or through internal DNS hostname lookups. Direct access to the proxies is not allowed and all requests must be made to the VIP. The proxy will accept the connection and

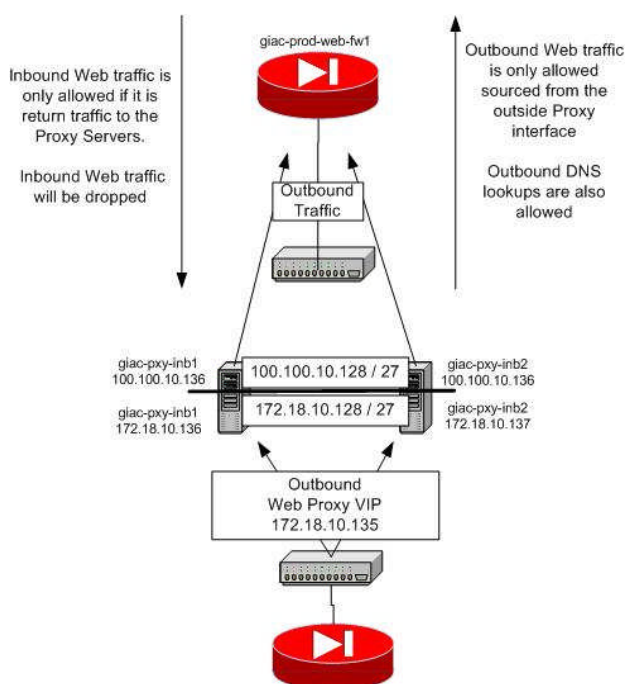


Figure 7 : Web Proxy Overview

request web resources on behalf of the requesting client. The resource only sees the source of the outside proxy interface and never knows the internal client.

The Blue Coat proxy also has a built in cache function that will store frequently used pages. This can speed up access for the internal user, as well as limit the number of external requests made by the proxy. For frequently used sites, this can drastically improve performance and better utilized bandwidth.

Included in the design component is a layered approach to traffic passing into and out of the core network. In Figure 8, the detail of traffic patterns is shown

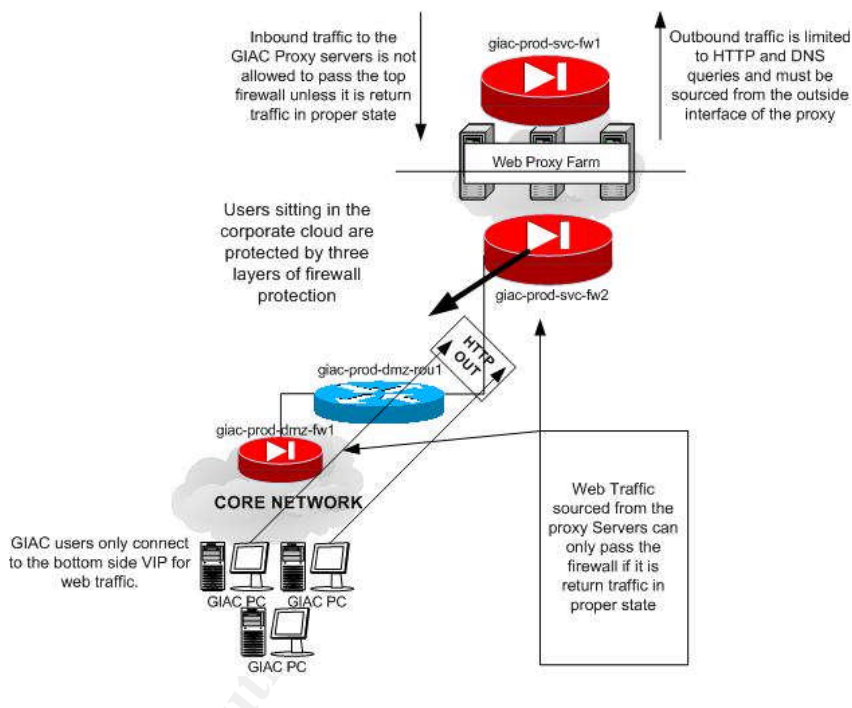


Figure 8 : Web Browsing Detail

and is similar in nature to the mail relay design. Core users sit behind the DMZ core router with a configured browser and make connections. The Blue Coat's operate on port 8080, so only port 8080 is required outbound of the DMZ Core firewall. Since there are a few hundred employees at the GIAC Headquarters any internal address has the ability to hit the proxy outbound of the DMZ firewall.

As with outbound SMTP traffic, once passed the DMZ firewall, the core router makes a routing decision and passes the traffic up to the service firewall. Only port 8080 traffic destined for VIP will pass the inspection engine and only return traffic can be sourced from the proxy VIP. Any traffic sourced from the inside proxy interfaces destined for other areas of the DMZ or internal cloud are dropped by the firewall.

Requests received by the proxy servers are processed, checked against the cache and then either returned to the user (cache) or requested from the internet. Outbound web requests and DNS queries are allowed to pass the topside firewall on port 80 and 443 (web) and 53 (DNS) for processing. Return traffic on those ports will pass, however traffic sourced externally destined for the proxy servers will be dropped.

The design weakness is inherent to any web proxy channel. The Internet is a dangerous place to do business and opening up web browsing capabilities only increases the chance of attack and compromise. The Blue Coat devices mitigate a

good portion of that risk. Their track record over the past few years has been excellent and as stated previously, they perhaps have the fewest known vulnerabilities on the market. The scaled down hardened OS specific to the appliance is a major contributor to that track record. Perhaps the biggest vulnerability on the Blue Coat appliances has been its vulnerability to overload. Since the topside internet pipe is relatively small when compared against the traffic load supported on the box, that weakness is mitigated to a large extent.

Client to Site VPN

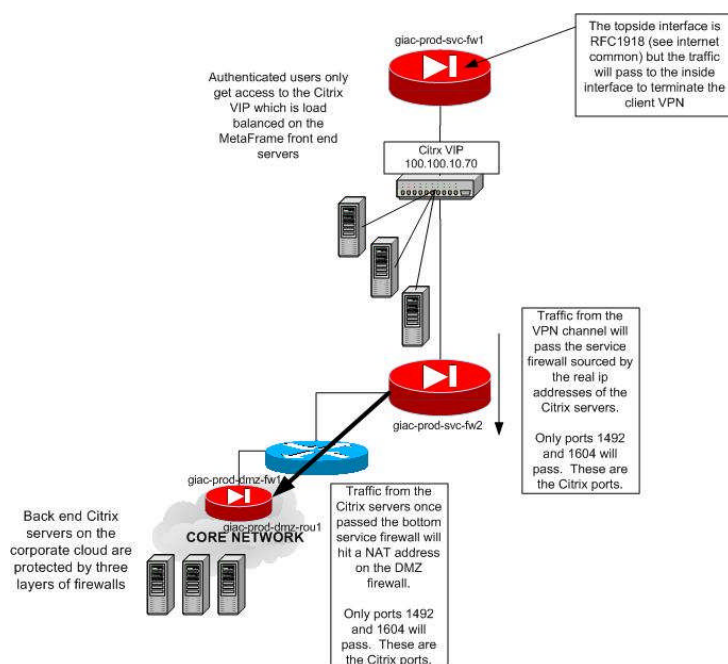


Figure 9 : VPN Traffic

The final major component for the perimeter is the need for a client to site vpn connection. Remote sales users and the need for work at home procedures drove the need for this requirement.

Standardizing on Checkpoint Firewalls makes VPN integration, management and maintenance a straightforward process. The VPN product is an easy add-on install to the firewall packages. SecureRemote and SecureClient are the products that Checkpoint distributes to setup client to site VPNs. The SecurClient package also allows for security policy enforcement and management on the client pc. Authentication is done via RSA/SecurID from the client. Individual users

authorized for remote access will be given tokens for remote access.

Also, GIAC internal technical personnel are very familiar with Citrix servers. The Citrix server farm component is the second component. Authenticated users will be granted access to the Citrix farm in the VPN channel, but no other boxes. Applications needed by corporate personnel are published to the Citrix MetaFrame servers on the edge.

Referencing figure 9, and keeping in mind the top firewall interface is RFC1918, VPN requests will pass to the bottom interface for processing. This maintains the crumple zone at the top of the Internet Common area. Using the SecureClient, users will enter their credentials for VPN 1 to pass to the Ace server. Upon successful authentication, the VPN rule will allow users access to the Citrix front end servers. User traffic should never pass beyond that VIP.

The real server ip addresses of the Citrix servers, while not accessible from the Internet, do need to communicate into the cloud. To accomplish this, rules are in place on the bottom side service firewall. Only the real server ip addresses of the Citrix box can communicate down into the cloud and the only ports available will be 1494 and 1604. As traffic passes down to the core network, the destination core servers are NATed at the DMZ router.

VPNs open up a whole host of problems. Since traffic is tunneled to the VPN endpoint and encrypted, ACLs on the border routers cannot stop malicious traffic and the topside firewall really can't detect it either. This problem is further compounded by the general lack of control of the client desktop where the VPN originates. To mitigate some of that risk, Checkpoint's SecureRemote client can enforce certain policies on the desktop.

The Citrix servers sit in a vulnerable position in this design. Since they are the only accessible hosts on the local subnet, they serve as even bigger targets. However, the design does lend itself to making attacks a bit more difficult. In order to compromise the server, the firewall module must be compromised first. Direct access to the Citrix servers is only allowed once users have authenticated, but that bottom firewall interface is local to the targets. Opening ports on the bottom service firewall also presents an opportunity for attack, but, the ports are limited and the only sources allowed through should be Citrix servers. A compromise of the topside firewall will not necessarily lead to the passing of malicious traffic down to the core. This layered approach is consistent throughout the DMZ design for GIAC.

Further augmenting that layered design is the DMZ firewall at the entry point to the core network. This firewall has host specific rules for defined ports. All other traffic will be dropped.

Network IDS

IDS placement in the GIAC environment is based on two factors:

- A need to monitor traffic and identify attacks
- A limited number of internal resources to monitor and support the IDS infrastructure

The need to monitor traffic and provide some form of analysis is key to an IDS implementation. However, it has been previously stated that the GIAC support staff is limited in size and knowledge.

In the DMZ environment, four IDS sensors are placed at strategic points to monitor traffic. Noticeably absent are IDS sensors above the primary firewalls. This decision is based on load. Since the support staff is limited, sensor placement is also limited. To monitor all traffic attempting to hit the DMZ would overload the support staff. All traffic entering the DMZ should be logged at the primary top side firewalls. This leaves two

major areas of traffic to monitor. The first area is directly behind the primary firewalls to monitor traffic on the registered subnets. The second area lies behind the internet accessible services at the entry points to the application servers and services. This placement monitors the key components of the DMZ and relies on firewall logs from the primary firewalls for additional traffic analysis. As previously stated, NIDS terminate backend connectivity in the Administrative network. The same network terminating the NIDS also terminate the firewall logs and syslog functions. A log correlation system has been implemented there as well.

A look at figure 10 demonstrates this thought process. Beginning just behind the primary web firewall, an IDS monitors traffic for both the secure and non-secure web presence. Keeping in mind that the most the internet bandwidth should grow to is a DS-3, the maximum possible throughput is 45MBs. The IDS should be more than able to keep up, particularly if it is configured correctly.

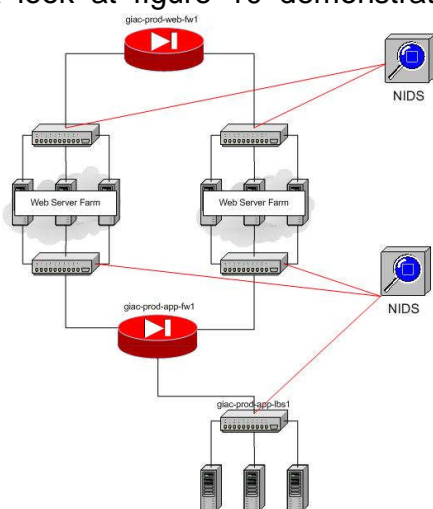


Figure 10 : NIDS Placement - WEB

A second NIDS is deployed to monitor traffic in the application zones. Bottom side calls from the web servers to the application servers, along with traffic on the application server segment is monitored.

The same placement approach is used for the service networks. A NIDS is placed below the top side service firewall and monitors traffic for the top side interfaces of the web proxy and smtp channels, along with the VPN segment. A second NIDS is

placed beneath the web proxy and smtp channels to monitor return traffic to the core network as well as outbound calls.

Since the NIDS monitor a number of segments, the log correlation point becomes critical. NIDS are responsible for primarily gathering data and will perform some basic analysis. However, the majority of data analysis is done on the correlation server.

GIAC Enterprises has standardized on Nokia IP 530 appliances running ISS Real Secure NIDS. The decision to work with the Nokia platform is made easy since it is the firewall standard hardware. ISS integrates into the Nokia platform in much the same way the Firewall 1 integrates making deployment and support an easier task.

The weakness in the design comes from the potential for overload of the NIDS and lost packets. Since each NIDS monitors a number of subnets, the traffic pulled can be extensive. Real time analysis by the NIDS appliance will be limited. Also, the load balancer component can account for a number of false-positives. We mentioned earlier that the health check performed by the load balancer to ensure servers are up and listening is a "syn / syn-ack" process that never completes a full TCP session. The NIDS will alert on this traffic as a syn flood attack if not configured correctly.

This weakness can be overcome by the correlation of logs from multiple sources. The admin network contains log servers from the NIDS, firewalls, routers and any other syslog compatible device. The log correlation server has the capability to provide extensive forensic data.

© SANS Institute 2004, Author retains full rights.

Administrative Components

While not placed at the perimeter, the administrative network is a key component in the design and management of the perimeter. In figure 11, the administrative zone is shown in detail.

