Global Information Assurance Certification Paper

DANIEL A. BACHRACH

LEVEL TWO FIREWALLS, PERIMETER PROTECTION AND VPNS

GCFW PRACTICAL ASSIGNMENT

LEVEL TWO FIREWALLS, PERIMETER PROTECTION AND VPNS

GCFW PRACTICAL ASSINMENT

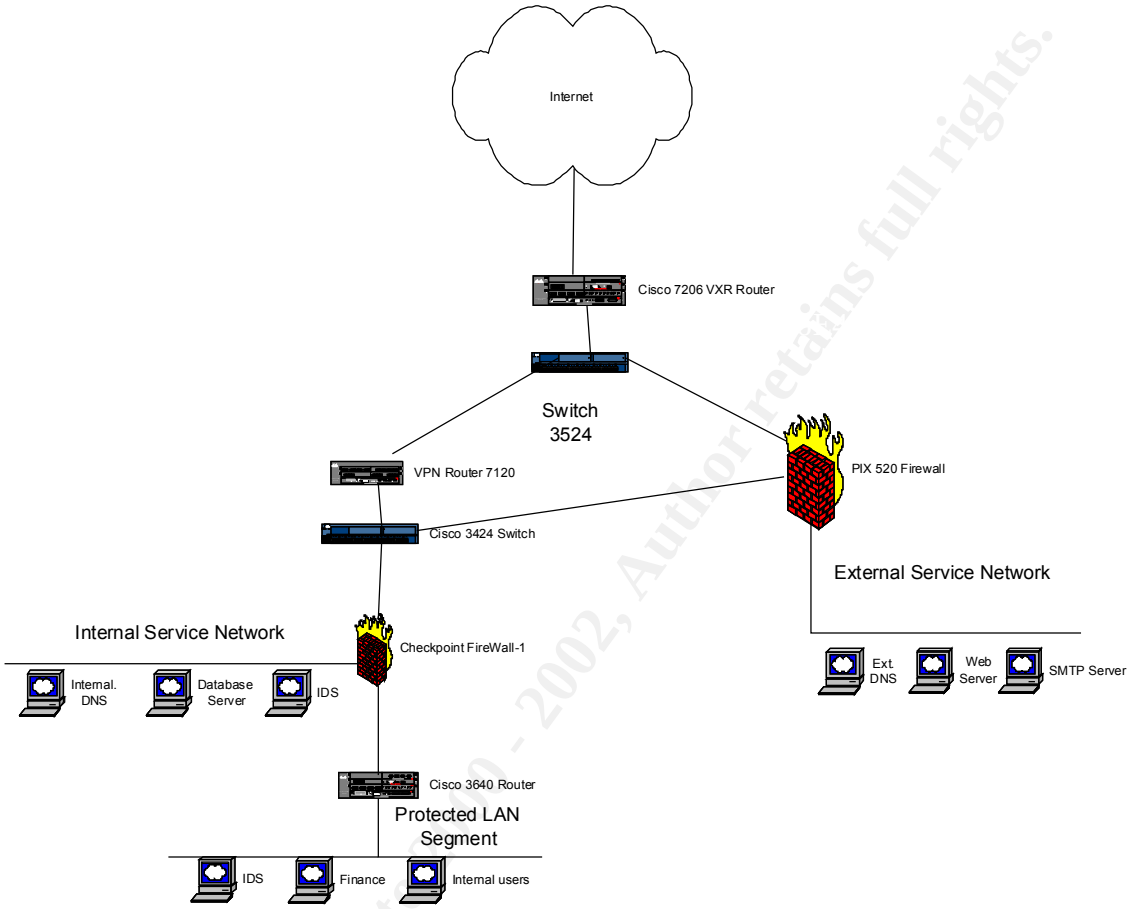
ASSIGNMENT 1 – SECURITY ARCHITECTURE (25 POINTS)

Define a security architecture for GIAC Enterprises, a growing Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings, and which has just completed a merger/acquisition. Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access and internal firewalls. Be explicit about the brand and version of each perimeter defense component. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

You must consider and define access for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes)

SOLUTION – ASSIGNMENT 1



The overall goal of any security solution should be to provide a defense in depth strategy, or the process of providing multiple layers of security to the network being protected. With multiple layers of defense in place, not only does it give the administrator time to further protect sensitive data when portions of the existing defenses fail, but also to provide him/her with as much information about the attack as possible.

