Global Information Assurance Certification Paper

GIAC Training and Certification
SANS 2001 New Orleans
GCFW Practical
Version 1.5d
Matthew P. Brown
May 2001

Assignment 1 - Security Architecture

GIAC Enterprises is a growing Internet startup that is expecting to earn $200 million per year in the sales of online fortune cookie sayings. GIAC has two main goals for its security architecture: to ensure communication and provide access. Ensuring communication applies to the administrative staff and their being able to manage all of GIAC's resources. Providing access falls to four groups of people, the international partners, the suppliers, the customers, and the remote home office staff. In providing access, GIAC will focus on the three pillars of security: confidentiality, integrity, and availability. It is often said that the most secure computer is the one that is not plugged in. By engaging in online commerce GIAC is opening itself up to many possible security risks and it is the goal of the administrative staff to mitigate these risks.

GIAC Enterprises' international partner is a company called WiseMan Inc. who will translate and resell the fortune sayings overseas. It was required in a merger agreement that WiseMan purchase and maintain the same configuration on a commercial VPN (virtual private network) solution. All that is required of GIAC is to provide a means for WiseMan to retrieve the fortunes, which can be accomplished through an https download.

GIAC will also have staff working from home or while out of town on business. Remote staff will access the same VPN appliance, mentioned above, from a local Internet Service Provider (ISP) on their GIAC laptops. These laptops will have a standard image containing a leading commercial virus. The staff remote users who connect via the VPN will first pass through the firewall on their way to the VPN appliance where the traffic will only be logged. Then from inside the designated network, the remote staff will pass back through the firewall to access any resources for which they are allowed. The configuration on the VPN and the traffic logs will be closely monitored for this is seen as one of GIAC's biggest potential security risks.

Both suppliers and customers of GIAC will be connecting to a web server where they can browse and purchase online fortunes. All purchases will be done over secure sockets layer (ssl) encryption, also know as https. Both the suppliers and customers will also have the option to email GIAC Enterprises for various reasons.

GIAC's network will be subdivided into four pieces:

- The Perimeter network
- The Services network

- The Partners' network
- The Internal network

Only the Perimeter network will be use public IP addressing while the other networks will use RFC 1918 compliant internal IP addressing.

The following are descriptions of the key elements in GIAC Enterprises' security architecture pictured in Figure1:

CISCO ROUTER

GIAC's border router will be a Cisco 3620, which will provide connectivity from the Internet to the local systems. The 3620 will employ some filtering or screening but will not duplicate the actions of the firewall. By filtering, we mean that the router will prevent malicious or unwanted traffic from ever reaching the firewall. To accomplish this the router will block all source addresses that are deemed "illegal" in the sense that they are not, not should they be, expected. We will go into this in more detail later. This is done to take some of the load off the firewall and to add another layer to our security. We have no expectation of eliminating all threats, but through defense in depth, we do hope to reduce risk as much as possible, and the router is the first piece.

CHECKPOINT FIREWALL-1

The centerpiece of our security architecture is our Checkpoint Firewall-1 running on the Nokia IP650. As with most firewalls you must keep the patch level current or you could leave yourself open to intrusions. The current version is 4.1 with service pack 3. We see the firewall as the main gate to our castle we call GIAC Enterprises and have decided to invest in it. The decision was made to purchase the Nokia appliance with the integrated Firewall-1. Using the Nokia IP 650 hardware/appliance solution for our firewall will help us to avoid the task of hardening the base operating system as well as the firewall.

The remote staff and our international partners will be connecting through the firewall to the VPN appliance for access. Since the firewall will be the main filtering device for GIAC's network, it must be robust enough to handle the load that will be put upon it. To further support our structure we have implemented dual firewalls for redundancy, to assure the availability and integrity of the company.

NORTEL CONTIVITY

Nortel's Contivity 2600 is a software/hardware combination that provides virtual private networking for remote users connecting to the home network. We have chosen to put the VPN in front of the firewall versus the popular idea of putting it beside (or behind) the firewall. We realize that this will put an increased load on the firewall, but we feel that the benefit of having the VPN traffic pass through the firewall is worth it. The 2600 will provide remote users with access to the home network through a local Internet Service

Provider and will provide access for our international partners to have access certain areas of the network.

In the Contivity, you can use a local radius server to obtain an IP address from certain pools based on group authentication. Based on these IP addresses, remote staff or our international partners will gain access to specific resources. The remote staff, after coming through the VPN, will then pass back through the firewall to access the internal network. At this time, we are only using the local radius server on the Contivity and the local group authentication. It is recommended that another form of authentication be added (i.e., SecureID) to provide two-factor authentication to help secure the VPN access.