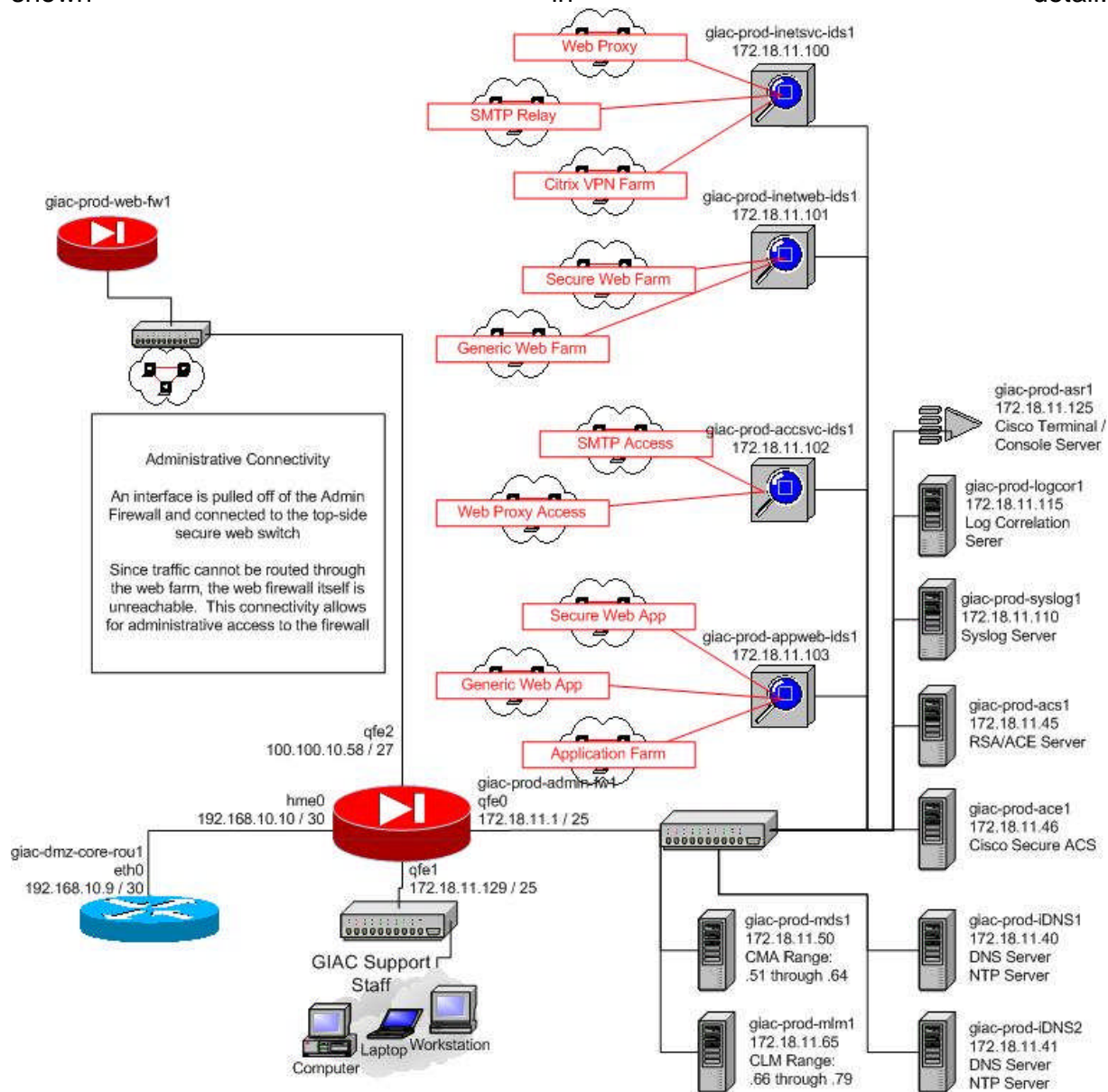


Figure 11 : Administrative Network

The admin firewall protects two specific networks from the perimeter. The first network is the GIAC support staff and their workstations. The second network is the perimeter services network. All address space in the admin network is RFC 1918 space that is non-routable outside the perimeter.

Admin Support Staff Net

The support staff network houses the GIAC support staff and their desktops. The room where the layer 2 segment terminates is a locked area requiring badge access to enter. The creation of the administrative LAN provides a centralized location for support staff to work that is secured from the rest of the network. There is a terminal server on the admin network that will allow for remote administration of devices. However, access to the terminal server is blocked at the admin firewall for non-authenticated users. A client to site VPN connection to the admin firewall using session authentication is needed to gain access to the terminal server.

Perimeter Services Net

Perhaps the most important area in the admin network is the perimeter services network. A number of critical functions are supported and configured from this network. Administrative access to all areas of the perimeter must be sourced from this network.

Checkpoint Firewall 1 has a centralized management tool called Provider 1. Provider 1 in the GIAC implementation resides on two servers: the MDS and the MLM. The MDS or Multi Domain Server centrally manages security policy, rule bases and VPN policies. Containers are created to logically group firewall objects together for ease of management. Virtual management stations are created on the MDS to aid in the ease of management. The MLM or Multi Log Server serves the same function as the MDS, however it manages log traffic. The MLM provides for the creation of virtual log servers to cut down on the size of the individual log files. The virtual log servers are created in conjunction with the virtual management stations.

Most perimeter devices resolve using DNS. Resolution for management traffic should be separate from resolution for general traffic. Perimeter devices use DNS servers in the services network for the purpose of resolving other perimeter devices. The DNS servers also run NTP services for the DMZ. NTP is an important function in the DMZ when deploying Checkpoint products. Checkpoint products verify authenticity of the management servers through a process called "SIC" or Secure Internal Communication. If the time functions of hosts are not synchronized properly, the SIC channel will fail and management of devices will also fail accordingly.

Both the Blue Coat proxy servers and the Mailstream Send Mail servers have centralized management consoles. As with Provider 1, these management consoles are located on the services network. By placing these consoles in this area, complete centralized management of the perimeter devices is achieved.

All NIDS devices have an interface connected to the services network. As NIDS pull traffic from the wire, backend connectivity to the log correlation database is achieved.

This backend connectivity also provides a secured location for the management interface. ISS's Site Protector management system is located in the services network and centrally manages the NIDS.

Logging is centrally located in the DMZ services network. Firewall logging and NIDS have already been mentioned. In addition, switch and router logging is maintained by a syslog server. The log correlation server can pull information from all of these sources to scan for events and provide forensic data.

Perimeter authentication and authorization uses SecurID tokens and TACACS+. This mechanism is in use in the secure web farm as well as the VPN channel. In addition, access to network devices (switches, routers, hubs and servers) requires SecurID as well. Users are managed via TACACS servers and authenticated via ACE servers. This design contains two server components: Cisco Secure ACS and RSA ACE Server. These servers reside in the admin services network.

The final piece to the admin services network is a Cisco Access Server Router (ASR) with Async ports. The ASR provides a mechanism for console access to devices. Every device in the DMZ has some form of console port for access. The ASR centralizes console access through reverse telnet functions to connected devices. It is the standard that all devices deployed in the DMZ have console access from the ASR.

Assignment 2 – Security Policy and Component Configuration

While the perimeter design in theory provides the appropriate functionality and security, actual implementation is key. GIAC Enterprises requested the actual security policy for the edge perimeter devices as proof of concept. In accordance with that request, the implemented configurations of the following devices are attached:

1. Border (Internet) Router
2. Web Firewall
3. Service Firewall (which will include the VPN configuration)

Border Router

The border router is comprised of GIAC-PROD-INT-ROU1 (IntRou1). IntRou1 is common to all DMZ and GIAC externally accessible components and is the foundation of the DMZ environment. In a fully deployed GIAC DMZ, the Internet Router will have two bottom side firewalls connected with a total of 5 accessible channels.

Overview

Specific to this design, the Internet Router only needs to route traffic to the generic and secure web farms, VPN channel, mail channel and web proxy channel. This is done via static routes. Beyond that, there is not a need for it to be aware of internal addressing, or, the DMZ addressing for that matter. Based on this design, dynamic routing protocols are not necessary on the bottom interfaces. BGP configured on the serial interface connected to the ISP in order to broadcast the available networks should be the only configured dynamic routing protocol.

The design aspect of the channelized approach puts the security burden on the firewalls as opposed to the router. However, the router itself needs to be hardened in order to mitigate risks at the entry point. Best practices for any bastion host dictates unnecessary services are turned off. A router on the edge is no different. The following commands have been issued to harden the internet router.

Global Configuration Commands

Remote administration of IntRou1 is allowed only via SSH. In order to setup SSH on a Cisco router, the following steps are necessary.

```
Hostname giac-prod-int-rou1
```

```
Ip domain-name giac.corp

Cry key generate rsa

Ip ssh time-out 25
Ip ssh authentication-retries 2

Line vty 0 4
access-class 99 in
Transport input ssh

access-list 99 permit 172.18.11.0 0.0.0.255
```

The hostname and domain name are required in an SSH configuration for the device to generate the RSA key. Internally, all DMZ devices have a domain name of “giac.corp” specifying them as internal. As .corp is not a legal publicly searchable suffix, external lookups for management ip addresses of internal devices is not possible. The next command generates the key used for SSH encryption from client to router. The time-out command specifies how long a requesting host has to pass credentials. While this setting seems somewhat high, it is set as such to allow for the requesting client to enter their pin and passcode from their SecurID token and for the router to receive a response from the ACS. Authentication retries refers to the number of failed passwords that can be sent before disconnect.¹

Simply setting up SSH is not enough. It must be applied to the administration point, in this case the virtual console line. The final two commands assign SSH to the virtual console. It is important to only assign SSH, and not other transports. If TELNET is also added, then the SSH setup can be subverted.

Now that the transport mechanism has been defined, the access mechanism must be hardened. The GIAC administrative network deploys a Cisco Secure ACS server and RSA ACE server. The ACS manages users and access levels while the ACE server manages authentication. The AAA commands create the setup for authentication (who are you), authorization (what can you do) and accounting (what did you do) on the router. These concepts are important as they allow us to make sure only specified users can make changes and for us to verify what changes they make. The access-class command matches to an access list specifying which networks can use the line. In this case, only the 172.18.11.0 / 24 network can access the router via the virtual console. This is the admin/support network.

```
aaa new-model
```

Creates the entry for AAA setup and configuration.

¹ Stephen Northcut, *Inside Network Perimeter Security* (Boston: New Riders, 2003), 143-158.


```
aaa authentication login DEVICE line
aaa authentication login DMZ group tacacs+ line
```

The authentication commands specify the types of authentication methods and gives them a name. This allows for the ability to specify different access methods for different access points. For instance, most of the administration of the box will be done via virtual console over the network. What if bottom side network connectivity was unavailable and a console was needed? If network connectivity is not there, then TACACS+ (explained later) will fail and router administration would be impossible. In this case two methods are specified: DEVICE and DMZ. The DEVICE method will use the line password and place the user in non-privileged mode. The DMZ method will use TACACS+ (prompting for a user name and passcode in the GIAC environment). However, if TACACS+ is unavailable, the line password will work after a timeout.

```
aaa authorization exec default group tacacs+ if-
authenticated
aaa authorization commands 15 default group tacacs+ if-
authenticated

privilege exec level 15 copy
privilege exec level 15 ssh
privilege exec level 15 reload
privilege exec level 15 write
privilege exec level 15 configure
```

The authorization commands specify the group access once successfully authenticated to the router. The first command specified that if a user is authenticated via TACACS+, place them in EXEC mode as opposed to non-privileged mode. The second command specified what the user can actually do in EXEC mode. Commands 15 references the privilege exec list and authorizes those commands for use by the user. Granular command listings are also specified in the ACS group on the CiscoSecure server.

TACACS+ is used as opposed to TACACS or RADIUS. TACACS+ is a TCP protocol where RADIUS and flat TACACS are UDP. Since we are working with user credentials, we need to guarantee delivery of the packets. Although UDP traffic is faster, TCP traffic is inherently more reliable.

```
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
```

Once users have been authorized for services, we must log what they are doing. The accounting commands will forward what the user is entering to a syslog server if authenticated via TACACS+.

```
Tacacs server host 172.18.11.45
```

```
line vty 0 4
  access-class 99 in
  exec-timeout 0 0
  transport input SSH
  password "ENCRYPTED PASSWORD"
  login authentication DMZ
```

```
access-list 99 permit 172.18.11.0 0.0.0.255
```

```
Service password-encryption
```

```
enable secret "ROUTER PASSWORD"
```

To complete the AAA setup, we must specify which TACACS server to use and then apply the authentication mechanism to the appropriate access method. Specification of the TACACS server is straight forward in the first command. Since we are going to use TACACS+ for remote administration, additional commands to the virtual terminal configuration are required. The access-class and associated access list along with the transport were described earlier. However the password and login commands have been added. The login command specifies the AAA method. Recall that DMZ was setup for TACACS+ first, then LINE. The password command specifies the line password for the virtual terminal. This password should be encrypted when viewing the config since the service password-encryption command was issued. This encrypts all passwords on the router except the enable password. Remember, when accessing via LINE the user is placed in non-privileged mode. This is useless for router configuration. The enable password is required for privilege access. The enable secret command encrypts the enable password using a different algorithm from the service password encryption method.

```
banner motd ^
```

```
*****
Warning - Warning - Warning Warning - Warning - Warning
This system is restricted to authorized individuals.
Unauthorized access is a criminal violation of the law and is
subject to prosecution.
```

```
All connections and changes are logged.
```

```
Warning - Warning - Warning Warning - Warning - Warning
*****
```

```
^
```

Finally, when anyone gains access to the router, they must understand they are accessing a secure device with penalties for unauthorized access. Also, they must know that there is a record of their actions. The banner accomplishes this.

Remote administration transport and logins are now effectively hardened on the Cisco Router. This should protect access to the device. Now, since the device is routing traffic, we need to lock down certain traffic flowing through the device. As mentioned in the architecture, the router is not the primary security device, however, disabling unused services and rudimentary filtering should be done at the edge

Globally, the following services should be disabled.

```
no service dhcp
no ip bootp server
```

The DHCP and BOOTP services are similar in nature. At the edge, there is not a need for dynamic address assignment or for the relay of address assignments to other machines.

```
no service config
no boot network
```

While backup copies of router configs are maintained for restoration purposes, GIAC does not allow for the remote loading of router configs. Disabling the network boot function restricts the router from looking for configs at a central location while disabling the service config turns off the remote configuration loading function of the router.

```
no ip source-route
```

Within IP, source routing can control the direction packets take to and from a destination. This is useful for man in the middle attacks and for traffic monitoring. Traffic should take its normal course traveling the internet to the GIAC border.

```
no service finger
```

Finger, while relatively old and obscure in nature, has some vulnerabilities and could provide user names of logged on administrators.

```
no ip domain-lookup
```

On the edge, and in the configuration used by GIAC, there is no need for the border router to execute DNS lookups. All the device is doing is passing traffic.

```
no ip http server
```

Cisco routers have a built in web server that allows for management and administration. Since router configuration can be done entirely at the command line, and most router

engineers have been using the command line over the years, it is an unnecessary function. Also, at the edge, HTTP administration is a dangerous option.

```
no service tcp-small-servers
no service udp-small-servers
```

Rarely used in nature, the small server services are susceptible to DOS attacks. Although these services are disabled by default in the IOS of choice for GIAC, it is good practice to explicitly disable the commands.

```
no ip unreachable
no cdp run
```

CDP or the Cisco Discovery Protocol is a method whereby routers can automatically configure next hop addresses for routing. On the edge, there is no need for this functionality. The IntRou1 should default out to the ISP interface on the topside, then static routes are used to point down into the DMZ as needed.

```
no ip classless
```

Unknown networks to the router may receive inbound traffic. Disabling IP classless limits the router from attempting to find routes for the packets.