Part of this assignment was very vague on the amount of money that could be spent for this project so a certain amount of assumptions will be made. While it could be assumed that a blank check exists for this project, it's unlikely that a real world scenario would exist that does so. Therefore costs considerations will be included as part of this design.

Coming in from the Internet a perimeter router, in this case a Cisco 7206, would direct the packets to the outer firewall, a Cisco Pix 520, which would direct customers to the

external Service Network (xxx.29.158.0/24). Suppliers and partners would be directed by the external firewall to an internal firewall, a Checkpoint Firewall-1, which would direct partners and suppliers to an internal service network (xxx.29.160.0/24), and allow company employees into the protected LAN (xxx.29.165.0/24).

Partners, suppliers and employees coming in via VPN would hit the external router, be directed over to a VPN router and then to the Checkpoint Firewall-1. The VPN router would be a Cisco 7120.

The protected LAN would house the most critical servers, such as those for finance. The internal service network would house the database server and intranet servers as well as the internal DNS server. The external service network would house the external DNS server, web server, SMTP server as well as and IDS system.

E-mail coming from the Internet would be sent to the SMTP server, which would be allowed to open a session through the Checkpoint Firwall-1 to deliver mail. The web server would be able to open as session through the Checkpoint Firewall-1 as well to retrieve fortunes from the database server located on the internal service network.

ASSIGNMENT 2 – SECURITY POLICY (25 POINTS)

Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:

- Border Router
- Primary Firewall
- VPN

You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By 'security policy' we mean the specific ACLs, firewall rule set, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners – you MAY NOT simply block everything!

(Special note VPNs: Since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP based VPNs are also fully acceptable as long as they are well defined.)

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, filter, rule, etc.
4. A description of each of the parts of the filter
5. An explanation of how to apply the filter
6. If the filter is an order-dependent, list any rules that should precede and/or follow this filter and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
7. Explain how to test the ACL/filter/rule

Be certain to point out any tips, tricks or "gotchas"

SOLUTION – ASSIGNMENT 2

Border Router-

In considering the requirements for the Access Control Lists (ACLs) for the border router, we want to consider how users will connect to us. First those users that connect via VPN must be allowed to connect and passed along to the correct VPN router and then into our interior firewall for access onto the internal service network or onto the protected LAN.

Second, we want to keep in mind that those users connecting to the company via the Internet and not using VPN should be routed to the external firewall and then to the external service network.

In addition we want to add some additional security policies onto our border router to start the first level of security. For instance, we want to turn off all ICMP echo, echo-replies, IP direct broadcasts, finger, telnet, as well as any other services that aren't expressly needed. In addition ports that aren't explicitly needed should also be turned off or denied by the ACL on the router.

As shown in section 1, the boundary router is a Cisco 7206. This router for the sakes of this exercise will have a connection to the Internet on a serial interface, denoted as Serial 1/0 with an IP of xxx.172.201.2 , and access to the inside, labeled FastEthernet 2/0 xxx.29.150.2. The ACL on this router list as follows:

no ip http
no ip bootp
no ip direct-broadcasts

The *no ip http* statement in the ACL prevents access to services from bootp hosts on the attached networks inside the router. If we were using bootp services across our network we would want to leave this enabled, but we are going to assume this is not the case at this point. *No ip http* prevents a web browser from using port 80 to access the router. By disabling the *IP direct broadcasts*, we stop the interface from converting directed broadcasts into local broadcasts and forwarding them on. For instance, if a workstation on xxx.172.201.0/24 sends a broadcast server request to xxx.29.150.2, the gateway interface would forward the request to network xxx.29.150.0/24 were it would be converted to 255.255.255.255 or ff.ff.ff.ff.ff.