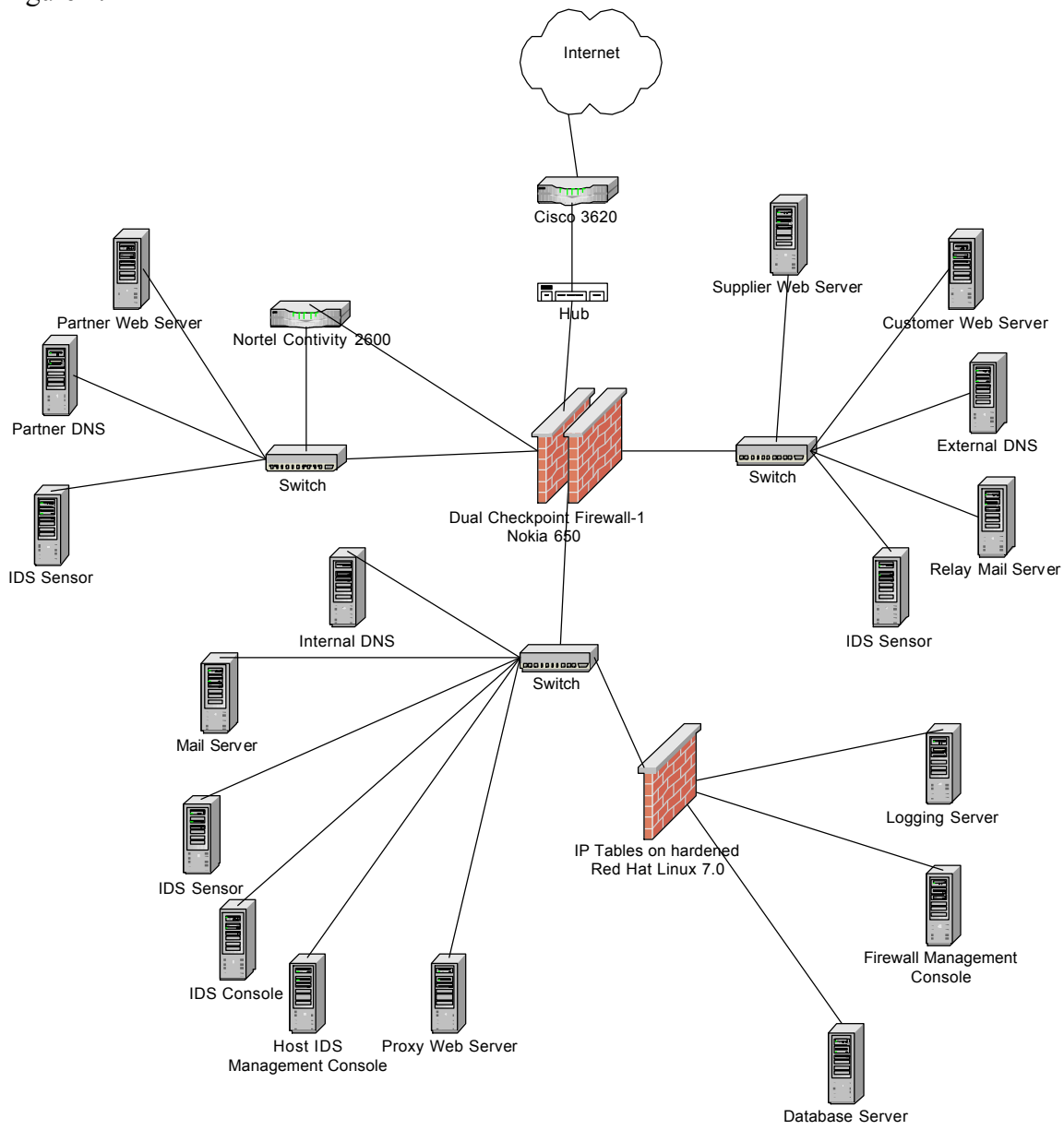
ISS REAL SECURE

We have chosen Internet Security Systems' Real Secure as our intrusion detection system. Network Sensors will be placed in all four of GIAC's networks to help monitor traffic, illegal and legal. Real Secure has a clean graphical user interface where policies can be customized and reports created. Each sensor will be running on Windows NT 4.0 and using ISS Real Secure 5.0.

IP-TABLES ON RED HAT LINUX 7.0

We feel that it is necessary to provide another layer of defense for certain servers that are considered essential for GIAC's business. The decision was made to go with Red Hat Linux's Ip Tables running on a hardened Red Hat 7.0 server operating system. The Ip Tables firewall will restrict access to the logging server, database servers, and the firewall management console. It is crucial that when you are going to have two different firewalls that you use two different vendors. It is also important to note that you do not use two vendors who have similar firewalls, such as Checkpoint's Firewall-1 and the Cisco Pix firewall.

Figure 1.



Addressing Scheme

GIAC Enterprises has been given the Class A address range of 115.50.25.0-115.50.25.255 and the external interface of the router has been given the address of 125.124.123.122. For the present situation, GIAC will use a 24-bit net mask for its external addresses. It is necessary to point out that this address scheme is arbitrary and relative only to this paper.

As mentioned previously, the GIAC network has been subdivided into four sections, the

perimeter network, the services network, the partners network, and the internal network. The perimeter network is where the internal interface of the router and the legal, external interface of the firewall lives and is often referred to as a DMZ. The services network is where the customers connect to purchase fortunes and where suppliers connect to supply fortunes. The partners network was designed to specifically meet the needs of our agreement with WiseMan Inc. Therefore, it contains only those resources explicitly needed to fulfill that agreement and it also contains the Nortel Contivity 2600. The internal network is where the rest of GIAC's resources are located. It should be noted that all four networks use a 24-bit netmask. The four networks were assigned address in accordance with RFC 1918 ("Address Allocation for Private Internets"), and the addresses are as follows:

Perimeter:	**115.50.25.0-115.50.25.255**
Cisco 3620:	125.124.123.122 (external interface)
	115.50.25.7 (internal interface)
Firewall-1:	115.50.25.14 (perimeter)
	172.16.1.19 (services network)
	192.168.1.9 (partners network)
	10.1.l.22 (internal network)
Services Network:	**172.16.1.0-172.16.1.255**
Supplier Web Server:	172.16.1.21
Customer Web Server:	172.16.1.22
External DNS:	172.16.1.23
Relay Mail Server:	172.16.1.24
Real Secure Sensor:	172.16.1.25
Partners Network:	**192.168.1.0-192.168.1.255**
Nortel Contivity 2600:	115.50.25.41 (external interface)
	192.168.1.4 (internal interface)
Partner Web Server:	192.168.1.5
Partner DNS:	192.168.1.6
Real Secure Sensor:	192.168.1.7
Internal Network:	**10.1.1.0-10.1.1.255**
Internal DNS:	10.1.1.2
Internal Mail Server:	10.1.1.3
Real Secure Sensor:	10.1.1.4
Real Secure Console:	10.1.1.5
Proxy Web Server:	10.1.1.6

IP-Tables Firewall:	10.1.1.17
Database Server:	10.1.1.7
Firewall Management Console:	10.1.1.8
Logging Server:	10.1.1.9

Assignment 2 – Security Policy

GIAC Enterprises security policy will be to deny everything except that which is explicitly permitted. Access will be permitted to allow basic business functions to be maintained, for users to have remote access, and for staff to be able to manage GIAC's resources. Access will be given to unauthenticated users coming from the Internet to provide them with the ability to purchase fortunes on the web server and send email responses/questions to GIAC.

GIAC is also outsourcing the writing of fortunes to suppliers who need the same resources as customers, but will be accessing a different web server. These suppliers will also be required to authenticate themselves in order to put fortunes onto the appropriate web server. We are considering using an encryption suck as PGP where we will exchange keys with suppliers so they can encrypt the fortunes before putting them on the server, but no such security is implemented at this time. Assuming the security is implemented, an email would be automatically sent to GIAC every time a supplier places fortunes on the server. GIAC would then be able to access the fortunes and decrypt them accordingly. For now, the fortunes are transmitted to the internal database server over sqlnet once they have been received.

Access will also be given to GIAC's international partner, WiseMan Inc., who, in a previous agreement, is required to accesses resources via the same Nortel Contivity 2600 that GIAC uses and with the same basic configuration settings.

This creates an interesting situation where one can ask the question, "who is actually using the VPN on the other end?" Due to this uncertainty it was decided to put the partners in their own network where all they will be able to do is obtain the fortunes that they will be translating and reselling. It is required that these users pass through the firewall so that the traffic will be logged, but all of the encryption/decryption will be taking place on the Nortel box.

At this time, no modems are allowed to directly connect to the internal network due to the inherent risks involved. The option desired by management is to install the client piece that comes with the Contivity on user laptops for those traveling or working from home so they can access the home office through a local Internet Service Provider. The users who have this privilege must have management approval, the most current antivirus software, and an ISP account to give them the Internet service. It is a luxury to access critical resources remotely, but with this luxury comes potential risks, which, at this time, is acceptable to management.

Only two types of traffic can be initiated from the services network, sqlnet from the web servers and smtp traffic from the mail relay server. In addition, the only traffic allowed to the internal network from the partner's network is initiated by the remote users via the VPN.

GIAC's System Administrators and Information Technology staff need to access the service and partner networks in order to perform administration and to place and retrieve fortunes. This will mainly be done with ssh, a version of telnet that uses encryption. Staff also will manage resources through web-based applications using ssl encryption. GIAC staff will also be allowed to browse the web via a web proxy server and send and receive email. Downloading any files from the Internet is subject to virus scanning and must be for a business use. Email is subject to virus scanning, is the property of GIAC Enterprises, and is available at any time for inspection of content by the management. All download and email scanning will take place on the firewall through one of many popular solutions, for instance Trend Micro or Symantec.

Implementation

Cisco 3620 Border Router:

The border router will be our first layer of defense. The main goal of the router, besides routing, will be to filter illegal traffic before it ever hits the firewall. The syntax here applies to our Cisco 3620 running IOS 12.1. The following is an extended router acl, which uses ip access groups for packet filtering. Logging is enabled and sent to the local logging server.