Interface Level Configuration Commands

Besides global router options, certain functions can be disabled on a per interface basis. This allows for greater flexibility in the design. Typically, most of these functions are better used in the network core and should be disabled on the edge where they can be exploited.

```
no ip redirects
```

In some network environments, best routes change based on network conditions. This is more common in large scale networks using dynamic routing protocols, MPLS or other self-healing environments. An ip redirect changes the gateway a router uses to send traffic. At the edge, all routes are static and should not be changed without a redesign of the network.

```
no ip proxy-arp
```

Proxy arp allows for layer2 additions to local subnets across the router. If an attacker successfully mapped the network behind the router, they can use this service to logically place a remote machine on a local subnet.

```
no cdp enable
```

In addition to globally disabling CDP on the router, it should also be shutoff on a per interface basis.

```
no ip directed-broadcast
```

The SMURF attack makes use of directed broadcasts. A packet is sent to the broadcast address of a subnet not attached to the router. All hosts on that subnet are forced to respond and DOS situation will exist. While there are some legitimate uses for ip directed broadcasts (many financial Market Data Services utilize this function) they should not be deployed at the edge. Also, GIAC has no need for such services.

```
no ip unreachable
```

ICMP messages are very common in reconnaissance. Once such measure is to analyze the return ICMP message. An unreachable message can tell an attacker information about the design of your internetwork.

```
no ip mask-reply
```

Attackers attempting to map the networks behind the edge router use ICMP mask requests. When enable, the recipient host will send the mask used. While not a direct attack, this is a common and effective reconnaissance method.

“SHUTDOWN”

All unused interfaces should be turned off.

Basic Filtering

Further hardening of the edge requires some traffic filtering at a basic level. The firewalls, as mentioned earlier, provide the core of the security functionality. However, the router should also perform some basic protective measures beyond the host and service hardening already described.

```
no ip forward-protocol udp bootps
no ip forward-protocol udp bootpc
no ip forward-protocol udp tftp
no ip forward-protocol udp domain
no ip forward-protocol udp time
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp netbios-dgm
no ip forward-protocol udp tacacs
```

The edge router passes traffic into the DMZ for service access. It does not have a need to route traffic within the DMZ environment and certain protections should be taken to keep traffic in. Cisco routers can provide helper services, meaning that they can act on behalf of other clients and forward information out. Commonly attacked services such as Microsoft Netbios and DNS can be proxied by an intermediary host. These services should not be forwarded or helped at the edge router.

```
interface Serial0/0/0.500 point-to-point
description "ISP CONNECTION"
bandwidth XXXX
ip address w.x.y.z 255.255.255.252
ip access-group SECURITY in
no ip redirects
no ip proxy-arp
no cdp enable
no ip directed-broadcast
no ip unreachable
no ip mask-reply
frame-relay interface-dlci XXXX
```

```
ip access-list extended SECURITY
deny 55 any any
deny 77 any any
deny pim any any
deny tcp any any eq finger
deny udp any any eq snmp
deny udp any any eq snmptrap
deny udp any any eq bootps
deny udp any any eq netbios-ns
deny udp any any eq netbios-dgm
deny udp any any eq netbios-ss
deny tcp any any eq 22
deny tcp any any eq telnet
deny tcp any any eq 135
deny tcp any any eq 137
deny tcp any any eq 138
deny tcp any any eq 139
deny tcp any any eq 27374
deny tcp any any eq 12345
deny tcp any any eq 12346
deny tcp any any eq 54321
deny udp any any eq 54321
deny tcp any any eq 54320
deny udp any any eq 54320
deny tcp any any eq 1433
deny tcp any any eq 1434
deny ip 127.0.0.0 0.255.255.255 any
```

```
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
permit ip any any
```

The final component to hardening the edge is to block known problem traffic. The above configuration is from the Serial Interface of the router pointing to the ISP. Using the basic interface hardening techniques mentioned earlier, unnecessary services have been shut off. An access list is then applied for inbound traffic to the interface.

The access-list blocks ports recently known to pass Trojans and exploits into the network. It also blocks SNMP access into the router which can be used to obtain information about the location and setup of the device. Commonly exploited Microsoft networking services are blocked as there is no need for them to enter the DMZ from the outside. Port 22, commonly used for SSH is also used for PC-Anywhere remote administration tools. While we can SSH from the DMZ to the edge router from the inside, we should not be able to do the same thing from the outside. TCP 22 traffic should also not pass THROUGH the router and into the DMZ area. Ports 135, 137, 138 and 139 are additional common Microsoft networking ports that have recently been known to pass hostile traffic. Sub-7 attacks are blocked by denying port 27374. NetBus traffic is blocked by denying ports 12345 and 12346. Back Orifice is blocked by denying TCP and UDP on ports 54321 and 54320. Since there are no SQL servers requiring access, ports 1434 and 1435 are also blocked. Finally, traffic sourced from RFC1918 space should not enter IntRou1 from the external interface. While it is used in the DMZ, that space should not route inbound.

Border Router Summary

While the edge router is not the primary security device in this design, care should be taken to protect it from attack. The GIAC border router uses SSH for remote administration to the virtual ports. Once connected, the AAA configuration provides authentication, authorization and accounting function for connected users for historical and forensic purposes. AAA also provides access levels for users. Passwords for terminal lines and configuration modes are encrypted within the config. A banner is deployed to provide a method of notification of a protected and logged environment. All unnecessary services are turned off and blocked where appropriate. Interfaces are hardened by turning off unused services and disabling unused ports. Finally, some basic filtering of known attack and Trojan traffic is done on the edge interface.

Primary Firewalls

In keeping with the GIAC customer service focus, the web server and service networks are separated from the rest of the DMZ. This will separate all customer traffic from employee traffic. A single firewall is used for the web networks that will segregate two top-side (internet facing) web-server farms. Farm one is for generic inbound web traffic

to the GIAC general public website. Farm two is for secure inbound web traffic to the GIAC web front end for customer, supplier and partner access. A second firewall is deployed for employee service traffic. The firewall will have three attached service networks for inbound and outbound mail relay, internal web browsing and client-to-site VPN traffic.

The firewall security policy is divided up into two parts. First, the underlying platform must be hardened. This is the Nokia IP530 appliance and the global firewall policy setting. The IPSO operating system has a number of settings to increase the security of the of the physical appliance while the global settings in Firewall 1 lock down access. The second component is the actual firewall policy installed on the device. This will be specific to the channel and will have its own specific rule base.

This section will have two parts and will be laid out as follows:

1. Primary Firewall Hardening
 - a. Nokia IP 530 / IPSO Settings
 - b. General Firewall 1 Properties
2. Primary Firewall Security Policy
 - a. Web Networks Firewall
 - i. Secure Farm Rules
 - ii. Non-secure Farm Rules
 - b. Service Networks Firewall
 - i. Mail Relay Rules
 - ii. Proxy Rules
 - iii. VPN Configuration

Since the Nokia hardening and general Firewall 1 properties are common to both sections, it will be discussed first. Upon working with the firewall rule base, the assumption will be that the underlying appliance is hardened the same for both the Web and Service devices. Due to their placement at the edge, this is a good practice to maintain standardization.

Primary Firewall Hardening

Nokia IP 530 Appliance

Nokia devices have a function called “Voyager” which is a web based administration and monitoring tool. For the purposes of demonstration, this tool will be used to provide settings and screen shots of configuration parameters. However, it is highly recommended that this function be turned off. Keep in mind that the Nokia appliance is a hardened FreeBSD Unix variant. As such, SSH access for the purpose of command line administration is available and should be used. Once connected via SSH, there is a text based administration tool called “Lynx” that provides all of the same information provided by Voyager. However, since it is text based it can be difficult to read at times. More on this hardening measure will be discussed later.

The IPSO settings are very expansive. Included in the package is a fully functioning router along with a fully functional (although hardened) OS. While expandability and versatility are great options to have, care must be taken in the setup. Figure 12 shows the main menu for the Nokia IPSO. Firewall appliances should be built off of the production network in an isolated lab.

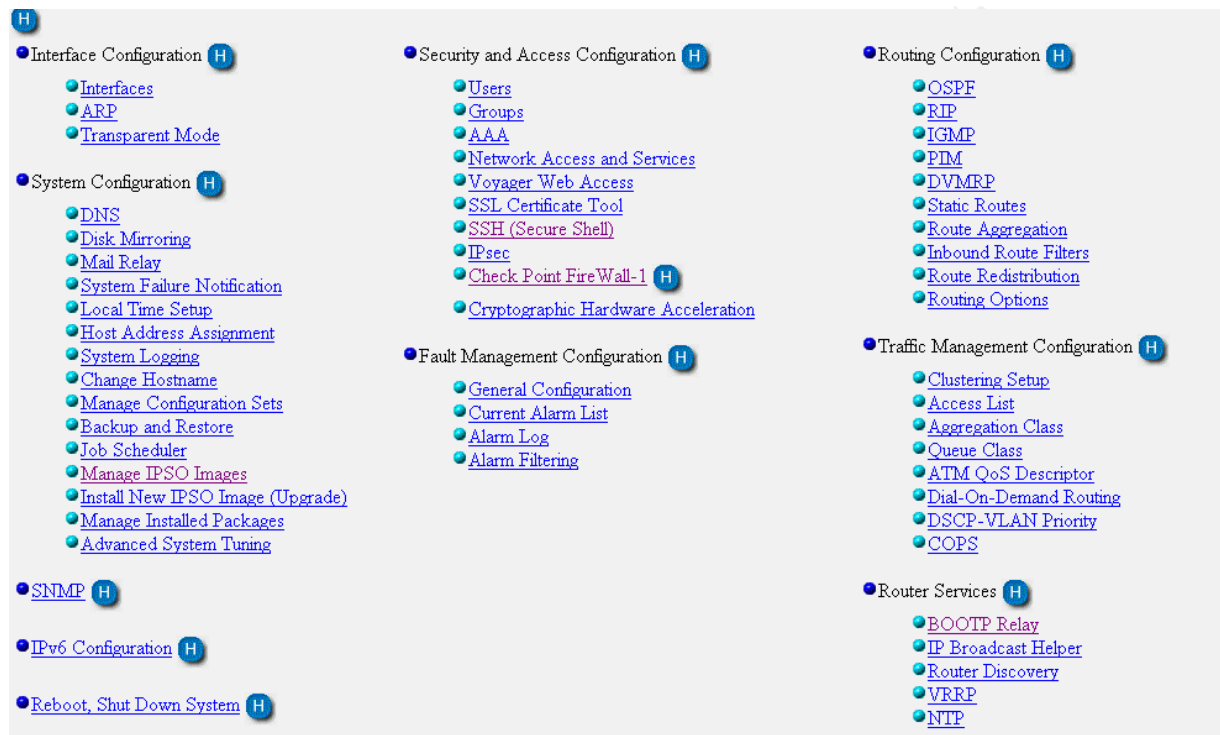


Figure 12 : Nokia Settings Main Menu

The Interface Configuration section contains general information regarding how the object is connected. Firewall 1 maintains access rights through those interfaces, so there is not an option to shut down services like we did on IntRou1. However, unused interfaces, like on IntRou1 should be shut down and turned off. There are two places to shut down an interface: logically and physically. If both are not turned off, it is possible to have an interface brought up if Layer 1 connectivity is sensed. In addition, it is preferable to hard code the link speed and duplex settings. When connected to various switches, the Nokia has shown to be problematic with auto speed/duplex settings. Of particular note in the interface configuration are the ARP settings. By default, the Nokia should not accept multicast arp replies. This protects the box from various Layer 2 and Layer 3 exploits as well as denies multi-cast arp packets. This is primarily used in QOS environments and can help with Voice Over IP and other traffic shaping functions. For the purposes of the perimeter, this is not necessary. Traffic should flow without interruption through the channels at the edge.

The System configuration contains the general networking functions that any host would require for communication in an internetwork. Some settings are important to mention for the setup of the appliance. The edge routers should point to the iDNS servers placed in the admin network for name resolution. There should not be a need for devices to resolve names externally. The Local Time setup needs to have its time zone set to the same as the NTP servers discussed later. If the configured time on the firewall varies too far from the management stations, SIC between the boxes will fail and policies will not install. System logging should be disabled as it is clear text, unencrypted traffic that is easily captured.

Upgrades and patches can be applied to the appliance from Voyager or Lynx as needed. The Manage IPSO Images and Install New IPSO Image sections allow for the upload of new OS images to the Nokia and installation. Installations require a reboot so this should be done carefully and only during scheduled outages. The Manage Installed Packages section allows for the upload of various software built to run on the IP appliance platform. Packages can be uploaded, then set to on or off for load upon boot. Package installation requires a reboot. SNMP can be turned off in the GIAC environment as it is not currently used anywhere.

The Security and Access Configuration is probably the most important portion of the configuration to lockdown. All access to the physical box is configured from this area. Like any OS, users and groups can be created to provide various functions. Like hardening any operating system, the ADMIN account should be renamed. Only users who need access should be given access and they should only be given the minimal access necessary to perform their jobs.

Network Access and Services is where the box can be hardened most at the appliance level. FTP, TFTP and TELNET access to the appliance can be shut off here. In addition, the "admin" account can be denied network access to the box. Since we shut off the admin account earlier and created a separate, renamed administrative account this is important. Some physical components can be shut off as well such as the COM ports and the PCMCIA card login. Administration in the GIAC environment is done only via SSH or console connectivity. TCP and UDP small services are the final options to disable. These services are disabled on ROU1 through a single command, however, in the IPSO each one needs to be disabled separately.

Voyager Web Access is also disabled. Again, screen shots are taken from the Voyager Interface for viewing purposes. But there is no need to keep it on in the production environment. Although it does make physically appliance configuration easier, there should not be many changes to the networking and security components of the appliance. The majority of the changes that take place will be firewall rules pushed to the Firewall 1 software component.

Voyager Access:	
Allow Voyager web access:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Cookie based session management:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Voyager port number:	<input type="text" value="80"/> (defaults to 80)
Voyager SSL port number:	<input type="text" value="7968"/> (defaults to 443)
Require encryption:	<input type="radio"/> None(Disable SSL) <input type="radio"/> 40-bit key or stronger <input type="radio"/> 56-bit key or stronger <input type="radio"/> 128-bit key or stronger <input checked="" type="radio"/> Require Triple-DES

Note: Changes to these settings may make Voyager unusable. You may use the 'voyager' command to reset them through ssh, telnet or console.


 H

Figure 13 : Voyager Access Settings

If GIAC decides in the future to enable Voyager, there are ways of locking down the connected TCP Port. SSL encryption is used for connectivity. Within the Voyager configuration, the port that SSL listens on can be changed to any port decided. This is good practice. Also, the encryption level can be set. A minimum of 128-bit should be set, with the preference going to Triple-DES. SSH connectivity can also be hardened and locked down. How SSH functions for network access is critical to maintaining the box. SSH is enabled by default, however the admin user is permitted log in rights by default. This should be turned off. Public Key and password authentication for SSH is enabled, but the older rhosts functions should be turned off.