no service finger
no service telnet
no service gopher

These lines turn off the services finger, telnet and gopher preventing them from accessing the router. Since this ACL would be applied to the outside interface, this would prevent someone from sending a telnet command into the router from the internet. The same holds true for gopher and finger. However, I should mention here that this is not a complete list of services that could be turned off. For instance, the command no service FTP could be applied and prevent someone from FTPing onto the network from the outside. However, we will assume that our suppliers may FTP there work to a server for review or that the partners may need to FTP to get to a new driver. Whatever the case, we will allow this to be passed through to the firewall. Other services that may want to be disabled could include NNTP, POP3, SNMP, Time Server, DNS, Echo Server or IMAP4. However, for the sake of this exercise we will again assume that we need these services for whatever reason being able to get into the network from the outside and not the three above.

banner/ NOTICE: This is a private network device. If you are not authorized
to connect or configure this device, disconnect at once! Actual
or attempted use, access, examination, or configuration change by
an unauthorized person will result in criminal and civil prosecution to the full extent of the law./

This adds a banner to the router so that when someone logs into it, they are made aware that this is a private router and that by accessing the router and/or making changes to it will result in prosecution.

Interface Serial 1/0
ip address xxx.172.201.2 255.255.255.0
access-group 101 in
access-list 101 deny tcp any any eq 137
access-list 101 deny udp any any eq 137
access-list 101 deny tcp any any eq 138
access-list 101 deny udp any any eq 138
access-list 101 deny tcp any any eq 139
access-list 101 deny udp any any eq 139
access-list 101 deny tcp any any eq 135
access-list 101 deny udp any any eq 135

access-list 101 deny tcp any any eq 42
access-list 101 deny udp any any eq 42
access-list 101 deny udp any any eq 67
access-list 101 deny tcp any any eq 136
access-list 101 deny udp any any eq 136
access-list 101 deny udp any any eq 123
access-list 101 deny tcp any any eq 1109

Here we are using an extended access list to deny access to the network by specific TPC and UDP ports. This is done in a couple of different ways. You could block each port from any host, as we've done above, or you could use the option to shut down access from specific hosts. I didn't go through each and every port, however, it normally is a good idea to shut down all the ports that you explicitly don't need to have open. For instance, I included port 136 to show that, although it isn't a commonly used port, it has been used since approximately 1988 for DNS type traffic.[i] Personally I would go through a list of ports and close each of them if there wasn't a specific reason to have them open. Also be aware the not all ports have both a tcp and udp port. For instance, I included udp 123 in my list. This blocks the ntp or network time protocol. I also showed that I blocked tcp port 1109 or kpop or POP with kerberos as an example of a port using only tcp. Also, be aware that some ports are used by more than one function. For instance, 111 tcp and 111 udp is used for both portmap and sunrpc. So be very careful blocking what you want to block.

access-list 101 deny icmp any any echo
access-list 101 deny icmp any any echo-reply
access-list 101 deny icmp any any packet-too-big
access-list 101 deny icmp any any time-exceeded
access-list 101 deny icmp any any traceroute
access-list 101 deny icmp any any unreachable
access-list 101 deny icmp any any net-unreachable
access-list 101 deny icmp any any administratively-prohibited
access-list 101 permit tcp any any
access-list 101 permit udp any any

This portion of the list shows blocking all of the ICMP protocols. Until I attended the SANs conference in New Orleans, I wasn't aware of the amount of damage that could be caused by ICMP pings. Since it was suggested by Lance that we create a black-hole for ICMP pings, we drop all of the packets and prevent the 'black-hats' from discovering anything about our network using this protocol. The last two statements allow everything else to be passed along to the firewall or the VPN router. Again, this isn't a complete list of ports that should be blocked, but an example of how to block the ports from any host.

Primary Firewall (CISCO PIX 520)-

The perimeter firewall is the next layer of defense and should deny anything not specifically required to access the network.

PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz-public security20
nameif ethernet3 dmz-extranet security30
nameif ethernet4 dmz-vpn security40
nameif ethernet5 pix/intf5 security50

We start by naming the interfaces and setting the security level on each interface. The first two are the outside and inside interfaces and are not configurable, however the other 4 are and can be named anything we want and can be assigned a value on the security portion between 1 and 99.

hostname GIACFW

We give our firewall a host name.

fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
no fixup protocol smtp 25

These statements perform protocol security checks. Notice I didn't do a security check on the SMTP protocol. Mainly I don't do this because anything coming in from the internet on this protocol will be sent to an SMTP scanner and scanned at that point.

names
name xxx.168.16.217 S07_VPN
name xxx.73.234.217 S07_IN
name xxx.168.16.38 WWWVPN_VPN
name xxx.219.131.81 SMTPscan_OUT
name xxx.172.201.23 SMTPscan_IN

Next we assign some names. This isn't required, but as we move further down, it will make it easier for us to understand our configuration. I've assigned more than we need here, so that you get the idea, but pay attention to the SMTPscan_OUT and the SMTPscan_IN as we'll use it further down.

logging timestamp
no logging standby
logging console debugging
logging monitor debugging
logging buffered debugging
logging trap debugging
logging history debugging
logging facility 20

logging queue 32000

These statements set up the logging that we want to know about. I would highly recommend sending your logs to a syslog server and using a program to parse them so you don't have to go through each and every line for something important. Here I've set up to log all of the debugging that takes place on my firewall.

interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
interface ethernet4 auto
interface ethernet5 auto

Next we set the speed. In this case I've decided to let the interface decide the best way to handle the speed issue. However, some administrators like to force the speed and duplex so you may occasionally see something like, *interface ethernet0 100half*, or *interface ehternet1 10full* instead.

ip address outside xxx.29.150.2 255.255.255.255
ip address inside xxx.29.158.0 255.255.255.0
ip address dmz-vpn xxx.29.160.0 255.255.255.0

These three statements define what is allowed to go where.

nat (inside) 0.0.0.0 0.0.0.0

This statement is fairly obvious. We kill natting on the inside.

static (inside,outside) SMTPscan_OUT SMTPscan_IN netmask 255.255.255.255 0 0

Let's add a static translation. This allows traffic to be directed to our SMTP scanner interfaces. Notice the 0 0. This shows that there are no metrics assigned at the end of the statement.

conduit permit tcp host SMTPscan_OUT eq smtp any
conduit permit tcp host SMTPscan_OUT eq ident any
conduit permit udp host SMTPscan_OUT eq 113 any

Here we have set up inbound access. Notice we've allowed access for the SMTP and IDENT protocols as well as authentication. In essence what we've done is said in the first line, allow any TCP protocols coming from SMTPscan_OUT, or xxx.219.131.81 using port 25, or smtp, to access any host.

route outside 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx 1
route inside xxx.29.0.0 255.255.0.0 xxx.xxx.xxx.xxx 1

Next we tell it how to get to the boundary router and to our internal network.

no rip outside passive
no rip inside passive
no rip outside default
no rip inside default
no rip services passive
no rip services default
no snmp-server location
no snmp-server contact
snmp-server community looking
no snmp-server enable traps

Here we stop the firewall from supplying rip and snmp to anyone. Really your firewall shouldn't be responding to these requests. Also we've turned off the snmp traps. One thing I do want to point out is that you can set the snmp community string, as we've done here. In this case it's *looking*.

floodguard enable

In order to help prevent TCP SYN attacks we're turning on the flood guard option. This should force the firewall into aggressive mode should it pick up this type of attack is occurring.

sysopt connection permit-ipsec
isakmp identity address
telnet timeout 60
terminal width 80

Finally, in order to allow IPSec through we have to have the first two statements here. The third statement simply says that if a telnet session hasn't actively done anything for 60 seconds kill the session. The forth and final statement, simply sets the terminal screen to a width of 80 columns for easier reading.

Because the PIX has deny all by default we don't need to express it in the configuration. One thing that must be remembered here is to ensure that the expressions are placed in the order that you want them to be. For instance, you don't want to add a permit statement after a deny statement because the packet will be dropped before it ever gets to the permit statement. As a rule, most administrators will copy the configuration to a WordPad or notepad document and make their changes in the document, review it two or three times then copy and past it into the configuration on the firewall. This helps to prevent any mistakes that most of us would make as simple typos.