Filtering for access-group 101 is done in this acl by blocking the RFC1918 local source address traffic from ever getting to the firewall. It also blocks the source address of 0.0.0.0, the local host address of 127.0.0.1, and the legal external ip's of GIAC Enterprises, 115.50.25.0/24. You should never see incoming traffic that has the same ip address as you do.

Filtering for access-group 102 is done in this acl by only permitting the legal ip address range for GIAC to leave and denying everything else. There are several reasons that you would want to allow only that which is a legal address to leave, but the main one is so that you will not be a nuisance to your neighbors on the World Wide Web. Allowing private addressed to leave could allow you to take part in distributed denial of service attacks (ddos), namely the smurf attack. More about smurf attacks can be found at http://advice.networkice.com/advice/exploits/ip/smurf/default.htm. There are many places on the web to learn about different attacks, two of my favorites are www.securityfocus.com and http://advice.networkice.com/advice.

You also want to make sure that you put a warning banner, just in case someone other than you accesses your router and later you can have just cause to pursue legal means.

router acl:

- service password-encryption

- no service finger
- no ip direct-broadcast

- ip access-group 101 in
- ip access-group 102 out

- access-list 101 deny 192.168.0.0 0.0.255.255 any log
- access-list 101 deny 172.16.0.0 0.15.255.255 any log
- access-list 101 deny 10.0.0.0 0.255.255.255 any log
- access-list 101 deny 0.0.0.0 0.255.255.255.255 any log
- access-list 101 deny 127.0.0.0 0.0.0.255 any log
- access-list 101 deny 115.50.25.0 0.0.0.255 any log
- access-list 101 permit any
- access-list 102 permit 115.50.25.0 0.0.0.255 any
- access-list 102 deny ip any any log
- logging 10.1.1.9

- Banner / WARNING: authorized access only/

router acl with tutorial:

There are many options that one can use to help harden the router and filter traffic to and from the firewall, we have chosen a few and they are as follows.

- service password-encryption
Here we see one of the options available in Cisco routers, service password-encryption. Cisco router passwords are usually stored in plain text in the configuration file, using service password-encryption forces the router access password to be encrypted. One should not feel safe just because the password is encrypted, the encryption can be broken. Never the less, it helps in our goal of defense in depth.

- no service finger
There are several options for disabling certain services at the router level; we have chosen to disable the finger service. Disabling the finger service stops the ability of a hacker to gain information about who is logged in and where on the GIAC network.

- no ip direct-broadcast
One other option that we chose to employ is the no ip direct-broadcast. This will stop broadcasted traffic from ever being sent to our firewall, which will help stop a denial of service attack.

The next part of the router acl will explain how to create the groups that will designate which interface on the router the certain filters will apply.

- ip access-group 101 in
This command defines the group that will apply to the serial interface of the router that connects to the Internet.

- ip access-group 102 out
This command defines the group that will apply to the Ethernet interface that connects to GIAC's perimeter network.

The following filters are for access group 101 which apply to the serial interface of the router that connects to the Internet.

- access-list 101 deny 192.168.0.0 0.0.255.255 any log
- access-list 101 deny 172.16.0.0 0.15.255.255 any log
- access-list 101 deny 10.0.0.0 0.255.255.255 any log
Perhaps the most important filter in the router's acl is the blocking of illegal source ip addresses. You should never see traffic coming to your firewall with any of these ip source addresses. So, the previous three filters block the range of IP source addresses that are designated only for internal use and not for public use.

- access-list 101 deny 0.0.0.0 0.255.255.255.255 any log
- access-list 101 deny 127.0.0.0 0.0.0.255 any log
It is also necessary to block the source address of 0.0.0.0 and the local host address of 127.0.0.1, which you should also not see in traffic coming to your firewall. As stated, this filter blocks the illegal source address of 0.0.0.0 and the local host address of 127.0.0.1.

- access-list 101 deny 115.50.25.0 0.0.0.255 any log
Another form of traffic that you should never see coming to your firewall is traffic that has a source address the same as your legal external ip address. This traffic has a spoofed source address and should not be allowed. You should never see someone trying to connect to you as yourself. This filter will block the traffic with GIAC's own external IP addresses and not allow it to reach your firewall.

- access-list 101 permit any
Now that you have written filters to restrict traffic, it is now time to write the rule that will actually permit you to do business. This filter will pass all traffic that is not explicitly denied by the previous ones.

The following filters are for access group 102 and apply to the Ethernet interface of the router that connects to GIAC's Perimeter network.

- access-list 102 permit 115.50.25.0 0.0.0.255 any

We have talked about what traffic you should restrict coming into your network, now we want to talk about the traffic you want to permit leaving your network. You should only see traffic with the legal external ip addresses of GIAC Enterprises coming from your firewall. This filter makes you a good neighbor by not allowing illegal traffic to be sent out on the Internet, and by only allowing traffic with a legal ip address to leave.

- access-list 102 deny ip any any log
Now that you have written a filter to only permit certain traffic to leave, you must write a filter to block all other traffic from leaving. This filter blocks all other ip addresses that are not legal ip addresses from leaving the GIAC network.

The last two filters are recommended for administrative and legal purposes.

- logging 10.1.1.9
This command tells the router which server to send the logged traffic. You should notice that we are not logging traffic that is permitted, but only logging traffic that is denied. You could log all traffic, but it would cause your logs to become quite large, and so we are only logging traffic that is denied.

- Banner / WARNING: authorized access only/
This line tells the router to display a warning message that makes a legal statement about who should be accessing the router. If you are not authorized to access the router then you should not be accessing the router.

Checkpoint Firewall-1:

The Firewall rules are implemented in the order that they will be most often used, to help reduce the processing load on the firewall. They are designed to explicitly meet the security policy of GIAC Enterprises and to not exceed them. Here are the following rules implemented in the order of expected frequency for matching traffic on Checkpoint's Firewall-1.

Firewall rules in the pattern of source/destination/service/(accept or reject)/(logging or not):

1. fw_admin firewall firewall-1 accept log
2. any firewall NBT/ident reject
3. any firewall any drop log
4. any Supplier_Web_Server/Customer_Web_Server http80/https443 accept log
5. any External_Dns udp53 accept log
6. any Mail_Relay_Server smtp accept log
7. International_Partners_IP External_Nortel_Contivity http80/https443 accept
8. Mail_Relay_Server Internal_Mail_Server smtp accept log
9. Internal_Mail_Server any smtp accept log
10. Internal_DNS Not_Internal udp53 accept log

11. Internal_Network Web_Proxy http80/https443 accept log
12. Web_Proxy Not_Internal http80/https443 accept log
13. Web_Servers Internal_Database_Server sqlnet accept log
14. Nortel_Remote Internal_Database_Server https443 accept log
15. Nortel_Remote Internal_Mail smtp accept log
16. Nortel_Remote Internal_DNS upd53 accept log
17. Internal_Network GIAC_Networks ssh accept log
18. GIAC_Networks Logging_Server udp_syslog accept log
19. Real_Secure_Sensors Real_Secure_Console tcp901 accept log
20. Real_Secure_Console any accept log
21. any any any drop log

The Checkpoint graphical version of these rules is located in Figure 2.