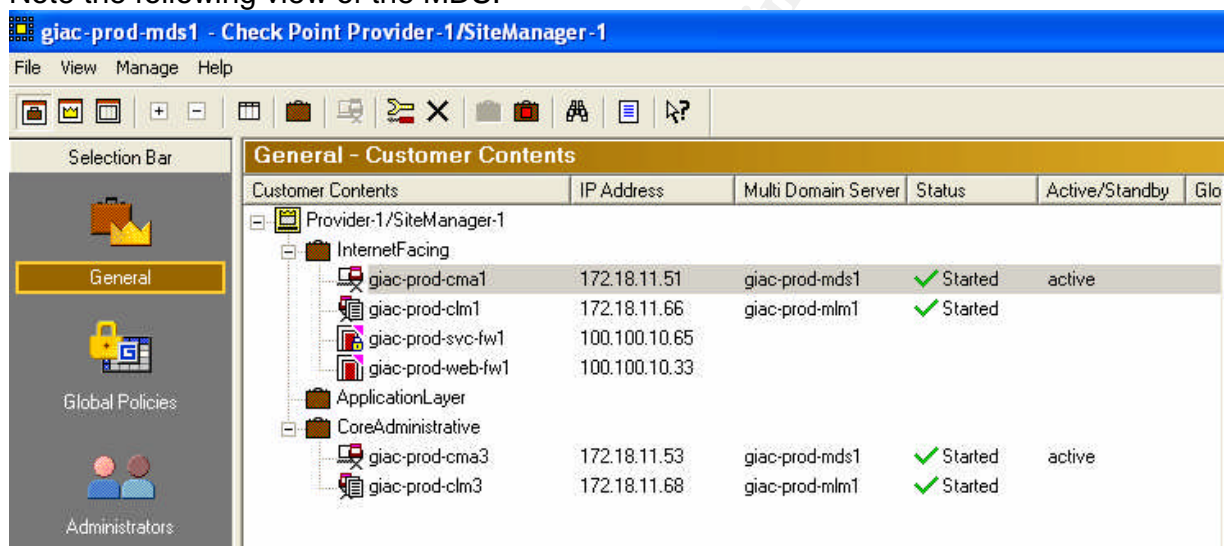
In the Routing Configuration, only static routes are used. The appliance at the edge should default up and out to internet. Static routes should be used to point back down into the DMZ only for specific subnets as needed. Again, the only access directly to the appliance should be made from admin zone. This should be the only route necessary to maintain connectivity and manageability. If the appliance receives a packet that it doesn't know what to do with, the firewall will log it, but it should then be passed out of the network. By default, in the Routing Options section, automatic router discovery is turned off. This is the desired setting and should be double checked prior to deployment.

Finally, Router Services manages at granular level on the interface BOOTP Helper, IP Broadcast Helper, Router Discovery and VRRP. All these functions should be turned off. NTP should be configured and turned on. This will allow the appliance to maintain proper system time from the GIAC NTP servers in the Admin network. As stated earlier the relationship of time between the Checkpoint components is crucial to centralized management.

Global Firewall Settings

Checkpoint Firewall 1 installed in any environment on any platform has the same functionality. GIAC chose Nokia appliances as the underlying platform system and it is now hardened and ready for use. The second standard step to complete is the global firewall behavior. While the Nokia configures the networking and access methodology through its own interface, the firewall module is configured via a Checkpoint Management interface.

For the GIAC implementation, as discussed earlier, Provider 1 Multi Domain Server (MDS) is used. Within the MDS, virtual Customer Management Agents (CMA) are used to manage the firewall modules. Customer Log Modules (CLM) are also virtual hosts within the management domain that manage the log functions of the firewall module. Note the following view of the MDS:



Giac-prod-cma1 is the master CMA for the Internet Facing container. This logical grouping allows for firewalls to be managed according to their function.

Administrators are defined within the GUI as well. Administrators can have various rights of management and this can be controlled at a granular level. Administrators can have access to all modules or only to certain containers. Based on function, administrators should be given the least permissions necessary to do their job. The Provider-1 SuperUser function should not be used as a permission level for daily activity. This is the security theory of least privilege.

For the proof of concept required by GIAC, the focus will be on the two edge firewalls: giac-prod-web-fw1 and giac-prod-svc-fw1. Both of these firewalls provide perimeter protection and as such are managed together. To manage the firewalls, launch the CMA application.

Additionally, GUI clients must be specified within the application. The MDS, MLM, CMA and CLM hosts will only accept connections from machines specified in the configuration. For GIAC enterprises, there are only two servers with access to the management gui. Both of the servers are Windows terminal servers located one each located in the DMZ Admin Service Network and DMZ Support Staff Network. The terminal servers are screened from the Core network by two firewalls and from the Internet by two other firewalls. Additionally, they are physically locked in a closet in a secured area in the data center. Access to the terminal servers requires a Windows username/password combination in addition to RSA/SecurID authentication.

Policies are managed the same way files are managed on a PC. They are saved to the CMA component and can be retrieved for editing. While a CMA will manage multiple firewalls, by default only one policy is created. Rules are specified based on target where they apply upon installation. This is not an effective or secure way of managing rules. Each firewall should have its own rule base and its own rule base file. From the CMA, you can select which rule base to work on with the FILE -> OPEN menu options. For GIAC, each firewall has its own rule base.

Each managed firewall on a CMA has a management object defined. That management object shows specific networking and Checkpoint information about the firewall module. There is a topology section of that configuration option that allows the administrator to specify whether interfaces are internal or external to the network. Internal interfaces are considered trusted, external interfaces are not. Using the topology section, GIAC is able to automatically configure anti-spoofing at the edge firewall. Attempts to spoof addresses inbound to the non-trusted interfaces are logged. This is the GIAC standard.

For this section of the policy configuration discussion, the focus will be on the Global Properties settings. This is accessed from the Policy Menu within the GUI. The Global Properties dialogue creates implied rules in the rule base. They are not seen when viewing the rules by default. In addition, some standard rules common and necessary to any good rule base implementation will be discussed.

The implied rules main dialogue page has settings of interest for maintaining a good security posture. For centralized management, certain settings must remain on. VPN-1 & Firewall-1 Control connections is a required setting for remote management in the GIAC environment. Since the service firewall in this group is also the VPN termination point, Remote Access control connections will remain on as well. On the web firewall, the VPN software was not installed therefore this setting will have no effect on that device and can be left on safely.

The setting for "Accept outgoing packets originating from Gateway" function allows for traffic originating from any interface to safely pass the inspection module for routing. This is important for routing log traffic through the firewall from the outside interfaces. RIP, TCP/UDP DNS (zone transfer and queries) and ICMP acceptance should all be turned off in the GIAC environment. None of these services originate from the firewall

and none of those services are required through the firewall from interface to interface. The most glaring default setting that has been changed is Track method. By default, Firewall-1 does not log traffic passed or dropped by the implied rules. This has been turned on for the GIAC environment. Since there is not an IDS on the edge outside of the firewall, it is important to track as much traffic as performance will allow for log correlation and analysis.

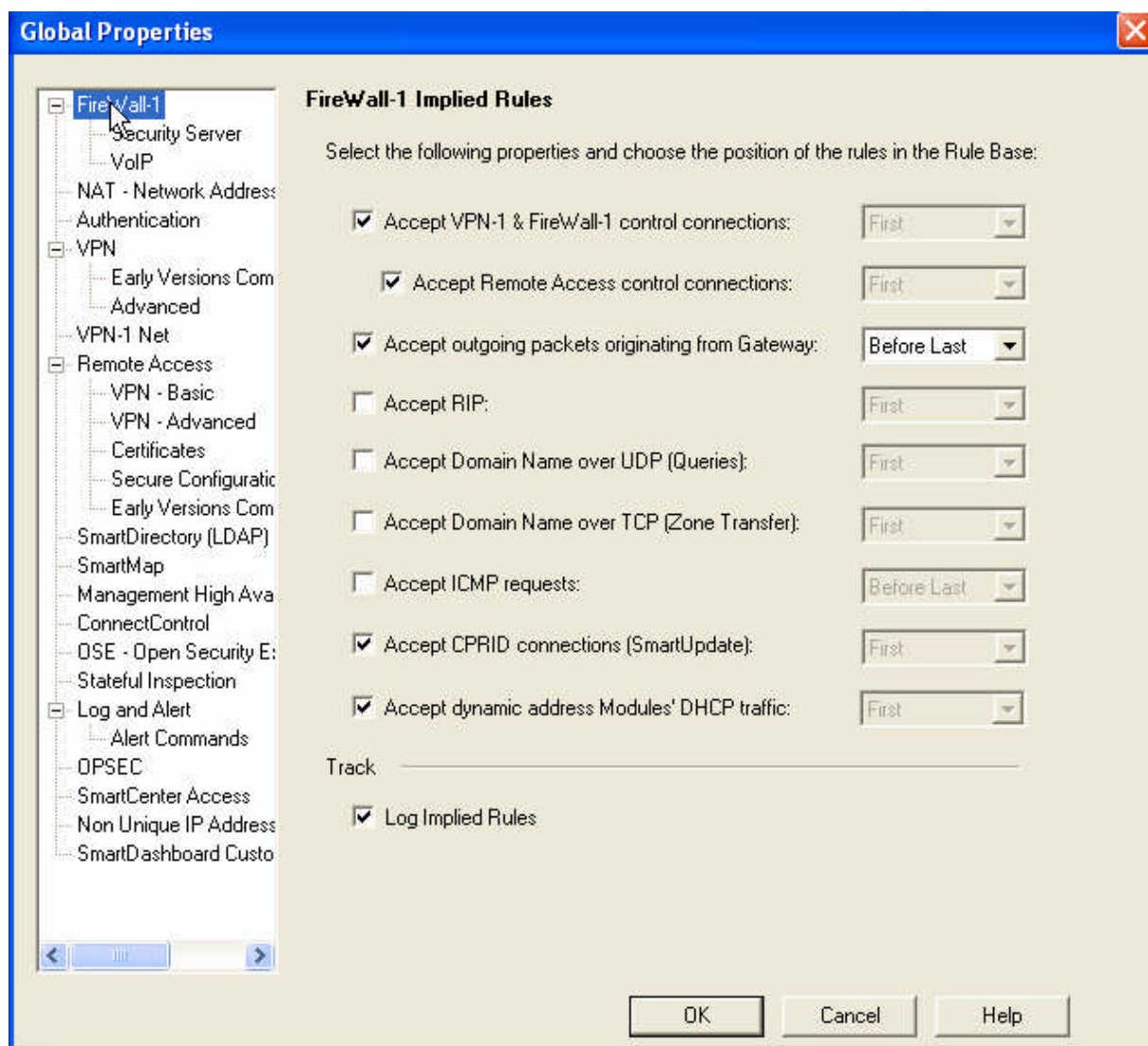


Figure 14 : Global Properties

A standard rule base is now created for module installation. GIAC adheres to the principal that all traffic not explicitly allowed to pass is dropped. Also, traffic destined for the firewall not explicitly necessary for administration is dropped. This leads to the implementation of two common rules: the stealth rule and the cleanup rule. These two rules, placed at the bottom of the rules base will drop traffic destined for the firewall and destined through the firewall respectively. The stealth rule attempts to hide the firewall

and prevent fingerprinting of the OS and software. The cleanup rule drops all traffic not specifically allowed.

The location of these rules is key. Checkpoint Firewall-1 operates on a first match basis. The first rule that applies to the specified traffic is used. Based on this, the rules need to be placed with the stealth rule near the top, but after any rules that will directly connect to the firewall (i.e. SSH) and the cleanup rule last. The implied rule to accept Firewall-1 control connections is setup first in the rule base. If the stealth rule were installed above the control connections rule, policy installation and Firewall-1 management would fail since the stealth rule drops that traffic. The cleanup rule drops everything that does not have a rule match in front of it. Any rules installed below it in the rule base will not be inspected. Hence it is aptly named as it “cleans up” any unwanted traffic and drops it.

SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
★ Any	 giac-prod-web-fw1	★ Any Traffic	★ Any	 drop	 Log	 giac-prod-web-fw1	★ Any	Stealth Rule
★ Any	★ Any	★ Any Traffic	★ Any	 drop	 Log	 giac-prod-web-fw1	★ Any	Clean Up Rule

Figure 15 : The Stealth and Cleanup Rules

Summary

Using these techniques, the underlying hardware, operating system and basic firewall configuration is secured. Beginning with the Nokia appliance, all unused services and interfaces are turned off, much in the same way we hardened IntRou1. Built in administrator accounts were disabled, and renamed ones were implemented to take their place. Telnet access was disabled and SSH access was locked down. Access to the management server for the firewall modules was locked down and only authorized servers can connect. Administrators are defined and only given access to the modules and containers they need to perform their duties. Each firewall module has its own policy file and these are managed on the CMA. The installed Firewall 1 software is then hardened using the global properties and implied rules are set to log to create a standardized firewall module appropriately hardened for the GIAC environment. Finally the stealth and cleanup rules are implemented to protect the firewall and the networks behind it.

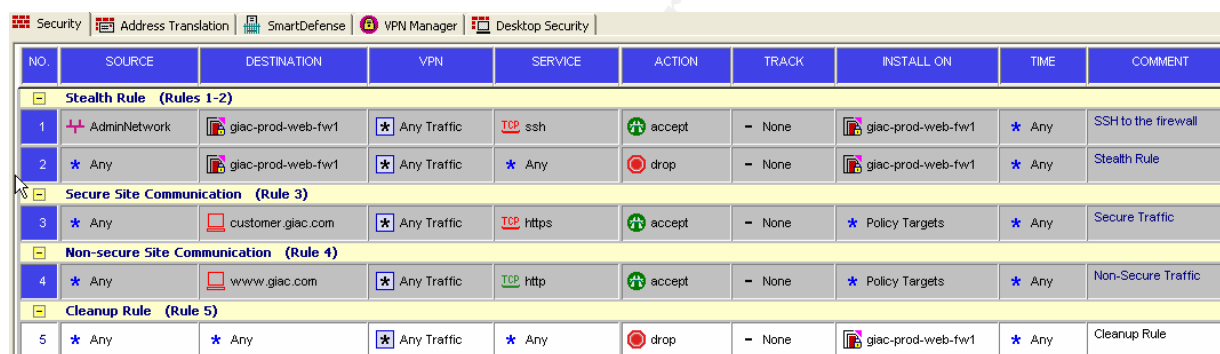
Security Policy for Primary Firewalls

There are two primary firewalls in the GIAC DMZ. One firewall protects the web networks and one firewall protects the DMZ services and VPN. The setup maintains customer focus. The larger a rule base gets, the harder a firewall has to work. Web farm rule bases are straightforward and simple and very few rules are needed. This removes much of the workload from the firewall. The DMZ services network is a bit more complicated and will require a larger rule base causing more load on the firewall module. However, the services network is built with the GIAC employee in mind and therefore if performance suffers, customers should not be effected.

Web Networks Security Policy

The primary driver for the implementation of the GIAC DMZ is to provide a system for GIAC customers to have access to an on-line ordering system where they could purchase, track and download their needs. In addition, as GIAC continues to grow, an Internet point-of-presence is desired for advertising and dissemination of non secure data to the rest of the world.