Another thing that must be mentioned, but isn't shown in the above configuration is the dropping of the RFC addresses. As added protection you would want to include the following at the top of the configuration file:

ip access-list usual INCOMING
deny 10.0.0.0 0.255.255.255 log
deny 172.16.0.0 0.15.255.255 log
deny 192.168.0.0 0.0.255.255 log
deny 127.0.0..0 0.255.255.255 log
deny (internal network addresses) log
permit any any

You would also want to block any addresses that don't come from your local network from leaving back out. Thus, helping to block denial-of-service attacks. Additionally, and as with most security it is at the discretion of the administrator, you may want to consider how to harden the firewall as well as the boarder router.

NOTES: One thing I didn't do was to go into extraordinary lengths to block every port that should be blocked. Most administrators will want to customize this portion. There may be certain ports that may need to be open for homegrown applications as well as ports that can both be harmful and useful. I would recommend that each administrator look long and hard at what needs to be explicitly opened for their environment. There are a lot of ticks to how an administrator may want to configure his/her firewall and boarder router and this is usually best left up to the individual to figure out based on their security policy.

VPN Router (CISCO Altiga 7100)-

The VPN router is basically setting up tunnels through the Internet that allows the secure transfer of data from one point to the next. In essence what this configuration does is allows IP traffic coming from one very specific location to access certain items on the network, in this case our internal service network.

hostname GIACVPN

Here, we've named our VPN router GIACVPN. !'s act as a place holder and don't really have a purpose other than to act as spacers between the different segments.

!
logging rate-limit console 10 except errors
enable secret 5 1i4X.$ckMGdPsUIFIJIrAZmISQv.
enable password 7 052C0929205F5A59481B542C43

We set the passwords, both to log into the router and to get to the enabled command structure, from the console port.

!
username (User 1) privilege 15 password 7 14231D1B2B1124
username (User 2) privilege 15 password 7 106906310A1A175B5D
ip subnet-zero
!

Next, let's set up two users who if they access the box remotely will have to identify themselves by name and password. Once the user puts in their user name and password they are given the highest level of security clearance into the box, 15.

```
!
no ip finger
no ip domain-lookup
```

Again, as on the boundary router, we block certain services from the outside. In this case finger and DNS.

```
ip host ROTFW xxx.79.181.42
ip host SEOULFW xxx.103.168.128
ip host JNB xxx.23.148.226
ip host TAIPEIFW xxx.79.9.193
ip host DURFW xxxx.23.148.162
ip host CPTFW xxx.36.164.34
ip host HONGKONGFW xxx.193.54.227
ip host HAMBURGFW xxx.68.129.66
!
```

Let's assume we are going to allow site-to-site access to our partners. Here we define the host IP addresses that the VPN sessions, or tunnels, will be allowed from. For instance, from the Rotterdam firewall we will allow access as long as it comes from IP address xxx.79.181.42. A similar situation will exist for the other sites that exist in Seoul, Johannesburg, Taipei, Durban, Capetown, Hong Kong, and Hamburg.

```
!
!
crypto isakmp policy 10
 authentication pre-share
 lifetime 40000
```

In the section above we set our ISAKMP policy to group 10, define our authentication as a pre-shared key and then set the lifetime of the tunnel to 40000 seconds or approximately 11 hours.

```
crypto isakmp key hope1 address xxx.79.9.193
crypto isakmp key hope1 address xxx.23.148.226
crypto isakmp key hope1 address xxx.23.148.162
crypto isakmp key hope1 address xxx.36.164.34
crypto isakmp key hope1 address xxx.11.85.161
crypto isakmp key hope1 address xxx.103.168.128
crypto isakmp key hope1 address xxx.193.54.227
crypto isakmp key hope1 address xxx.68.129.66
crypto isakmp key hope1 address xxx.79.181.42
crypto isakmp keepalive 10
!
```

This section sets the shared secret key with the address of the router. This is stored in the clear in the configuration file of the VPN router and in this case is *hope1*.