Firewall rules with tutorial:

1. fw_admin firewall firewall-1 accept log
2. any firewall NBT/ident reject
3. any firewall any drop log
When you start to write your firewall rules you want to put the most frequently used rules a the top of the list. One of the other important things to remember is to allow yourself to access the firewall so you can manage it. I have heard several horror stories of people publishing policies that do not allow the administrator to manage the firewall. The first rule gives the administrators that access. The second rule blocks netbios traffic and drops it without logging. This is mainly for blocking the "noise" that could clog and rapidly fill up your firewall logs. The third rule blocks and logs all other attempts to contact the firewall.

4. any Supplier_Web_Server/Customer_Web_Server http80/https443 accept log
We expect that the most frequent traffic will be from the Internet to the web servers for customers to purchase fortunes and for suppliers to supply fortunes. This rule permits this traffic to be done on basic http and https.

5. any External_Dns udp53 accept log
For people to connect to our web servers they will need to perform dns lookups. This rule permits Internet users to do name resolution, but at this time GIAC is not allowing nslookups due to the greater risk associated with it. This is essential for web transactions.

6. any Mail_Relay_Server smtp accept log
Another important business function will be providing electronic mail service for customers and suppliers. This rule allows inbound email traffic to our mail relay server. So far, we have put the rules that allow traffic for purchasing and supplying the fortunes at the top of the rule base due to their expected frequency of use.

7. International_Partners_IP External_Nortel_Contivity http80/https443 accept

This is the rule to allow our International partner to connect to the VPN appliance. We also expect this rule to be frequently used so it is put with the other rules permitting web traffic.

8. Mail_Relay_Server Internal_Mail_Server smtp accept log
9. Internal_Mail_Server any smtp accept log
Sending and receiving mail is an important business function as well as a personal one. Internal and external users need to be able to receive mail and to send mail. Rule 8 allows the mail relay server that is located in the Services network to send mail to the Internal network and rule 9 allows internal mail to be sent out.

10. Internal_DNS Not_Internal udp53 accept log
DNS is also an essential function that must be also available for internal users. It is important that the DNS server not be allowed to initiate a connection to the internal network in case of it being compromised in some way. Again, GIAC is not permitting nslookups on tcp53.

11. Internal_Network Web_Proxy http80/https443 accept log
12. Web_Proxy Not_Internal http80/https443 accept log
We decided to provide Internet access for the home office staff and to do this via a web proxy server. This will make administration simpler and keep the number of firewall objects to a minimum. Rule 11 permits users to connect to the proxy server while rule 12 permits the web proxy server to browse the Internet, but not to access anything on the Internal network.

13. Web_Servers Internal_Database_Server sqlnet accept log
Once our customers and suppliers have accessed the web servers and performed the transactions or uploads, we need to be able to get that information in real time. We are allowing the web servers to send data to the internal database server over the sqlnet port. This permits the Services network to initiate connections to the Internal network, but only on that port. This traffic will be closely monitored.

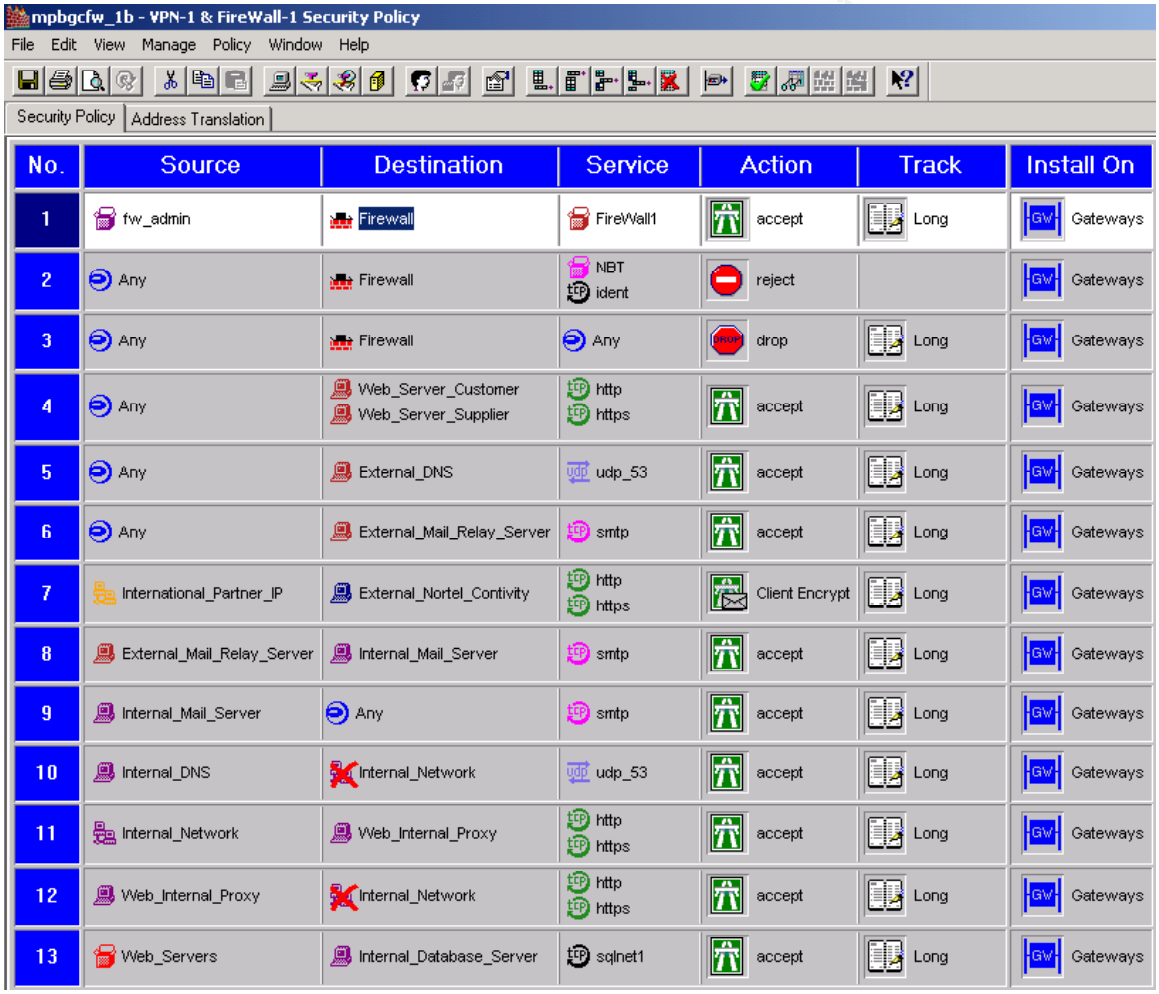
14. Nortel_Remote Internal_Database_Server https443 accept log
15. Nortel_Remote Internal_Mail smtp accept log
16. Nortel_Remote Internal_DNS upd53 accept log
17. Internal_Network GIAC_Networks ssh accept log
In our security policy, we were instructed to provide access to remote staff. For this to take place we are providing email, dns lookups, ssl connectivity to the database server, and ssh to the Internal network. This is another area where the logs will be closely monitored.

18. GIAC_Networks Logging_Server udp_syslog accept log
This rule allows log traffic to reach the logging server on port 514/udp. We have implemented a centralized logging server to help with administration and storing of logs.