The architecture calls for a web network with two web farms. One farm for secure traffic and one farm for non-secure. Referring back to Figures 2 through 4, the primary firewall only protects the top side interfaces of the web servers. Traffic passing through the firewall is routed to the appropriate VIP based on the request. No other services are required to meet the customer need at the perimeter. This makes the rule base for the web network very small. Since Checkpoint Firewall-1 uses a stateful inspection engine, return traffic is automatically allowed. The secure and non-secure web farm rule base should only have five rules as follows:



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Stealth Rule (Rules 1-2)									
1	AdminNetwork	giac-prod-web-fw1	* Any Traffic	TCP ssh	accept	- None	giac-prod-web-fw1	* Any	SSH to the firewall
2	* Any	giac-prod-web-fw1	* Any Traffic	* Any	drop	- None	giac-prod-web-fw1	* Any	Stealth Rule
Secure Site Communication (Rule 3)									
3	* Any	customer.giac.com	* Any Traffic	TCP https	accept	- None	* Policy Targets	* Any	Secure Traffic
Non-secure Site Communication (Rule 4)									
4	* Any	www.giac.com	* Any Traffic	TCP http	accept	- None	* Policy Targets	* Any	Non-Secure Traffic
Cleanup Rule (Rule 5)									
5	* Any	* Any	* Any Traffic	* Any	drop	- None	giac-prod-web-fw1	* Any	Cleanup Rule

Figure 16 : Web Firewall Rule Base

The security requirement for the web farm states:

Customers, partners and suppliers need access to a secure system to purchase GIAC products, work with GIAC applications or supply GIAC with goods and services

A web presence on the Internet for GIAC

All unnecessary traffic to be discarded

These four rules meet that need at the edge. Two objects are created representing the GIAC systems for access:

customer.giac.com is created with an ip address of 100.100.10.37

www.giac.com is created with an ip address of 100.100.10.5

These are the only two externally accessible addresses required. Figure 4 demonstrates the VIP configuration on the load balancer beneath the firewall. The “real” or configured ip addresses of the web servers are not required externally. Communication will flow through the firewall to the VIP. The VIP will broker connectivity to and from the web servers on behalf of the client. All traffic inbound is destined for the

VIP and all return traffic is sourced from the VIP as brokered by the load balancer. This functionality is built into both web channels.

One of the goals is to protect the web servers from potential compromise. Since direct access to the webserver is not allowed, we mitigate this risk at the firewall by using the VIP on the switch. Also, SSL (443) traffic flows only to the VIP. The VIP can hand traffic off to the real server ip addresses on any port specified in the configuration. This further protects the web servers. An uncommon port (eg 34443) can be used in place of the standard on the web server.

The order of the rules shows the emphasis placed on the customer web site. Access to the customer web site is placed first in the rule base after administrative access is locked down. Access attempts are logged at the firewall. NIDS are not placed above the firewall and this logging function allows for better traffic analysis and forensic data. Since the support staff is limited in resources, access attempts to the non-secure web site is not logged to reduce the amount of traffic stored. The first rule in the rule base allows administrative access, followed by the stealth rule. The last rule in the rule base is the cleanup rule explained earlier.

Rule management in Checkpoint Firewall-1 is made easier by a new feature that allows for rule headings. This creates logical groupings of rules to make it easier to organize multiple functions running on the same box. GIAC is a growing company and in the future new secure and non-secure websites are planned for implementation within this architecture. If new services and applications are deployed, the headings will make rules easier to manage cutting down on the potential for mistakes that could lead to vulnerabilities at the edge.

Service Networks Security Policy

The service networks firewall has a more expansive rule base. Three major services are deployed in the service networks:

1. Web Proxy
2. SMTP Relay
3. VPN

Each of these will have specific rules for functionality. As discussed in the web networks policy, rules will be grouped according to function in an attempt to ease administration. Also, even though the same CMA manages both firewall modules. A separate policy file will be managed to separate the rules. As with the web farm rules, the final rule in the policy will be the cleanup rules. The stealth rule still needs to be placed near the top, however it must come after any rules specified for VPN access since that traffic terminates at the firewall.

Web Proxy Security Policy

The web proxy topside network does not require inbound access. All sessions flowing to and from the web proxies are originated from the inside. Therefore no inbound rules are necessary. Return traffic will be allowed provided it is in state.

Figure 7 shows the web proxy architecture. Four objects are created for inclusion in the rule base:

1. giac-pxy-inb1 / outside interface – 100.100.10.136
2. giac-pxy-inb2 / outside interface – 100.100.10.137
3. ISP DNS Server 1 – 125.125.125.1
4. ISP DNS Server 2 – 125.125.125.2

The rule base specific to the web proxy looks like this:

WEB Proxy Rules (Rules 4-5)									
4	giac-pxy-inb1 giac-pxy-inb2	ISP-DNS1 ISP-DNS2	Any Traffic	dns	accept	Log	giac-prod-svc-fw1	Any	Outbound DNS queries for Proxy
5	giac-pxy-inb1 giac-pxy-inb2	Any	Any Traffic	http https ftp	accept	Log	giac-prod-svc-fw1	Any	Outbound HTTP, HTTPS and FTP

Figure 17 : Web Proxy Rules

Rule 4 allows the web proxy server to query the DNS servers of the ISP. The Blue Coat Proxy will perform this function on behalf of the client pc. This is important to maintain the anonymity of the core network. Rule 5 allows the proxy server to make requests on behalf of the client for http, https and ftp. No other web services are allowed.

As previously stated, there are no inbound rules necessary. Proxy servers are typically vulnerable devices since they perform an easily exploitable function. GIAC has mitigated a good portion of that risk by choosing the Blue Coat platform based on its good track record. However, since no externally sourced inbound traffic is necessary for the web proxy function, it will be dropped at the edge firewall.

SMTP Relay Security Policy

Only slightly more complex than web proxy rules, SMTP relay traffic is still fairly simple to create security policy for. Reference the following rule base:

SMTP Relay Rules (Rules 1-3)									
1	giac-smtp-otb1 giac-smtp-otb2	ISP-DNS1 ISP-DNS2	Any Traffic	dns	accept	Log	giac-prod-svc-fw1	Any	Outbound DNS Queries for SMTP
2	giac-smtp-otb1 giac-smtp-otb2	Any	Any Traffic	smtp	accept	Log	giac-prod-svc-fw1	Any	Outbound Mail traffic from outbound relays
3	Any	smtp-giac.com	Any Traffic	smtp	accept	Log	giac-prod-svc-fw1	Any	Inbound SMTP traffic to MX VIP

Figure 18 : SMTP Rule Base

The SMTP Relay rule base needs the following objects:

1. Mail Relay VIP – 100.100.10.99

2. giac-smtp-otb1 / outside interface – 100.100.10.102
3. giac-smtp-otb2 / outside interface – 100.100.10.103
4. ISP DNS Server 1 – 125.125.125.1
5. ISP DNS Server 2 – 125.125.125.2

As with the web proxy function, the outbound mail relays need to initiate DNS requests to the ISP DNS servers. Rule 1 allows for this function. Rule 2 then allows the outbound mail relays to send SMTP traffic to a recipient host on the internet.

Rule 3 is all that is required for inbound mail. Only traffic destined for the GIAC MX registration of 100.100.10.99 is allowed. Inbound traffic destined for the outbound interfaces of the relays needs to be dropped. The VIP will broker traffic on behalf of the inbound relays. This function will work the same as it did for the load balancing done in the web farms. The bastion hosts are the most vulnerable. It is possible to mitigate some of that risk through the use of VIP configurations on the layer 2 segment behind the edge protection device.

VPN Configuration and Security Policy

Setting up VPN connectivity is more complex than simply adding traffic rules. There are a number of steps involved. The basic configuration has the following steps:²

1. Configure the gateway object for SecuRemote
2. Create SecuRemote Users
3. Define the Client encryption rules and RAS community rules
4. Configure the global properties
5. Configure the Desktop Security policy
6. Install the policy to the firewall module

In configuring the gateway object, a VPN community must be built. This creates an overview of how the VPN network looks, who has access and what they can access. The VPN community pairs with the defined user objects to create rules and allow access. From the policy menu, enter the VPN configuration window by selecting its appropriate tab. Right click in the top window and create a new community. The GIAC Community created for this implementation is a star topology. This allows users to connect to internal resources as permissions allow. In the general dialogue, the important setting is the VPN routing selection box. The option for “to center” is selected. This allows remote access users access to an internal resource, and nothing more. It prevents routing to other remote access clients and it prevents traffic from routing outside the DMZ.

The service firewall gateway object is then added to the community. This specifies which gateways can terminate the VPN connection. Only the GIAC service firewall should terminate VPN endpoints. The global properties have already been setup for VPN access when we standardized the initial implementation of the firewall device.

² Dameon D. Welch-Abernathy, *Essential Checkpoint Firewall-1 NG*. (Boston: Pearson Education, 2004), 426-427.

Once the VPN community is created, it is then defined on the object properties of the service firewall. In the object properties is on the general window. SecureClient Policy server is selected. GIAC rules for VPN require strict adherence to corporate security policy for remotely connected users. SecureClient will allow for that policy enforcement. While within the global properties of the firewall object, authentication methods are chosen. GIAC, explained in further detail later, requires two-factor authentication. SecurID is the only method selected on the GIAC VPN device. The authentication tab also has a drop down box to select user groups for remote access. A VPN users group has been created (explained later) and is selected.

On the global properties dialogue from the Policy menu, select Remote Access, then VPN basic from the tree. Within that frame, is a setting for IKE over TCP support. In today's environment, many GIAC personal have personal firewalls at their home providing NAT services. With some of these devices, UDP encapsulation is not supported and the VPN will fail. This setting supports improved translation of IKE packets when communicating with a NAT device.³

The next step is to configure the user objects for remote access. This is done by selecting the users section of the objects tree. In the GIAC DMZ design, all VPN users have access to only one resource, the Citrix VIP servicing the Citrix farm. Also, since it is only necessary to define users on this firewall module if they are authorized for remote access, the easiest configuration is to edit the default user profile. All new users created will use the default user profile as their template. The User Properties dialogue box allows the control of many settings.

³ Chris Tobkin, *Check Point NG/AI* (Rockland, MD: Syngress, 2004), 457 – 461.

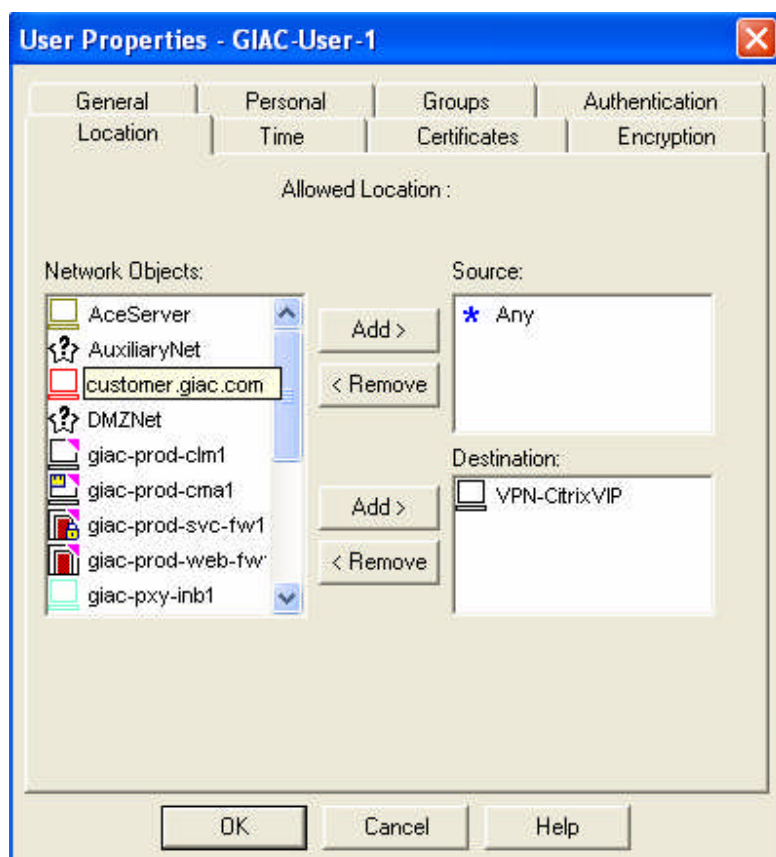


Figure 19 : User Properties

First is location. This creates the rule and specifies which resources a user can access. GIAC users, as mentioned earlier, only get access to the Citrix VIP. This is defined on the location tab. The rule will allow a user from anywhere on the Internet to VPN “in” to the network then get access to the Citrix farm. The next important tab is the authentication tab. GIAC requires two-factor authentication for all external access. In the authentication tab dialogue box, SecurID is selected.

Now that the firewall is configured, a rule needs to be added for access. Users are restricted to a single destination host, the Citrix VIP based on the user properties for the VPN users group. Checkpoint NG simplifies the rule creation through the use of the global and object properties. The actual rule to implement the VPN looks like this:

Remote Access Rules (Rule 6)									
6	VPN-Users-Group	VPN-CitrixVIP	GIAC-VPN	* Any	accept	Log	giac-prod-svc-fw1	* Any	All user access to the Citrix Farm via VPN

Figure 20 : VPN Rule

As stated earlier, some control of user traffic and desktops will be required for VPN user. The basis for this was created when the SecureClient Policy Server option was selected. This option installs a personal firewall onto the desktop of the VPN client and enforces a separate rule base defined in the Desktop Security portion of the policy editor for users while connected.

Since VPN traffic is tunneled to the VPN endpoint, the protections from known problem ports and traffic configured on IntRou1 are bypassed. Since VPN users are only allowed to access the Citrix VIP, GIAC configured a desktop policy to block all traffic except for traffic destined for the VIP using the Citrix protocols.

Inbound Rules						
NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMMENT
1	* Any	All Users@Any	* Any	Block	- None	Block traffic destined for the desktop

Outbound Rules						
NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
2	All Users@Any	VPN-CitrixVIP	TCP Citrix_ICA UDP Citrix_ICA_Bro Citrix_metaFran	Accept	Log	Allow Citrix traffic
3	All Users@Any	* Any	* Any	Block	- None	Block all non Citrix traffic from the client

Figure 21 : Desktop Policy Rules

The installed policy on the desktop is stateful in nature. Return traffic will be allowed so communication to the Citrix VIP will flow freely. However, any other connectivity request, in either direction will be blocked.

The full security policy for the Service Firewall is as follows:

Security Address Translation SmartDefense VPN Manager Desktop Security									
NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	AdminNetwork	giac-prod-svc-fw1	* Any Traffic	TCP ssh	accept	- None	* Policy Targets	* Any	Administrative Access
SMTP Relay Rules (Rules 2-4)									
2	giac-smtp-otb1 giac-smtp-otb2	ISP-DNS1 ISP-DNS2	* Any Traffic	dns	accept	Log	giac-prod-svc-fw1	* Any	Outbound DNS Queries for SMTP
3	giac-smtp-otb1 giac-smtp-otb2	* Any	* Any Traffic	TCP smtp	accept	Log	giac-prod-svc-fw1	* Any	Outbound Mail traffic from outbound relays
4	* Any	smtp-giac.com	* Any Traffic	TCP smtp	accept	Log	giac-prod-svc-fw1	* Any	Inbound SMTP traffic to MX VIP
WEB Proxy Rules (Rules 5-6)									
5	giac-pxy-inb1 giac-pxy-inb2	ISP-DNS1 ISP-DNS2	* Any Traffic	dns	accept	Log	giac-prod-svc-fw1	* Any	Outbound DNS queries for Proxy
6	giac-pxy-inb1 giac-pxy-inb2	* Any	* Any Traffic	TCP http TCP https TCP ftp	accept	Log	giac-prod-svc-fw1	* Any	Outbound HTTP, HTTPS and FTP
Remote Access Rules (Rules 7-8)									
7	VPN-Users-Group	VPN-CitrixVIP	GIAC-VPN	* Any	accept	Log	giac-prod-svc-fw1	* Any	All user access to the Citrix Farm via VPN
8	* Any	giac-prod-svc-fw1	* Any Traffic	* Any	drop	Log	giac-prod-svc-fw1	* Any	Stealth Rule
Cleanup Rule (Rule 9)									
9	* Any	* Any	* Any Traffic	* Any	drop	- None	giac-prod-svc-fw1	* Any	Cleanup Rule

The first rule in the rule base allows GIAC administrators to access the device from the network via SSH. Rules two through four setup SMTP relay traffic to the inbound VIP as well as allow the outbound relays to send mail. Rules five and six allow the proxy servers to browse on behalf of the users without allowing inbound traffic sourced externally to hit them.