NOTE: For simplicity sake I've chosen to make them all the same, but normally most administrators would choose not to do this for the added security that if one is compromised, the others are not.

```
!
crypto ipsec transform-set SHA.DES.SHA ah-sha-hmac esp-des esp-sha-hmac
!
```

The line above sets our IPSec protocol to use, as well as the encryption and authentication. As you can see, I've chosen the transform set DES with .

```
crypto map OUTSIDE 1001 ipsec-isakmp
 description Taipei PIX506 to xxx.29.160.0/23
 set peer xxx.79.9.193
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address TAIPEI1
crypto map OUTSIDE 1011 ipsec-isakmp
 description Johannesburg South Africa PIX506 to xxx.172.160.0/24
 set peer xxx.23.148.226
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address JNB1
crypto map OUTSIDE 1021 ipsec-isakmp
 description Durban South Africa PIX515 to xxx.172.160.0/24
 set peer xxx.23.148.162
 set peer xxx.36.164.34
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address DUR1
crypto map OUTSIDE 1031 ipsec-isakmp
 description Capetown South Africa PIX to xxx.172.160.0/24
 set peer xxx.36.164.34
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address CPT1
crypto map OUTSIDE 1041 ipsec-isakmp
 description Rotterdam PIX to xxx.172.160.0/24
 set peer xxx.79.181.42
```

```
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address ROT1
crypto map OUTSIDE 1051 ipsec-isakmp
 description SEOUL PIX to xxx.172.160.0/24
set peer xxx.103.168.128
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address SEOUL1
crypto map OUTSIDE 1061 ipsec-isakmp
 description HONG KONG PIX to xxx.172.160.0/24
 set peer xxx.193.54.227
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address HONGKONG1
crypto map OUTSIDE 1071 ipsec-isakmp
 description HAMBURG PIX to xxx.172.160.0/24
 set peer xxx.68.129.66
 set security-association lifetime kilobytes 20000
 set security-association lifetime seconds 3000
 set transform-set SHA.DES.SHA
 set pfs group1
 match address HAMBURG1
!
```

The sections above define our Crypto-map or the IPSec Map. Basically it takes everything that we've done earlier in the configuration and puts them all together. Once this is done, we need to apply it to the interface on the Internet, or external, side of the VPN router. *Let's look at the portion starting with Crypto map OUTSIDE 1071 ipsec-isakmp*. Outside is just a name and the number 1071 identifies the portion of the map being configured. The line set peer xxx.68.129.66 associates the peer router with this map as does the transform-set line and the match address HAMBURG1 line. You'll notice two extra lines one setting the security of the association lifetime to 20000 kilobytes, and one setting the lifetime seconds to 3000 seconds. This adds addition protection to the tunnel and helps to prevent replay attacks.

```
!
interface FastEthernet0/0
 description Internet Connection
 ip address xxx.29.150.4 255.255.255.240
 duplex auto
 speed auto
```

```
 crypto map OUTSIDE
!
interface FastEthernet0/1
 description Internal
 ip address xxx.29.160.0 255.255.255.0
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
!
interface Serial1/1
 no ip address
 shutdown
!
interface Serial1/2
 no ip address
 shutdown
!
interface Serial1/3
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
no ip http server
!
```

Once we have defined the crypto-map we must apply it to the interface the traffic will flow through. In this case we've applied it to interface FastEthernet0/0.

ASSIGNMENT 3 – AUDIT YOUR SECURITY ARCHITECTURE (25 POINTS)

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate the costs and level of effort. Identify risks and considerations
2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this,

including the tools and commands used. Include screen shots in your report if possible.

3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

SOLUTION – ASSIGNMENT 3

Step 1: Plan the assessment.

The first phase of the audit would have to be the planning portion. We will want to look at both the boundary router as well as the primary firewall.

One of the first things to take into consideration is how much of an impact the audit will have on the system. As with most companies the amount of traffic that the router and firewall are dealing with as well as the size of the ACL will limit how much pounding the system can take during an audit. For that reason a couple of time periods should be established for conducting the audit. It should be determined the peak period of traffic as well as when the least amount of traffic is hitting the two systems. During the peak times, a light to moderate amount of traffic generated by the audit should be used to ensure that the ACLs on the router and firewall aren't allowing items in because they are overwhelmed, and during the lighter periods a moderate to heavy audit can take place to ensure that the ACLs hold up to a stronger dedicated attack. This will have the advantage of ensuring the reliability of the systems without causing problems for the users in a live environment.

The second item would be determining what tools to use for the audit. Besides the well-known Nmap, for documenting ports and scanning TCP, ICMP as well as RPC, there are a myriad of other tools, such as those found on hacker sites, which could be used. Others might include Patchwork, from The Center for Internet Security, Shields Up from GRC.com and for logging, Private I from Open Systems.