19. Real_Secure_Sensors Real_Secure_Console tcp901 accept log
20. Real_Secure_Console any accept log
If you are going to have IDS sensors in your different networks you are going to have to allow them the ability to talk to the management console. Rule 19 opens up port 901/tcp for the Real Secure sensors to send information to the management station. You also must open up the firewall for the management console to talk to the sensors, and this is done in rule 20.

21. any any any drop log
No firewall is complete without the drop all rule. There is no point in only allowing access to certain devices on certain ports if you are not going to then restrict all other access. The purpose of this rule is to drop all of the unauthorized traffic and to log it. Here is a good tip: Checkpoint Firewall-1 does not log traffic when it is dropped, so we added the logging in this rule to correct that.

Figure 2.



No.	Source	Destination	Service	Action	Track	Install On
1	fw_admin	Firewall	FireWall1	accept	Long	Gateways
2	Any	Firewall	NBT ident	reject		Gateways
3	Any	Firewall	Any	drop	Long	Gateways
4	Any	Web_Server_Customer Web_Server_Supplier	http https	accept	Long	Gateways
5	Any	External_DNS	udp_53	accept	Long	Gateways
6	Any	External_Mail_Relay_Server	smtp	accept	Long	Gateways
7	International_Partner_IP	External_Nortel_Contivity	http https	Client Encrypt	Long	Gateways
8	External_Mail_Relay_Server	Internal_Mail_Server	smtp	accept	Long	Gateways
9	Internal_Mail_Server	Any	smtp	accept	Long	Gateways
10	Internal_DNS	Internal_Network	udp_53	accept	Long	Gateways
11	Internal_Network	Web_Internal_Proxy	http https	accept	Long	Gateways
12	Web_Internal_Proxy	Internal_Network	http https	accept	Long	Gateways
13	Web_Servers	Internal_Database_Server	sqlnet1	accept	Long	Gateways

14	Nortel_Remote_Users	Internal_Database_Server	https	accept	Long	Gateways
15	Nortel_Remote_Users	Internal_Mail_Server	smtp	accept	Long	Gateways
16	Nortel_Remote_Users	Internal_DNS	udp_53	accept	Long	Gateways
17	Internal_Network	GIAC_Networks	ssh	accept	Long	Gateways
18	GIAC_Networks	Logging_Server	udp_syslog	accept	Long	Gateways
19	Internal_ISS_Sensor Services_ISS_Sensor Partner_ISS_Sensor	ISS_RealSecure_Console	tcp_901	accept	Long	Gateways
20	ISS_RealSecure_Console	Any	tcp_2998	accept	Long	Gateways
21	Any	Any	Any	drop	Long	Gateways

The reviewing of firewall logs should be a daily task with special attention put upon who is coming from the service and partner networks to the internal network. We went with dual firewalls to reduce the risk of a single point of failure. In the case of one firewall being taken out, then the other would step in and take over.

Nortel Contivity 2600 VPN

When configuring a VPN, you have the option to go with two different security protocols that are available in IPSEC, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is the simpler of the two protocols offering such services as connectionless integrity and data origin authentication. AH protects the TCP header but not the data part of the packet, which provides packet header security but not data integrity. ESP encrypts both the TCP header and the data parts of the packet. We will go with ESP for benefit of the added encryption. We will also use ISAKMP to perform the Internet Key Exchange in the IPSEC sessions.

Access for our international partner, WiseMan Inc., is made possible using Nortel's Contivity 2600. The 2600 has a local radius server, which can be used to distribute pools of IP addresses. We will have two main pools, one for our international partner and one for remote staff. The pool of addresses for remote staff will have subdivisions based on which level of access is granted. Access for our international partner will require those connecting to our VPN to have DES SHA1 and/or 3DES SHA1 encryption levels. No others will be permitted.

In the client software that remote users have installed on their pc's, authentication options are available. One such option is for group authentication where each remote user will have his/her corresponding group name and password, which is a will be the basis for which ip address they receive when they connect. The basic authentication to get into the VPN will be based only on user name and password at this time. The password is

required to be of significant length (8 or greater characters) and be a "strong" password, i.e. it contains letters (lower and upper case), numbers, and symbols (!@#$%.?, etc…) and will be completely different from their GIAC network username and password. Future considerations will allow for the use of a token type of authentication that would employ two-factor authentication, which would greatly improve the authentication parameter in our cryptography scheme. One such product would be RSA's SecureID.

The same standards for the username and password will be required for WiseMan Inc. They will have a unique group name and password, which allot to them their distinguished ip from the radius pool. A product like SecureID would hopefully also be implemented for the international partners as well.

Assignment 3 – Audit Your Security Architecture

The main goal of GIAC's auditing policy will be to verify that the security policy is being followed and still contains its integrity. Testing will be done periodically from outside the perimeter and from the internal network using various auditing tools. Any security policy can and will have standards that need to be implemented, but without the authority to enforce the necessary changes the policy goes for naught. Therefore, it must be understood by such departments that the security administrative staff will have such rights to enforce the security policy and the results of the following audits.

Once a security policy has been established, the audits that follow are an attempt at mitigating risk. Mitigating risk is a form of risk assessment where the effort is put into minimizing the risk as much as possible. Eliminating risk would be nice, but not feasible. The following are the main points of GIAC's auditing policy:

1. Periodic penetration tests
2. Periodic risk assessments
3. Fire drills
4. Process tests

Periodic penetration tests are to be performed on the internal and perimeter networks by GIAC staff and external third party companies as desired. These tests will range from partial intrusion testing, where one sub network might be scanned, to full-blown tests where everything is open to testing. The preferred tool of the GIAC administrators is nmap, a free tool available at www.insecure.org/nmap. Nmap is able to simulate denial of service attacks, able to scan entire networks to see which hosts are alive at what addresses, able to scan single hosts and determine what ports are open and what services are running there, and even able to determine which operating system is running on the machine. Tests will be run at off peak hours, usually between 6pm and 6am on Sundays and Mondays. Possible partial testing can be run on other days but only from 12am to 6am in order to not have any effect on the daily business activities. All scanning must be done with the written permission of management should there be any unfortunate results on any system. The cost of testing done by GIAC employees would only be the possible

overtime or comp time that they work during these off hour test. The cost of hiring a third party company to perform penetration testing will depend highly on the frequency of testing and the name of the company hired.

Prior to testing, all internal systems will be checked to make sure that their timing is in sync, all host based intrusion detection systems and all network sensors will be tested to insure that they are operating and reporting properly to the correct console, and the various logs from the firewall and IDS systems are correct and functional. There will be two main scans done in the penetration tests, the first will be a scan of the firewall itself to verify that the firewall is secure and the second is to verify that the firewall is blocking the traffic that it is supposed to be blocking.

In preparation for the scan that will verify the firewall rules, we have consulted a paper written by Lance Spitzner, "Auditing Your Firewall Setup." There are two main steps, the first is to audit the actual firewall to ensure that it is secure and the second is to verify the rule base. To ensure that the firewall is secure you first need to make sure that it is physically secure, that the operating itself is as locked down as possible, and to port scan the firewall to make sure that there are no open ports. The first is taken care of by your physical structure and the second can be taken care of by consulting an armoring checklist, such as the ones for NT, Solaris, and Linux found at http://www.enteract.com/~lspitz. You can do a port scan on your firewall itself to see what is open on it.