The service rule base has the Stealth Rule lower in the rule base than the web firewall. Since the stealth rule would block VPN termination, it needs to be applied after the VPN rule. Finally, the cleanup rule drops all traffic not explicitly allowed.

Summary

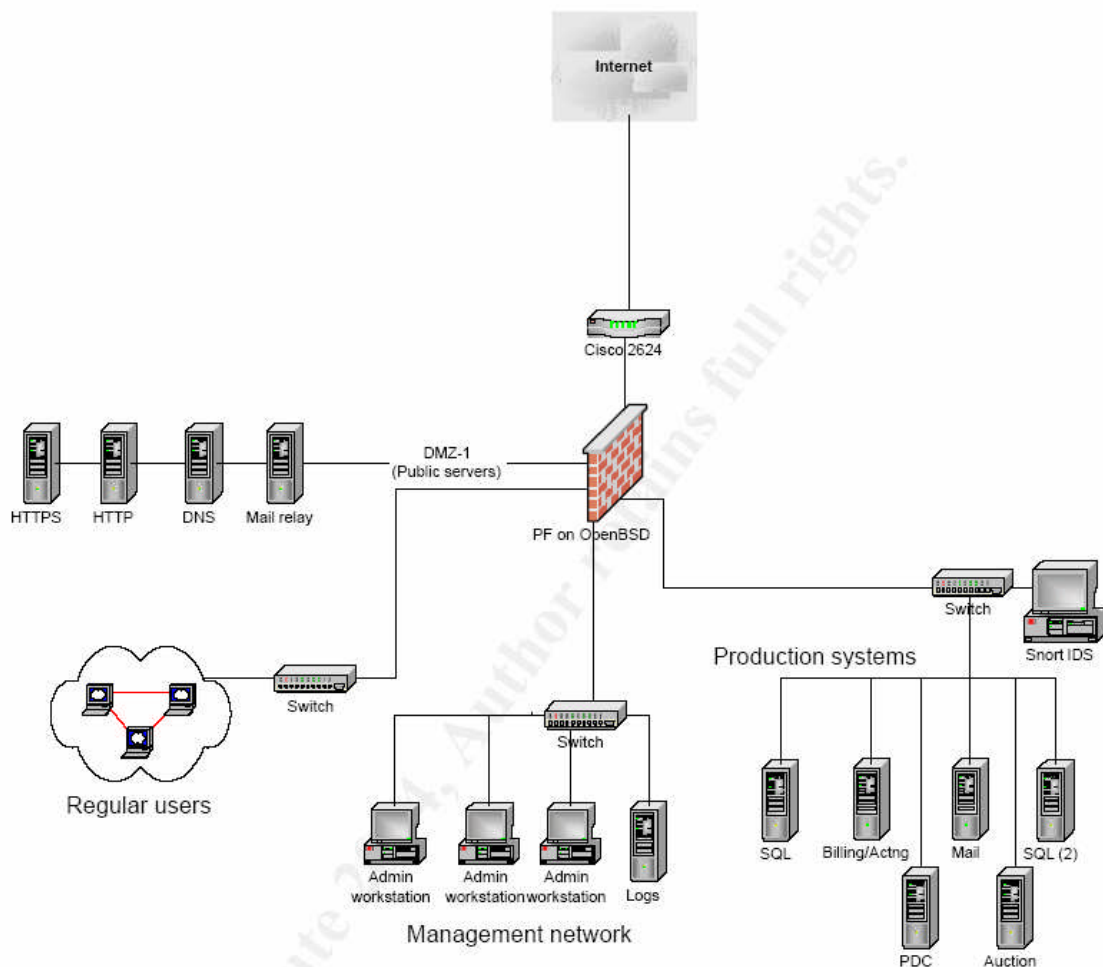
Firewall policy and management is the key component to security in the GIAC DMZ. Care was taken to harden the OS and the general firewall properties, however certain holes had to be opened up to provide customer and employee access. The use of VIPs for inbound traffic consistently proves to be a protection point for bastion hosts. Outside real ip addresses of servers are not available for probing. This is shown in the secure web, non-secure web and mail relay farms. Inbound and outbound traffic limited to necessary services and ports. Client to site VPNs utilize the same VIP functionality as seen elsewhere, and through the use of SecureClient software, VPN desktops are locked down to protect internal resources.

Assignment 3 – Design Under Fire

For the purpose of completing the Design Under Fire scenario, the following GCFW Practical has been chosen:

http://www.giac.org/practical/GCFW/Micho_Schumann_GCFW.pdf

The submitted network diagram for GAE is as follows:



Overview

Mario Giac inherited a portion of the paranoia exhibited by the older members of his family. Realizing that competition in the business world was heating up, and many of the GIAC Competitors already had on-line services, he felt extremely threatened. In addition, the SANS conference that Mario attended not only brought to life the need for internet operations, it also opened up his eyes to the dangers and pitfalls of doing business in that arena.

While at the SANS conference, Mario spent a good deal of time with a number of students who attended Track 4, *Hacker Techniques, Exploits and Incident Handling*. Through his discussions with those students, he struck up a friendship with an unnamed engineer we will call "Al." (Al wishes to have his name remain anonymous.)

Mario hired Al to find out information about GIAC's competitors. Specifically, a company called GAE had come in to the marketplace recently and made great strides in building market share. GAE was headed by a former GIAC employee who left on unsettled terms. Mario remained suspicious of the former executive. Although knowing it was completely illegal, Mario contracted Al to move forward with the project.

Reconnaissance

Mario already knew certain information about GAE's online presence since the industry was fairly small with only a few major players. The location of the corporate headquarters along with the major players in the sales force were among the known pieces of information of GAE. Al, posing as a potential customer, contacted the sales personnel in attempts to gain information. Sales people generally do not have extensive technical knowledge, however they are usually good sources of general information. In addition, they typically are not focused on the security of their internet systems – rather they are focused on generating revenue and building a customer base.

Citing GIAC's history of inefficient business practices, Al quickly developed a good rapport with the sales person. The sales person freely explained how efficient and cost effective their DMZ installation was. Having just completed their IPO, this was an important factor in the design for investor approval. The sales person also bragged that he had 100% access to the network and all of his applications anytime, anywhere. This allowed him to provide customer service far and above what his competitors could offer. The sales person continued to explain how their supply chain processes were streamlined and integrated into their sales systems to provide products quickly to their customers. Al asked the salesperson to demonstrate the functionality which was met with little resistance. Al was able to see the VPN client as well as the VPN endpoint. Finally, the sales person eagerly provided Al with a link and test login to the GAE secure site so he could get an idea of how they did business.

Al thanked the sales person for his time. He left the meeting, then reviewed his notes. From this basic piece of social engineering, he was able to determine the following: The DMZ implementation was cost effective - In the network security world there are realistically two kinds of products: free/cheap or expensive/corporate. If the DMZ implementation was inexpensive, then chances are the products were of the free/cheap category. This would mean that servers and devices were probably running some Linux or OpenBSD flavor of operating system on x86 type hardware. Sun Sparc or Opteron based systems are typically very expensive to purchase and maintain and are likely not used.

The DMZ implementation was efficient – Efficient implementations are generally small and make use of existing systems to provide services. Typically, the internal LAN is extended somewhat to the DMZ areas and locked down. Internal LAN operations typically revolve around Microsoft Operating Systems. Again, Microsoft OS runs on x86 platform hardware which is less expensive than Sparc or AIX based hardware. Also, Windows 2003 is really not largely deployed. Chances are there could potentially be Windows 2000 servers in the DMZ area.

The sales person had 100% access – One hundred percent access from anywhere means some sort of remote access. Cost effectiveness and efficiency would not lend itself to dial-up RAS pools, but some sort of VPN implementation. Also, support for desktop protocols and ports would be required upon setup of the VPN connection. This would lead to either a Citrix/ICA type connection and/or some form of Microsoft network access structure.

The VPN client is freeware using standard IPSec to 10.100.10.1. OpenBSD is commonly used with the PGP Client and is the likely operating system of the firewall/VPN Endpoint. PF is a common firewall technology used on OpenBSD.

There was a test account on the secure server – Al had access to the encrypted SSL portion of the web server. This would allow him to test the functionality of the servers themselves and fingerprint the behavior. Also, by having the URL of the customer website, he could determine through NSLOOKUP the hosting ip address and potentially the physical location.

Planning the Attack

Armed with his notes from his conversation with the sales person, Al decided to craft an attack plan. Al began with the domain name. Al searched through Domain Registrations and found the ip address of the authoritative name server. He learned the authoritative name server and the hosting ip address were in the same general network range of 10.10.1.X. He did not know the mask information to determine how the space was used, so he decided to look it up. He connected to:

<http://ops.sprint-canada.net/>

Address <http://ops.sprint-canada.net/>

About Sprint Canada | Careers | Contact Us

Choose a Route Server

Sprint RS (Toronto)

enter your Query

24.74.121.100

Choose a Query Type

☒ bgp

☐ bgp summary

☐ dampened-paths

☐ flap-statistics

☐ ping

☐ traceroute

Action

run the query (graphical view)

Sprint results returned from [Sprint RS (Toronto)]

Query: **show ip bgp 24.74.121.100**

BGP routing table entry for 24.74.64.0/18, version 22756900

Paths: (2 available, **best #1**)

Advertised to non peer-group peers:

64.235.244.128 128.223.60.102 128.223.60.103

3602 1239 1668 11426

204.50.223.11 (metric 101) from 204.50.223.11 (204.50.223.11)

Origin IGP, localpref 100, valid, external, **best**, multipath

Community: 1239:321 1239:1000 1239:1004 **3602**:123 **3602**:1239 **3602**:2000 **3602**:2002

3602 1239 1668 11426

204.50.223.10 (metric 101) from 204.50.223.10 (204.50.223.10)

Origin IGP, localpref 100, valid, external, multipath

Community: 1239:321 1239:1000 1239:1004 **3602**:123 **3602**:1239 **3602**:2000 **3602**:2002

This is the Sprint looking glass server that will show how BGP routes are laid out for various networks. An example is shown using a common cable modem address as follows in Figure 22. Since the company is based in Canada, the best chance to find good routes would be on a large Canadian ISP looking glass. From the output of the search information about how the network is divided can be determined. The first line in the returned query shows the BGP entry. In the case of GAE, a /24 mask was returned. Typically, if an ISP hosts a block of addresses, it will summarize on a bit-count much higher than 24. The cable modem range used in the example underscores this as a /18 was returned. AI can reasonably determine that GAE owns the /24 and is advertising the range out of their point-of-presence.

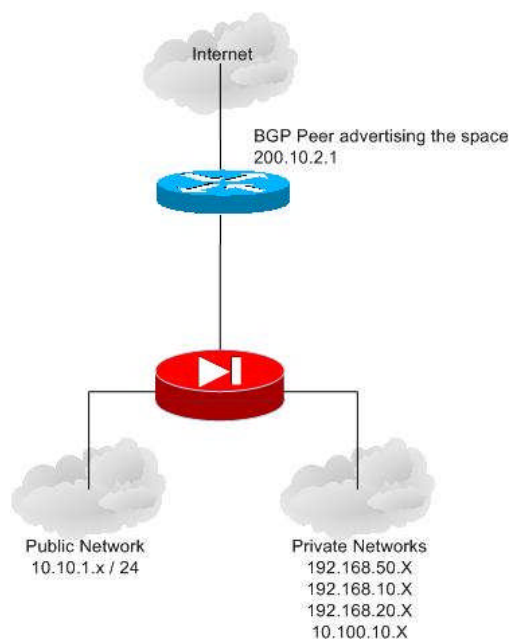
Figure 22 : Canada Looking Glass

Having the IP range gives AI a place to start. The next step is to determine what might be in the DMZ hosted on that DNS server. To do this, AI performed lookups using the GAE DNS server as his authority. This is accomplished with the following command:

```
C:>nslookup server=10.10.1.100
```

He attempted a zone transfer from the server and was unsuccessful. He then proceeded to do reverse-lookups on every address in the range. The reverse lookups returned server and workstation names of the entire corporate network – including the DMZ. The reverse lookup information gave him insight to the ip addressing scheme in use. The following IP address ranges were returned:

- 192.168.50.X
- 192.168.10.X
- 192.168.20.X
- 10.10.1.X (Public Space for the use of this example as described the author)



Based on the information returned from the BGP trace and the DNS Reverse lookups, AI could determine the a basic map of what the network probably looks like. The BGP peer advertising the address space is the external interface of the network router. When tracing to the registered address, the last hop returned is that address: 200.10.2.1. Requests time out after that hop. More than likely, a firewalling device protecting the internal networks lies directly behind that hop. At this point it can be determined that the firewall device has at least three interfaces:

- an interface connected to the border BGP router
- an interface connected to the public lan
- an interface connected to the private subnets (either one interface connected to a router, or one interface per subnet)

DNS records are typically non-cryptic and easy to interpret. Based on DNS entries, AI also determined that GAE had the following devices:

multiple SQL servers

- a mail server
- a secure web server
- a non-secure web server
- a mail relay
- an IDS
- a log server
- Microsoft authentication servers (Domain Controllers)
- A terminal server

Attacking the Network

AI started with the easiest access which was his test account to the GAE system. Once connected, he tried various changes to the URLs to see what was returned. In most cases he as kicked off by the web server for using different URLs. However, he was able to change the case of the requested URL pages and still return a response. Since Microsoft Web Servers are not case sensitive in most cases, this told AL that he was connected to a Microsoft Windows (IIS) based web server. AI could also reasonably assume that all other web servers were Microsoft as well. At this point we now know we have a company with Microsoft Web Servers and Microsoft Domain Controllers. Users have 100% access to the network at all times, including all their applications. There is also a Microsoft Terminal Server on the network. This Microsoft centric approach leads AI to also determine the SQL and Mail Servers are more than likely Windows Based as well.

Al decided first to attack the edge router. Based on GAE's size, he made the assumption that Cisco networking products were used. They are the most common and the easiest to support. He also knew that it was providing BGP peering through his Sprint lookup.