Another item that must be considered is what you are trying to determine. Some may want to test the logging capabilities of the router and/or firewall, while others may want to know if the configurations of the ACLs on the router and/or firewall are working properly. This will also help to determine the type tools to use.

Finally, the cost of the assessment would have to be considered. It might be wise to contract out, for instance, the assessment to a third party to give an independent review of the devices. This can range from a few hundred dollars to several thousand. Two items often come into play when considering this. One, whether GIAC Enterprises desires an independent third party to attempt the review and second how much money can be spent. Additionally, even if the audit isn't contracted out, the tools themselves may have a cost

associated with them. Tools like NMap or Patchwork (http://www.cisecurity.org/patchwork.html) can be found for free. Others however can be quite expensive. I prefer the free ones, as they usually don't have hidden agendas (i.e. sales) associated with them. One product that may be useful for checking the logging on the router and firewall is a product called Private I (http://opensystems.com). This product essentially sets up a syslog server and helps produce reports in a very readable format. One other option that can be considered is using a web site such as http://grc.com that does scanning, using their shields up software, and tells you what ports are open. This is a free service and one that I have found invaluable in the past.

Step 2: Implement the assessment:

Lets start by trying the different services that the boundary router should be dropping. For instance, trying a Telnet session into the router using its various interfaces should be immediately dropped without reason from the device. Second trying to finger a known host on the inside of the router should be dropped without reason. If the ACLs are performing correctly the service attempts should appear to go into a black hole. However, they should be getting logged and a review of the log files on the router would confirm this. Again, I would attempt a light attempt during the busiest part of the day for the device and a much heavier attempt during the lightest.

Next, let's go ahead and use Nmap to determine what ports are open and listening for connection. If all goes as planned only those ports that are needed are open and we should get responses back such as:

Port 21/TCP Open ftp
Port 80/TCP Open http
Port 25/TCP Open smtp

Indicating that these ports are open and what service they provide connection for. If however, we saw a port that shouldn't be open listening, and then we could investigate further to determine why that port is open or if we missed one that should have been closed.

The final portion that I might attempt against the router, and this also tends to work for firewalls are the known bugs that allow you to attempt hacks against the passwords on the boxes. Assuming that the passwords are encrypted and that the box is adequately hardened, this should fail as well. This could be done utilizing programs such as L0PHTCRACK.

Next, we should test the ACLs on the firewall to ensure that they are doing what we want them to do. Let's test the ports using the Nmap scan again and see if any new ports are open that shouldn't be. Assuming that they are secure, we could use the TCP SYN attack to ensure that the SYN flooding is being intercepted properly. Again a review of the logs is very important to insure that they are capturing what we want to analyze.

Just to help double check our work we'll use the Shields Up program from GRC located on their website at www.grc.com. If everything works the way it's supposed to only those

ports that should be open will be reported back to us. A sample of what you will get back looks like this:

Your computer at IP:

xxx.xxx.xxx.xxx

Is now being probed. Please stand by. . .

Port	Service	Status	Security Implications
21	FTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Closed	Your computer has responded that this port exists but is currently closed to connections.
25	SMTP	**OPEN!**	Servers for the Simple Mail Transfer Protocol (SMTP) have a long history of intrusion vulnerabilities. Any intruder with time on his hands will want to come back and explore this open port on your machine more fully.
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
80	HTTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
139	Net BIOS	**OPEN!**	As you probably know by now, the NetBIOS File Sharing port is the single largest security hole for networked Windows machines. The payoff from finding open Windows shares is so big that many scanners have been written just to find open ports like this one. Closing it

			should be a priority for you!
143	IMAP	Closed	Your computer has responded that this port exists but is currently closed to connections.
443	HTTPS	**OPEN!**	The presence of this secure web port in your system implies that this system is establishing secure connections with web browsers. The number one reason for doing this is the transmission of credit card information. This implies that the successful intruder could access the web server's credit card database and score bigtime. This is a VERY bad port to have open unless you are actually conducting secure web commerce!