Determining whether your firewall is secure can be done by an nmap scan. There are very many options available with nmap, which is what makes it so great of a tool. The following suggested scan is one that we probably take a while to complete, but it is quite thorough:

nmap –v –g53 –sS –sR –P0 –O –p 1-65000 –o firewall.out 115.50.25.14

A couple of things to note about this scan is the –g, option which lets you specify the source port and the –p option which lets you specify the range of ports to scan. The –o specifies the output file and 115.50.25.14 is the external ip address of GIAC's firewall.

Here is a following sample output of running nmap with the described options.

Nmap (V. nmap) scan initiated 2.53 as: nmap -v -g53 -sS -sR -P0 -p 1-65000 -o realfw1.out 115.50.25.14
(The 64991 ports scanned but not shown below are in state: filtered)

Port	State	Service (RPC)
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
138/tcp	closed	netbios-dgm
443/tcp	open	https

1010/tcp closed unknown
1017/tcp closed unknown

Nmap run completed at Sat Jun 2 05:29:03 2001 -- 1 IP address (1 host up) scanned in 34526 seconds

Is this what we expected? It was expected that 25, 52, 80, and 443 to be open for traffic to be able to reach the web servers, send email, and resolve names. Ports 1010 and 1017 will have to be investigated to find out why nmap brought back the information that it did, as the same for port 138. A better test could be run on the firewall with nmap spoofing different address, such as a private ip address, to see if it would even try to pass that traffic. Tcpdump or SNORT should be run on the inside of the services network to actually see what traffic is coming through.

To test the perimeter we will run nmap against the mail server, dns server, web servers, and the Nortel box.

Testing the mail relay server:

Nmap (V. nmap) scan initiated 2.53 as: nmap -v -sS -o exchange.out mail.giac.com
Interesting ports on (172.16.1.24):
(The 1519 ports scanned but not shown below are in state: closed)
Port State Service
25/tcp open smtp
80/tcp open http
110/tcp open pop-3
143/tcp open imap2

Nmap run completed at Fri Jun 1 17:33:25 2001 -- 1 IP address (1 host up) scanned in 26 seconds

The syntax for this nmap scan is one that is verbose, -v, and that attempts a SYN scan, or half-open connection scan which tests the tcp ports on the mail server. Here we see that the expected port of 25 is open, but we also see that port 80 http is open. There should be no http traffic allowed from the Internet to the mail relay server.

Testing the external DNS server:

Nmap (V. nmap) scan initiated 2.53 as: nmap -v -sU -o dns.out dns.giac.com
Interesting ports on (172.16.1.23):
(The 1519 ports scanned but not shown below are in state: closed)
Port State Service
53/udp open domain

Nmap run completed at Fri Jun 1 17:36:53 2001 -- 1 IP address (1 host up) scanned in

26 seconds

For this scan the verbose option was again used, -v, but this time the –sU was used since dns operates on the udp protocol. We see that only udp 53 is open which is what was expected.

Testing the external web servers:

Nmap (V. nmap) scan initiated 2.53 as: nmap -v -sS -o web.out www.giac.com
Interesting ports on (172.16.1.22):
(The 1519 ports scanned but not shown below are in state: closed)

Port	State	Service
80/tcp	open	http
443/tcp	open	https

Nmap run completed at Fri Jun 1 17:40:40 2001 -- 1 IP address (1 host up) scanned in 26 seconds

To test the web servers we ran the same scan as we did on the mail relay server. Here we see that only ports 80 and 443 are open to the Internet. Another interesting scan to be done on the web servers would be to scan from the Internal network and see if these ports as well as that of 23 (ssh) would be open. It would also be good to see if regular telnet could be used to access any resource on the Services or Partners network.

To test the Nortel Contivity:

Nmap (V. nmap) scan initiated 2.53 as: nmap -v -sS -o nortel.out 115.50.25.41
All 1523 scanned ports on (115.50.25.41) are: filtered
Nmap run completed at Fri Jun 1 17:59:59 2001 -- 1 IP addresses (1 hosts up) scanned in 429 seconds

Again we ran the TCP SYN scan for the Nortel Contivity's external interface. No open ports were found on the VPN box.

Similar tests were run on the Partners network for the web server and dns server, but the output is not included in this report for brevity.

Periodic risk assessments will contain the reviews of penetration testing and will promote awareness of information security. This can be done through meetings with management and possibly done through training or orientation classes.
Nmap is one of many network assessment tools freely available on the Internet. If you go to www.insecure.org/tools.html you will find a top 25 list of tools and where to find them. Two of my favorites are SNORT found at www.snort.org and NESSUS found at www.nessus.org.

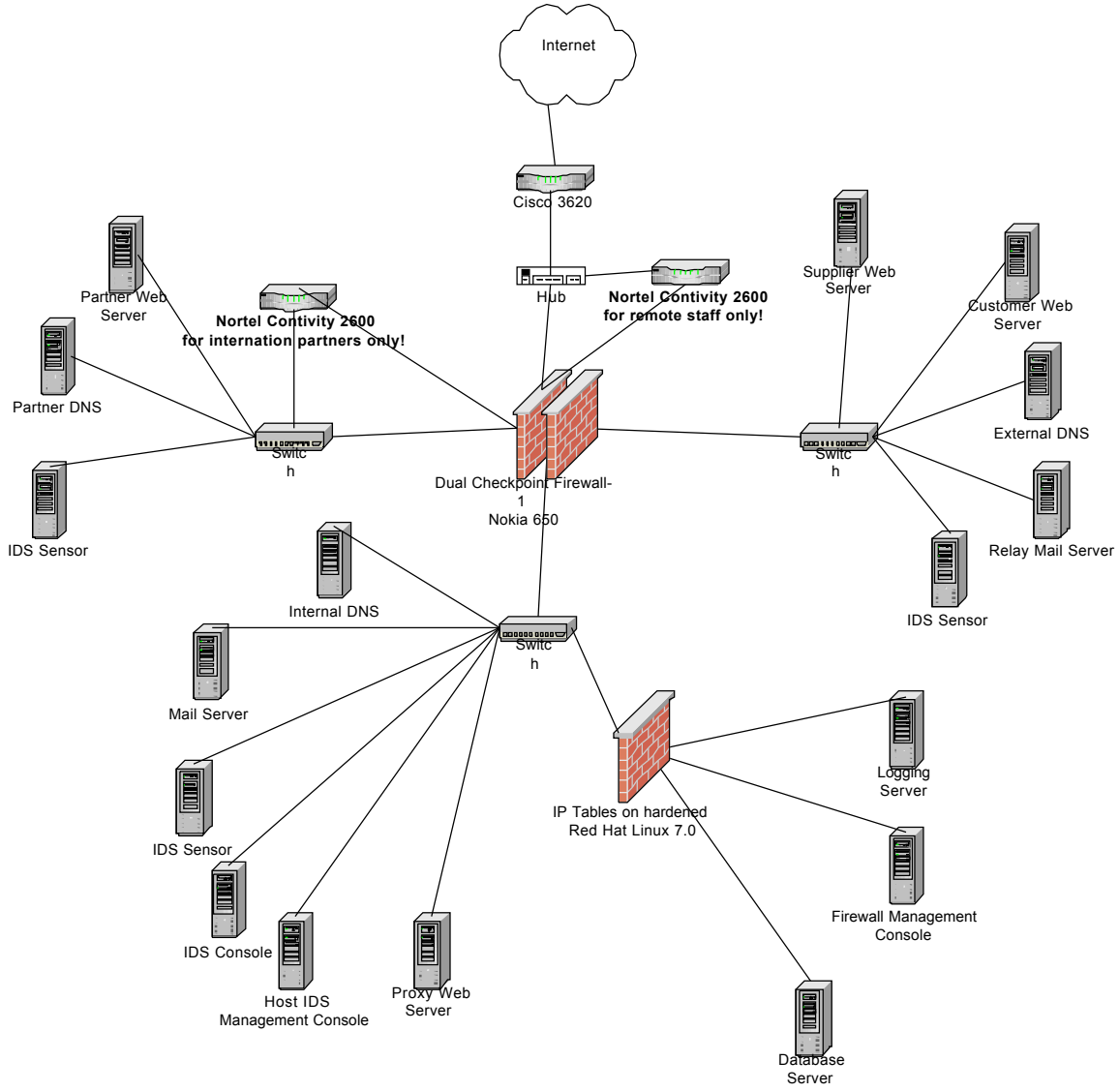
Fire drills are simulated "live fire" tests where the security and support staff and given a situation and must respond to it accordingly. Such a situation would be where a fortunes database has been corrupted and the staff must correct the problem, figure out how it occurred, and fix it so that it won't occur again. Other similar situations would be simulated intrusions, firewall crashes, and the screaming boss attack. The screaming boss attack is where management approaches one of the staff and demands for certain things to be open on the firewall or some other similar situation. This would be to test the certain employees knowledge of the security plan and how they respond in the face of upper management. Fire drills are an excellent preparation tool and are necessary for any security and support staff to ensure their preparation.