On April 29, 2004 Cisco released the following updated security bulletin:

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>

It describes how TCP resets could be used to DOS a Cisco router. The confidentiality and integrity of the router itself is not compromised, but a DOS condition will exist. BGP is the most susceptible protocol. Since BGP is not auto-updating, this is not really a major issue. However, it is possible to send BGP resets to the router. Al decided to spoof packets from the ISP's BGP peer to the external interface in accordance with the advisory. By doing this, as explained in the advisory, he could isolate the GAE network for a period of time. If the condition holds true, then Al would know that the border router was a Cisco branded product. Mario was particularly thrilled with this attack as it took down the GAE network completely for a time. In order to craft the packets, Al used a tool called hping. Some good references for hping are:

<http://www.hping.org/manpage.html>

The actual hping command would look similar to the following:

```
Hping -c 1000000 --fast -a <isp BGP Peer> -p 179 -R 200.10.2.1
```

- -c / specifies how many packets to send
- --fast / rapidly send packets to flood the host
- -a / sets the source of the packet to the ISP BGP peer to GAE
- -p / sets the protocol used to 179-BGP (2605 can also be used as it is a port used for BGP as well)
- -R / sets the Reset flag in the packet. This is vulnerability
- 200.10.2.1 / is the destination (the GAE Border Router)

Next Al used Firewalk to determine what ports were open on the firewall. The following white paper explains a bit about how it works:

<http://www.packetfactory.net/projects/firewalk/firewalk-final.pdf>

As described in the white paper, two pieces of information are required:

- the ip address of the last known gateway before the firewalling takes place
- an ip address of a host behind the firewall

AI knows both of those addresses based on his reconnaissance. Firewalking sends crafted packets with a TTL + 1 of the destination over a given port. If the ports are open and the traffic passes, it will die on the wire and receive a return response of `TTL Exceeded in Transit`. If the port is not open, the firewall should drop the packet and no response will be given. If any of the destination addresses are NAT addresses, or if they are proxied, no response will be given. However, since responses were sent back on the open ports (DNS, HTTP, HTTPS and SMTP) AI determined the firewall device is not doing NAT or Proxy functions to the public subnet.

To complete the scan, the Firewalk command would look like the following:

```
Host#firewalk -n -P 100 -S1-1024 -pTCP 10.10.1.1 10.10.1.253
```

- -n / turns off address resolution
- -P / specifies a network writing pause to avoid congestion and possible detection
- -S / specifies the destination ports in the scan
- -p / dictates only TCP should be used
- 10.10.1.1 10.10.1.253 / address range to scan (we learned this earlier)

Firewalk has two phases: network discovery and network mapping. The discovery phase determines the number of hops to the firewall device and the last hop address. The mapping phase shows which ports are open. The output will look like the following:

```
Firewalking through 10.10.1.1 (towards 10.10.1.254) with a
maximum of "XX" hops.
```

```
Ramping up hopcounts to binding host...
```

```
probe: 1 TTL: 1 port 33434: <response from> [10.10.1.1]
probe: 2 TTL: 2 port 33434: <response from> [10.10.1.2]
Probe: 3 TTL: 3 port 33434: <response from> [10.10.1.3]
probe: 4 TTL: 4 port 33434: <response from> [10.10.1.4]
probe: 5 TTL: 5 port 33434: Bound scan: 5 hops <Gateway at 5
hops> [10.10.1.5]
```

```
port 1: *
port 2: *
port 3: *
port 4: *
```

Etc through the range. Open ports would look like the following:

```
port 25: open
port 53: open
port 80: open
port 443: open
```

```
XXX packets sent, XXX replies received
```

Attacks can then be crafted based on destination ports opened.

The firewall seemed to be locked down pretty well, as was the web server. Al easily mapped the network, however he was not yet able to compromise a box. He finally decided to exploit a known issue with Distributed Web Authoring in IIS. Microsoft released a security bulletin as follows:

<http://www.microsoft.com/technet/security/bulletin/ms03-007.msp>

However, attempts failed since the web server was locked down the Microsoft IIS Lockdown tool.

Al reported his findings back to Mario who was somewhat disappointed. However, since the Denial of Service attack was successful, it wasn't a complete loss.

Assignment 4 – Work Procedure

GIAC places great emphasis on their attempts to grow their business through their new Internet presence. The modular approach to the DMZ design reflects the potential future need to grow the business and potentially build out new sites. Physical site growth also means employee growth. As such, GIAC has requested a work procedure to detail the build of a Web Firewall. This entire process should be completed on an isolated network.

Nokia IP 530

The Nokia IP platform will ship with any number of different IPSO images. In order to maintain a consistent state across the enterprise, the IPSO needs to be upgraded first. The difficulty in doing that is two fold. First the IP 530 does not have a floppy drive or CDROM on it. Second, it comes shipped completely stripped of any network configurations.

Begin by using the console cable provided by Nokia. This is important because the Nokia console cable is unique to Nokia. Although it is a DB-9 to DB-9 cable, its pinouts are different than other manufacturers. A Cisco Systems cable or Foundry Networks console cable will not work. Set your virtual terminal software to the standard settings of 8 data-bits, no parity and 1 stop bit. The baud rate is 9600. Out of the box, log on locally as username admin and password admin.

Once connected, the easiest way to configure the box is to use Voyager. However, you need network connectivity for that to work. This is easily setup and well worth the few extra minutes it might take. From the console prompt, type the command, "lynx" and hit enter. You will be prompted for a username and password. Use the same password as the console.

In Lynx, a text based representation of the web configuration is given. Use the TAB key to move forward, Shift-Tab to move back. The enter key selects a radio button. Use the back arrow key to move up one level in the menu tree. The idea from lynx is to configure one Ethernet interface, then connect to that interface using a PC or laptop and a crossover cable. This will enable us to use the graphical setup, as well as ftp standard packages to the box.

At the main Lynx screen, Config is already highlighted. Tab to INTERFACES, and hit enter to select. This will bring up the interfaces physically installed on the Nokia. In order to enable interfaces, they must be enabled in two places: physical and logical. Tab to "eth-s1p1" and hit enter. This is the first built-in interface on the appliance. Identifiers for the text radio buttons are to the right of the selection point. This can look confusing. Tab to "on" for eth-s1p1 and hit enter. Then tab to the mac address on text radio button and hit enter. This will configure the physical interface up. These changes

must be saved before they will function. Tab to [applybutton.gif] and hit enter. After the change is applied, the save button will be available. Tab to it and hit enter. The physical interface is now on.

Next we need to configure the logical settings. Tab to UP and hit enter to move to back to the interfaces page. Then tab to eth-s1p1c0 and hit enter. Tab to active and hit enter. Then tab down to the ip address and enter an ip. Its best to enter the ip address this interface will have when its deployed to save yourself the hassle later. Input the appropriate bit length in the mask field. Tab to apply, then save. Configure your laptop or PC with an IP address on the same subnet, then connect a crossover cable from your Ethernet port to the interface. Open up a web-browser and type, <http://<ip-address-of-Nokia/>> to bring up the Voyager web interface. Figure 12 shows you the main configuration screen.

The first steps are to get the appropriate files copied to the Nokia. Start up an FTP server on your desktop. Enter the config page, then select Install New IPSO Image under the System Configuration section of the page. Enter the location of the image as an FTP command next to "Enter URL to image location" in the text box. This will copy the new image to the appropriate directory. Next, select "UP", then Mange IPSO Images from the same section. A listing of the available images is now present. Select the radio button next to the one you installed under the "Select image for next boot" section. Select Apply, then save. Reboot the Nokia. After the box reboots, reenter Voyager.

Now we are ready to install the appropriate Checkpoint Firewall 1 version. Select "Manage Installed Packages", then select "FTP and install packages." A similar FTP screen is shown as the IPSO screen. Select your FTP server location once again and upload the image. Once completed, it will show in the lower right hand selection box. Select it, then click apply. This will unpack your file. Return to the Manage Installed Packages page. Select the radio buttons for the Firewall-1 packages you just unpacked and deselect the old packages. Click apply, then save. Reboot the Nokia. Reenter Voyager and go to the Mange Installed Packages and delete off the old unused packages. Do the same for the IPSO images. The box is now ready for configuration.

Using Voyager, harden the Nokia installation the same as previously discussed. Leave Voyager access on for now. Obtain the usernames and passwords to be configured from your team lead or manager. Configure the interface IP addresses based on the diagram you were given using your Voyager connection. Other than the interface you are using to connect to Voyager, leave the interfaces off.

Return to your console prompt and login. From a command line run the command, "cpconfig" to install the security policy and configure Firewall-1. Use the default settings and do not enter a license when prompted. Licenses are centrally managed and will be discussed later. You will be prompted for an authorization key. The key is specific to the firewall. Be sure to keep the key in a safe place. It will be used later when the box is installed. Upon completion of the checkpoint configuration tool, reboot the Nokia

once more. Log in via console and return to the Lynx text based configuration tool. Turn off Voyager access and turn off the interface you were using to configure the box. Exit voyager and type halt. This will gracefully shutdown the box. The box is now ready to be racked.

Be sure when the box is racked and cabled that a console cable is run to the Cisco ASR at the site where it will be implemented. When the box boots up, it will have the default security policy of “any/any – drop” meaning you will not be able to access it from the network. You will need the console access from the ASR to complete the installation.

Checkpoint Firewall-1 Management

The appliance is now racked and ready for implementation. All the interfaces are off and a default policy blocking all traffic is installed. From your desk in the GIAC admin network, SSH to the Cisco ASR. Login using your credentials and SecurID. From the ASR you will reverse telnet to the console of the Nokia appliance. For instance, if the box were deployed in the corporate headquarters and connected to port 35 on the asr, the command from the ASR would be:

```
telnet 172.18.11.125 2035
```

In this scenario, telnet is not a bad thing. This is a physical connection to the console of the box and the telnet traffic never traverses the network. From your reverse telnet session to the console, log into the firewall. Type the command:

```
Fw unloadlocal
```

This command will remove the security policy effectively turning the firewall into a router. All the interfaces are still off. Using Lynx, browse to the Interface Configuration and turn on the bottom side interface pointing down into the network where the firewall will be managed from. This should be the ONLY interface turned on.

From your desktop, open up a Windows Remote Desktop connection to one of the terminal servers in the administration network and log in. Only the terminal servers have GUI client access to the Checkpoint MDS Provider 1 management implementation. Traffic must be sourced from the terminal server to Provider 1. Once logged in connect to Provider 1 using the GUI shortcut. It is now necessary to add the firewall module to Provider 1 for management.

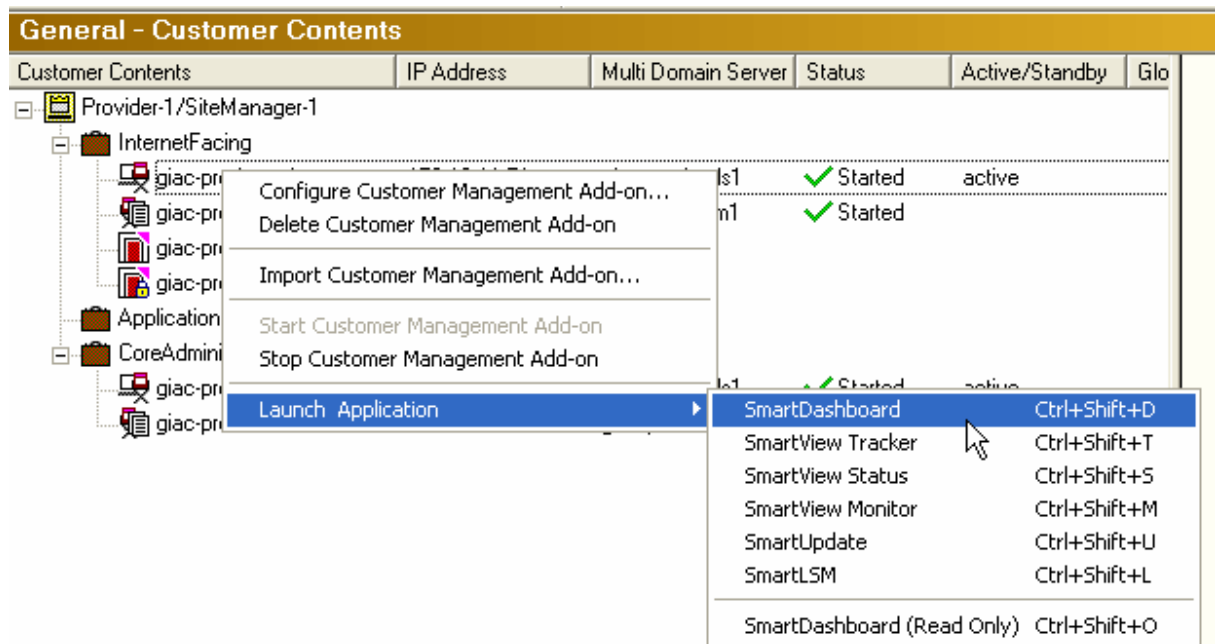


Figure 23 : MDS GUI to launch the CMA

Right click on `giac-prod-cma1`. This is the CMA that houses all internet facing firewall modules. Select **Launch Application**, the **Smart Dashboard**. This is the GUI application for policy development. Once the application is opened, right click on **CheckPoint** under **Network Objects**. Select **New Checkpoint -> Gateway**.

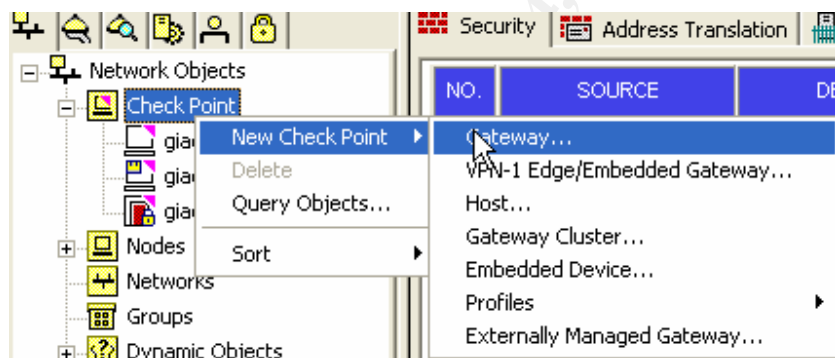
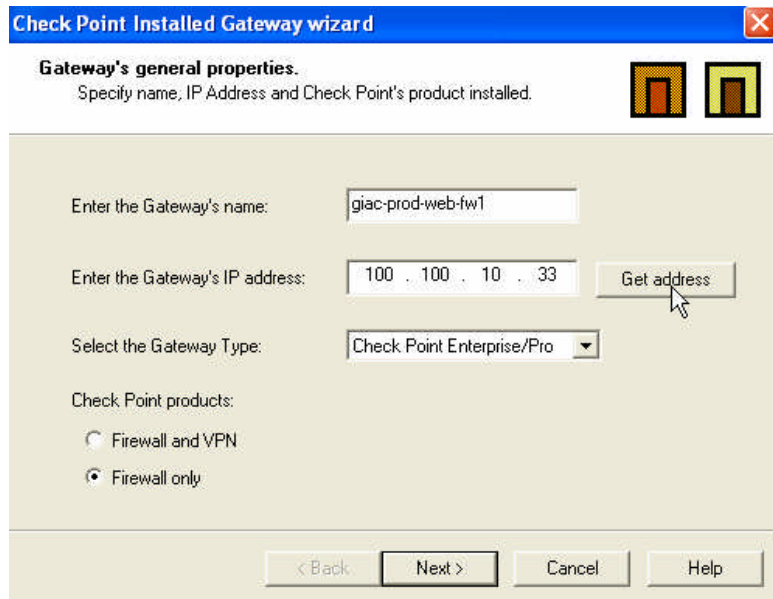


Figure 24 : Creating a new Gateway

Select **Simple Mode**, then **OK**. Enter the host name of the firewall, then select **get address**.