Process testing has to do with many of the basic functions at GIAC. Ranging from limiting password age to 3 months, issuing a password complexity standard, to testing the possibility of "social engineering." Social engineering is the term given to where someone would call the help desk and impersonate some director or executive requesting a new password and to get his current one because he has forgotten his. Though we don't want to admit it, this can be a very serious security hole.

Conclusion:

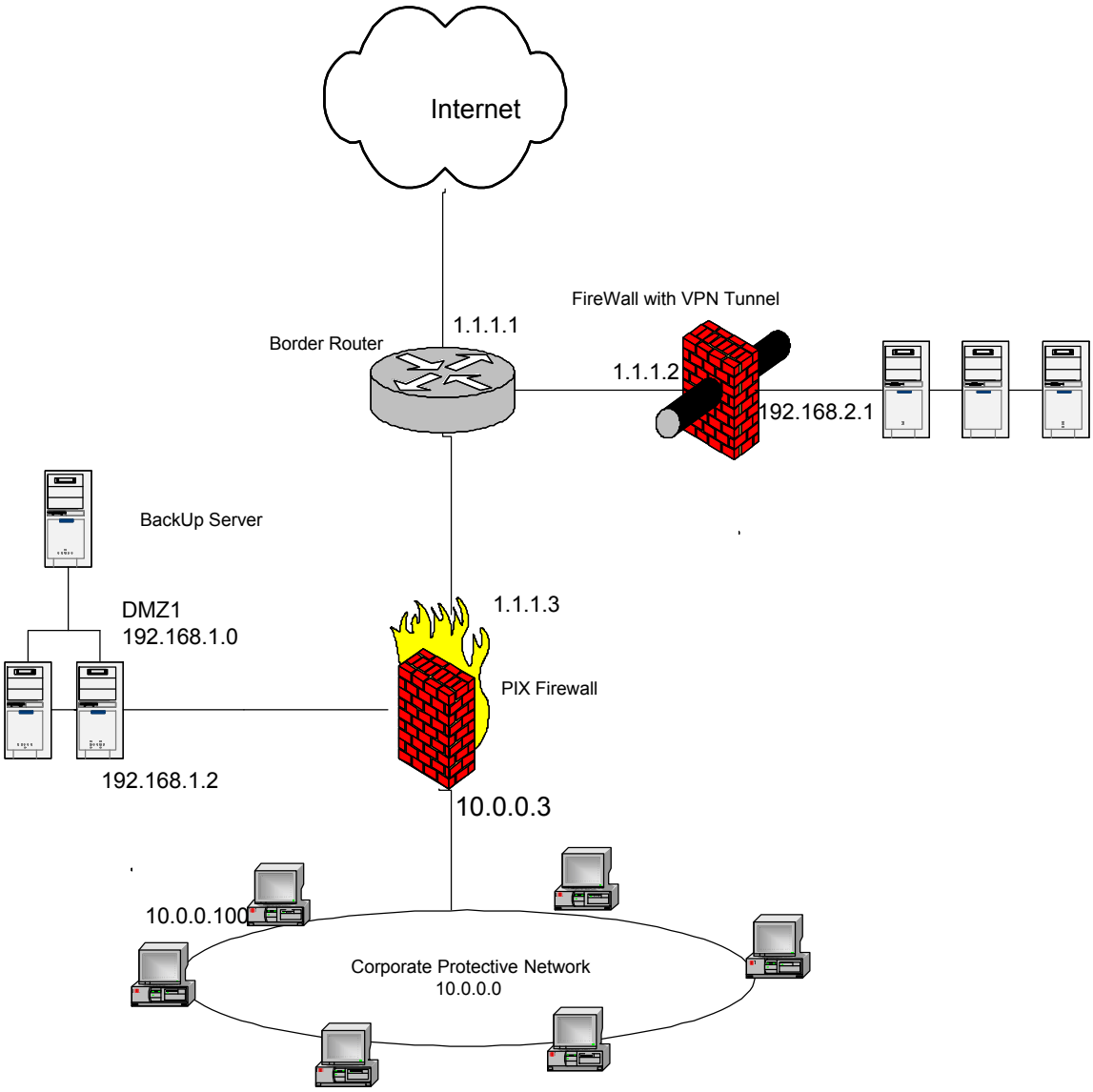
The audit was only performed on our primary firewall and was performed against the internal firewall running iptables. An audit of traffic from the Nortel Contivity was not conducted and it is felt that this could be a weakness in the architecture. It is recommended that a second VPN appliance be purchased so that the International partners and the remote staff do not pass through the same network, as is illustrated in figure 3. In this way the primary firewall would still authenticate users coming from the Contivity for access into the Internal network, but it would not be shared in the Partners network. This would completely isolate the remote staff connections from the all of the business related connections. Further investigation will put into why some of the primary firewall ports are closed and not filtered. The primary firewall was found to pass http traffic to the email relay server, which was not expected. It is recommended that GIAC hire an independent company to do a penetration test of GIAC's networks to see if their results are similar.

Figure
3.



Assignment 4 – Design Under Fire

For the design under fire, I have chosen Deepak Midha's paper located at http://www.sans.org/y2k/practical/deepak_midha_GCFW.doc. His network diagram is as follows:



The first thing that we notice is that he is running a Cisco PIX Firewall with as he says "version 5.0(1) or higher." Deepak is running the PIX firewall version 5.0(1) or higher and this opens himself up to several vulnerabilities, especially since he leaves it open to any version at or higher than 5.0.