Check Point Installed Gateway wizard

Gateway's general properties.
Specify name, IP Address and Check Point's product installed.

Enter the Gateway's name:

Enter the Gateway's IP address:

Select the Gateway Type:

Check Point products:

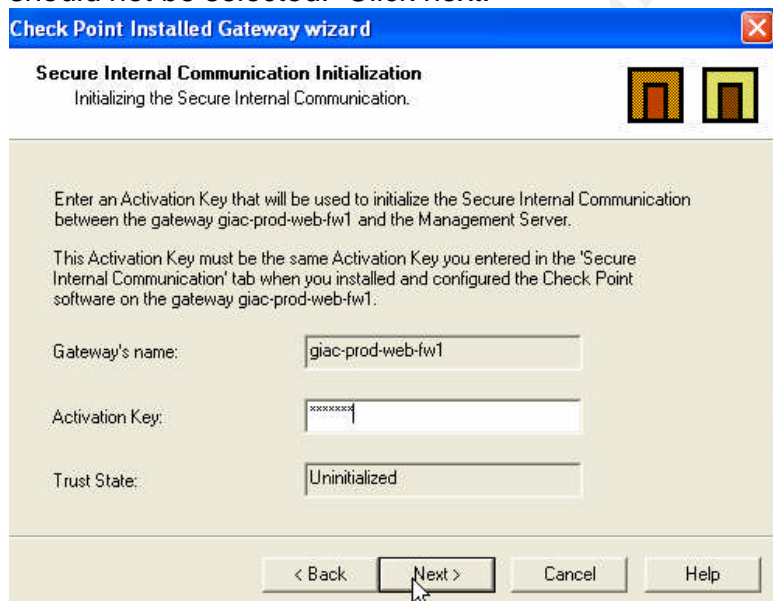
☐ Firewall and VPN

☒ Firewall only

< Back Next > Cancel Help

Figure 25 : Specifying the gateway and products

Provider 1 will do a DNS lookup on the firewall and resolve the name. As this is a web services firewall, make sure that Firewall 1 only is selected. The VPN component should not be selected. Click next.



Check Point Installed Gateway wizard

Secure Internal Communication Initialization
Initializing the Secure Internal Communication.

Enter an Activation Key that will be used to initialize the Secure Internal Communication between the gateway `giac-prod-web-fw1` and the Management Server.

This Activation Key must be the same Activation Key you entered in the 'Secure Internal Communication' tab when you installed and configured the Check Point software on the gateway `giac-prod-web-fw1`.

Gateway's name:

Activation Key:

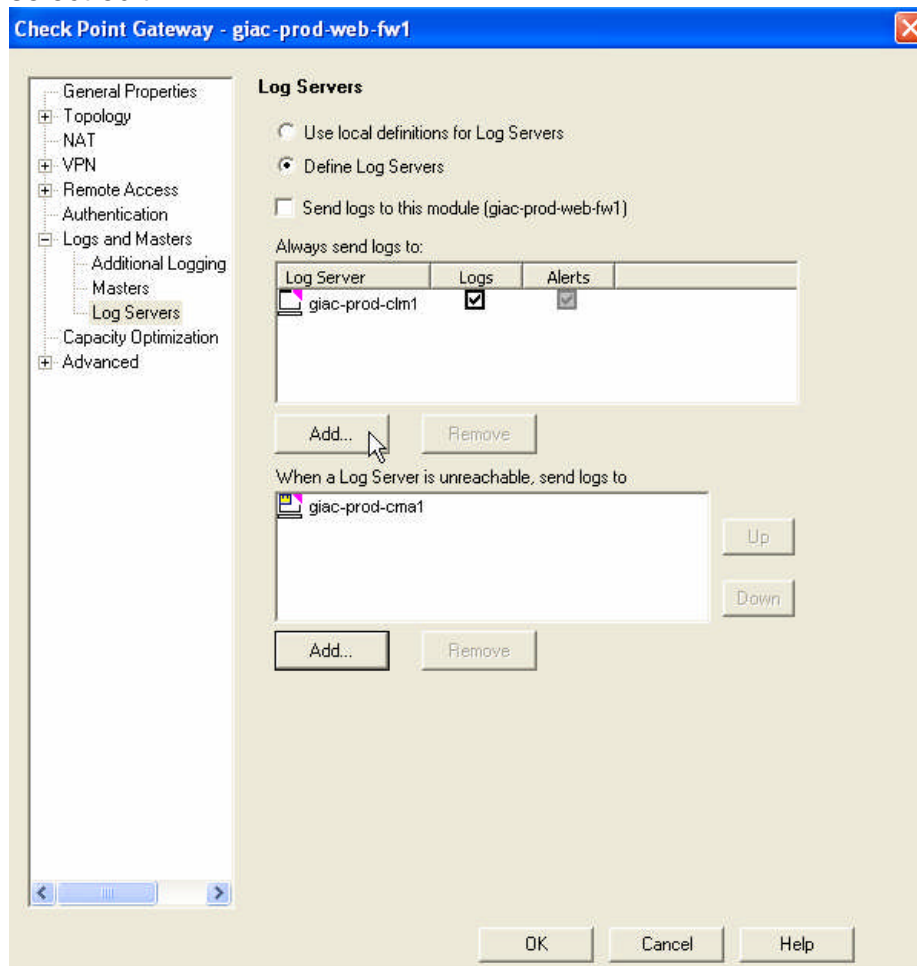
Trust State:

< Back Next > Cancel Help

Figure 26 : SIC Setup

SIC is the process that Checkpoint uses to secure communication from the management server to the firewall module. The key you entered during the Nokia configuration is now necessary. Enter the key in the dialogue box, then select continue. The management server will attempt to contact the firewall module and establish secure communications. Complete the interface configurations of the Firewall object in accordance with the guidelines laid out during the hardening section of this document.

The final configuration of the firewall module is the log location. This is set on the properties dialogue box for the firewall object. Right click on the firewall object, then select edit.



Firewalls in the GIAC implementation using the CLM to capture log traffic that is assigned to the CMA in the Provider 1 gui. Expand Logs and Masters then select Log Servers. Under “Always send logs to” click Add... then specify the CLM. Click ok. Under “When a Log Server is unreachable, send logs to” click Add... then specify the CMA. This sets up a process whereby the firewall module logs to the CLM and will forward logs to the CMA only when the CLM is unavailable.

Web Firewall Rule Creation

The Firewall 1 rule base is comprised of objects. Rules either allow or deny traffic to objects based on allowed IP ports. Objects can be networks, hosts, address ranges, users or any other network accessible function. The web firewall network only requires two objects:

1. Virtual IP address for the secure site

2. Virtual IP address for the non-secure site

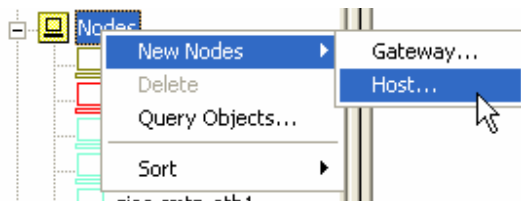


Figure 27 : Adding an Object

From the objects view on the left of the CMA screen, select Nodes -> New Nodes -> Host. Enter the name of the host along with the IP address associated with it. For the secure site, the name would be "customer.giac.com" with an IP address of 100.100.10.37. Create a second object for the non-secure site in the same manner using www.giac.com as the name with an ip address of 100.100.10.5.

Now that our objects are created, we can begin to create a rule base from within SmartDashboard. The first two rules that are created are the stealth rule and the cleanup rule. No connections made directly to the firewall other than SSH should be allowed. Also, any traffic not explicitly allowed should be denied. This was discussed earlier.

From our basic set of rules, add a new rule:

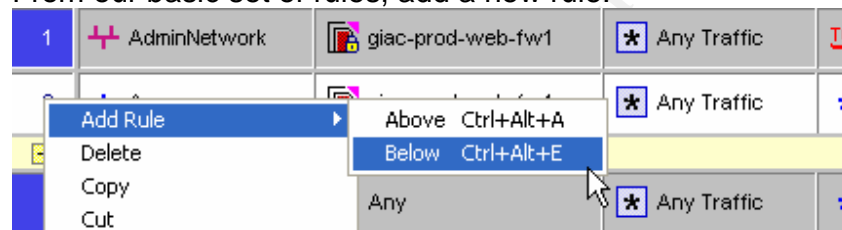


Figure 28 : New Rule

We will add two rules, one for each site. You can drag objects from the tree into the rule for quick installation. Left click on the object you want to add, and drag it into the destination.

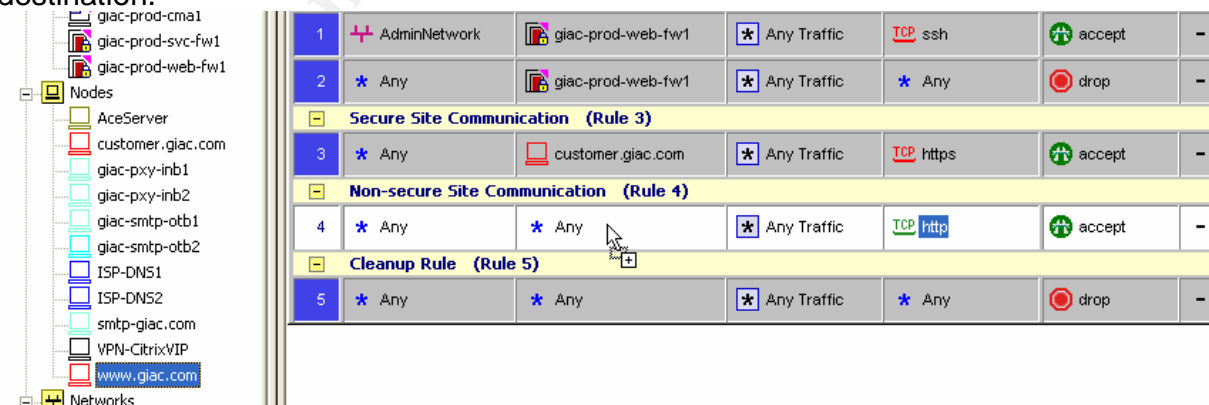


Figure 29 : Dragging Objects to a Rule

The rule base for the web firewalls is now complete. The full rule base is as follows:

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Stealth Rule (Rules 1-2)									
1	AdminNetwork	giac-prod-web-fw1	Any Traffic	ssh	accept	None	giac-prod-web-fw1	Any	SSH to the firewall
2	Any	giac-prod-web-fw1	Any Traffic	Any	drop	None	giac-prod-web-fw1	Any	Stealth Rule
Secure Site Communication (Rule 3)									
3	Any	customer.giac.com	Any Traffic	https	accept	None	Policy Targets	Any	Secure Traffic
Non-secure Site Communication (Rule 4)									
4	Any	www.giac.com	Any Traffic	http	accept	None	Policy Targets	Any	Non-Secure Traffic
Cleanup Rule (Rule 5)									
5	Any	Any	Any Traffic	Any	drop	None	giac-prod-web-fw1	Any	Cleanup Rule

Figure 30 : Web Firewall Rule Base

The final step in completing the policy implementation is to “push” or install the policy out to the target. Select Policy from the menu, then install.

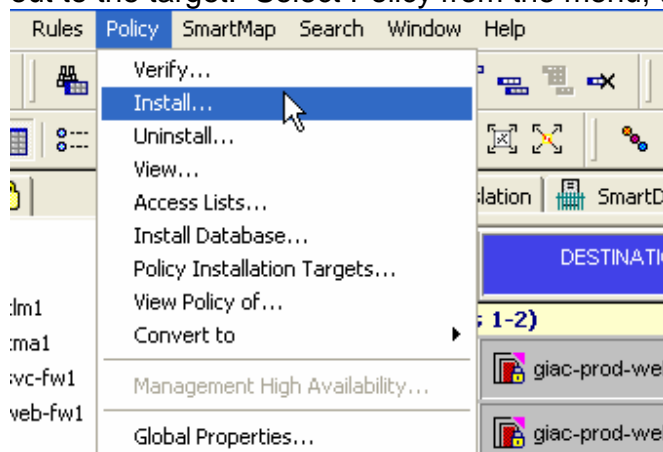


Figure 31 : Install a New Policy

A very common mistake is made at this point when managing multiple firewalls from the same management station. All managed firewalls will show up as targets. However, if you install the wrong policy to a firewall, you will more than likely disable services on that firewall and cause an outage. Take care to install the policy to the correct firewalls and deselect any firewalls where the policy doesn't belong.

In addition, Checkpoint has a featured called “Create Database Version” via a checkbox on the bottom of the installation dialogue. It is GIAC corporate standard to use this box to maintain a history of policy changes. Click OK and the policy will install to the firewall. Now that the firewall is completely setup and its security features are correctly configured, SSH to it and turn on all the interfaces.

The web firewall setup is complete.

Appendix A - Bibliography

- Benjamin, Henry. *CCIE Self-Study: CCIE Security Exam Certification Guide*. Indianapolis: Cisco Press, 2003.
- Carasik-Hemni, Anne, ed., Robert J. Shimonksi, Debra Littlejohn Shinder and Dr. Thomas W. Shinder. *Best Damn Firewall Book Period*. Rockland, Maryland: Syngress, 2003.
- Doraswamy, Naganand, and Dan Harkins. *IPSEC: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, Second Edition. Upper Saddle River, NJ: Prentice Hall PTR, 2003.
- Hunt, Craig. *TCP/IP Network Administration*. Sebastopol, California: O'Reilly & Associates, 1998.
- Koziol, Jack. *Intrusion Detection with Snort*. Indianapolis: Sams Publishing, 2003.
- Krutz, Ronald L., and Russell Dean Vines. *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*. New York: Wiley Computer Publishing, 2001.
- Leveille, Valerie, and Sarvang Shah. *CCSE NG: Check Point Certified Security Expert Study Guide*. Alameda, California: SYBEX, Inc., 2003.
- Marcell, Albert J., and Robert S. Greenfield, eds. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Boca Raton: Auerback Publications, 2002.
- McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions, Fourth Edition*. Berkeley: McGraw-Hill/Osbourne, 2003.
- Menga, Justin. *CCSA NG: Check Point Certified Security Administrator Study Guide*. Alameda, California: SYBEX, Inc., 2003.
- Northcut, Stephen, et al., *Inside Network Perimeter Security*. Indianapolis: New Riders, 2003.
- Shimonksi, Robert J., ed, Will Schmied, Dr. Thomas W. Shinder, Victor Chang, Drew Simonis and Damiano Imperatore. *Building DMZs for Enterprise Networks*. Rockland, Maryland: Syngress, 2003.
- Tobkin, Chris. *Check Point NG/AI*. Rockland, Maryland: Syngress, 2004.
- Welch-Abernathy, Dameon D. *Essential Check Point FireWall-1 NG*. Boston: Pearson Education, 2004.