An attack against the firewall itself:

To attack the PIX firewall we are going to do a two-step attack. First, we will take advantage of a vulnerability in the firewall's inability to handle exceptional conditions in smtp filtering to allow us to execute code on the smtp server in DMZ-2. Second, once we are able to execute code on the mail server we will use a flaw in the firewall's inability to

handle multiple requests from an unauthorized user for TACACS+ authentication to starve the firewalls resources, which can cause the firewall to crash. The two vulnerabilities were found at www.securityfocus.com and are as follows:

2000-09-19: Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability
bugtraq id 1698, class Failure to Handle Exceptional Conditions
vulnerable Cisco PIX 5.0, 5.1, 5.2

2001-04-06: Cisco PIX TACACS+ Denial of Service Vulnerability
bugtraq id 2551, class Origin Validation Error
vulnerable Cisco PIX 5.1.4

The smtp vulnerability plays on a flaw in PIX's exceptional conditional handling. It is possible to "evade the smtp command restrictions by tricking the firewall into thinking the body of the message is being sent went it isn't." The firewall allows all text between the "data" command and "<CR><LF><CR><LF>.<CR><LF>", so if we malformed some messages we can get some openings to work with. If during communication with the smtp server in DMZ-2 of Deepak's network, you send the "data" command before you normally would, like before the "rcpt to" command you get an error on the smtp server, but the firewall knows nothing of this and still lets traffic through. This opens the door for you to do what you want on the smtp server. In our case, we are going to use this chance to execute some TACACS+ authentication requests back to the firewall from the smtp server. The bugtraq report states the following:

"PIX firewalls using TACACS+ are vulnerable to a resource starvation attack which results in a denial of service. Upon receiving multiple requests for TACACS+ authentication from an unauthorized user, the firewalls resources can be exhausted. This causes the firewall to crash, requiring power cycling to resume regular service.

This makes it possible for a user from either the public or private side of the PIX to crash the firewall, and deny service to legitimate users."

From the smtp server, we will send multiple requests from a bogus user for TACACS+ authentication to the firewall. This will deplete its resources causing it to crash, thus disallowing any communication to the network and therefore stopping business transactions from DMZ-2.

A denial of service attack:

In this attack, we have been able to compromise 50 cable modem/DSL systems and will attempt to take out the router of GIAC Enterprises, as Deepak has designed it. We will first point out that we will not use an ICMP floods in out attack since in his router acl

Deepak as rejected all udp packets related to snmp, as we see in the following:

Access-list 100 deny udp any any eq snmp

This leaves us with the option of performing a TCP SYN flood or a UDP flood (apart from snmp) to DoS the router. The TCP SYN attack is also known as a half-open connection, which is where you send a bunch of SYN packets but never ACK the SYN-ACK that the server sends back. By sending many of these SYN packets we use up the number of connections allowed to that router at a time so that the router can no longer accept requests from anyone else. The basic idea behind a DoS is to send so many packets to a host or number of hosts that there cpu is maxed out trying to deal with all of the fake packets. The result will be that either the machine crashes or that stays so busy that it cannot perform its business function.

To perform our DoS against GIAC we will take advantage of our 50 compromised hosts and of one specific vulnerability in the Cisco IOS software.

2000-10-25: Cisco IOS Software "?/" HTTP Request DoS Vulnerability
bugtraq id 1838, class Failure to Handle Exceptional Conditions
vulnerable Cisco IOS 12.0, 12.1

This vulnerability applies to machines running the Cisco IOS software and those that do not have a password enabled on the router. In Deepak's router acl he does not have mention of the option, enable-password, thus leaving him open to this vulnerability. If you send an http request with "?/" in the address and an enable password then it will cause the router to crash and restart after the watchdog timer has timed out. An example of such a request is the following:

http://targer/anytext?/

This will be the first move in our DoS attack.

Since we have compromised 50 cable modem/DSL systems we will use them as the second part of our attack. Once we send our http request and cause the router to enter in a loop and reboot we will further complicate the matter by causing our compromised host to run the following command:

nmap –sS 1.1.1.1 (where 1.1.1.1 is the legal ip address of GIAC's router)

We will also have our compromised hosts sending http requests to the router with the malformed "?/" in the http request. The combination of the nmap SYN flood and the http vulnerability will keep the router either timing out trying to process the url or locked up from all of the SYN packets directed at it.

One way to fix this from happening will be to have a strong password enabled on the

router which would eliminate the vulnerability of the "?/" in http requests. Imposing rate limits from certain hosts on the router help reduce the risk of a denial of service attack from any certain host.

An attack plan to compromise an internal system through the perimeter system.

When one goes to penetrate the internal system of a company, it is not about getting one server through one vulnerability, it is about attempting to get in as many ways as possible until you get your final result. In our attempt to penetrate the internal network, we are going to use two vulnerabilities in the Cisco PIX firewall.

For this we will use one of the before mentioned vulnerabilities in the PIX firewall.

2000-09-19: Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability
bugtraq id 1698, class Failure to Handle Exceptional Conditions
vulnerable Cisco PIX 5.0, 5.1, 5.2

This is the vulnerability in the smtp filtering function of the firewall that allows us to execute code on the smtp server in DMZ-2.

The second is a vulnerability in the ftp server located in DMZ-2.

2000-10-03: Cisco PIX PASV Mode FTP Internal Address Disclosure Vulnerability
bugtraq id 1877, class Failure to Handle Exceptional Conditions
vulnerable Cisco PIX 5.2

This is the vulnerability where if you send many requests to enter PASV ftp mode during the ftp session that the ip address will eventually be disclosed.

The reason I chose the ftp and smtp server is that I found these two vulnerabilities in the two servers. Creativity is necessary, and this is what I found to work with. Exploiting the smtp weakness will be implemented the same as in the firewall attack. We will craft emails so that we hide smtp commands in the fake text of the email message, which will enable us to gain access to the smtp server and issue commands from it. From the smtp server we can use netbios or some other protocol to find shares on other servers on that particular DMZ and from all of them attempt connections to the internal network. Attempting to crack the passwords stored on that server could lead us to gain access to other machines on that DMZ.

To implement the ftp weakness we can run the following code:

echo USER someuser

```
sleep 2
echo PASS somepassword
sleep 2
echo SYST
while true
        do
        echo PASV
        sleep 1
        echo PASV
        echo PASV
        sleep 1
        echo PASV
        echo PASV
        sleep 1
        echo PASV
        echo PASV
        sleep 1
done
```

If this code is run, perhaps many times it will yield an open connection to the server and give you its internal ip address. Once you gain access to the ftp server, you can try a variety of ways to enter the internal network. Attempting to find another machine on the same DMZ with has a trust relationship with it to hopefully access that machine, also trying to attempt connections to the internal network from the ftp server.

For both of the servers, once you gain access you should be able to find out what version of the operating system it is running. From there you could use a known vulnerability to get what is desired, access to the internal network.

Conclusion

To be secure in the changing world around us you must stay up to date on the most recent security holes and patches. Each day I here of a new idea or request for service on some web based application, which can add tremendous functionality to a companies business capability. With these opportunities come risks, and mitigating these risks is a full time effort and quite a journey. Firewalls and routers are wonderful tools that if used correctly can do a world of good, but they are not the end-all be-all of security, they are merely the beginning.

Matthew P. Brown
SANS 2001 New Orleans

References:

Chris Brenton, Lance Spitzner, and Stephen Northcutt. The SANS Institute: Track 2-Firewalls,
Perimeter Protection, and Virtual Private Networks. Volumes 2.1-2.5

Lance Spitzner. "Auditing Your Firewall Setup" http://www.enteract.com/~lspitz