Note: Several of the "Service" names shown above link directly to items on the ShieldsUP! FAQ Page to provide specific discussion of ports and services. If the port status shown above concerns you, please read the general descriptions below, then click on the port's service name for specific discussion.

Port Status Descriptions:

Stealth!

If all of the tested ports were shown to have stealth status, then **for all intents and purposes your computer doesn't exist to scanners on the Internet!**

It means that either your computer is turned off or disconnected from the Net (which seems unlikely since you must be using it right now!) or an effective stealth firewall is blocking all unauthorized external contact with your computer. This means that it is **completely opaque** to random scans and direct assault. Even if this machine had previously been scanned and logged by a would-be intruder, a methodical return to

this IP address will lead any attacker to believe that your machine is turned off, disconnected, or no longer exists. You couldn't ask for anything better.

There's one additional benefit: scanners are actually hurt by probing this machine! You may have noticed how slowly the probing proceeded. This was caused by your firewall! It was required, since your firewall is discarding the connection-attempt messages sent to your ports. A non-firewalled PC responds immediately that a connection is either refused or accepted, telling a scanner that it's found a live one ... and allowing it to get on with its scanning. **But your firewall is acting like a black hole for TCP/IP packets!** This means that it's necessary for a scanner to **sit around and wait** for the maximum round-trip time possible — across the entire Net, into your machine, and back again — before it can safely conclude that there's no computer at the other end. That's very cool.

FALSE STEALTH REPORTS

A "Stealth" port is one from which no reply is received (neither acceptance nor refusal) in response to a connection initiation request. This ShieldsUP web site sends a series of **four connection requests**, waiting for any reply after each one. If no reply is received to any of them, the port is declared to be "Stealth" **. . .** and for all intents and purposes that's exactly what it is. But Internet "packets" are continually being lost in route to their destination. When Internet "routers" are overloaded with traffic they have no recourse other than to simply drop packets completely, hoping that they will be resent when the destination fails to acknowledge their receipt. This, of course, is why we try four times to get through.

Therefore, if prime-time Internet congestion coupled with a slow or noisy connection were to cause those four packets to become lost or garbled, our port test would show "Stealth" when your port would have replied if it had ever received the request.

If you suspect that this may have happened during the assembly of the report above, simply refresh your browser's page to re-run the tests. If the results differ you can presume that congestion or a weak connection were the temporary cause.

Closed

"Closed" is the best you can hope for without a stealth firewall in place.

Anyone scanning past your IP address will immediately detect your PC, but "closed" ports will quickly refuse connection attempts. Your

computer might still be crashed or compromised through a number of known TCP/IP stack vulnerabilities. Also, since it's much faster for a scanner to re-scan a machine that's known to exist, the presence of your machine might be logged for further scrutiny at a later time — for example, when a new TCP/IP stack vulnerability is discovered.

You should stay current with updates from your operating system vendor since new "exploits" are being continually discovered and they are first applied upon known-to-exist machines **. . .** like this one!

OPEN!

If one or more of your ports are shown as OPEN! then one of the following two situations must be true:

You have servers running on those open ports:

If your system is running Internet servers on the ports shown as OPEN, you should stay current with PC industry security bulletins. New security vulnerabilities are being found continually. When crackers learn of a new vulnerability, they quickly grab their scanner logs to search for systems that have been scanned in the past and are of the known-to-be-vulnerable type. This allows them to be attacking logged systems within moments of learning of a newly located security hole. It is therefore important for you to respond to any news of new vulnerabilities in your systems as quickly as possible. The crackers are hoping you'll take your time.

You DO NOT have servers running on those open ports:

If you are not actively offering Internet services through the ports shown as OPEN, something is very wrong with your system:

It is actively advertising its presence on the Internet and soliciting the attention of ALL PASSING PORT SCANNERS!

NOTE: I've pointed out twice that a review of the logs on both the firewall and the router is important. I can't stress this enough as many companies and administrators ignore this simple security measure.

Step 3: Conduct a perimeter analysis:

As with any security system, there is always room for improvement. We could look at tightening down the ports and ensuring as few as possible are open.

Second, an increase in the encryption of the passwords on both routers and firewalls could always be strengthened. One method that might be considered is changing the passwords often, maybe monthly. Also setting up user names and passwords with different security levels might help to protect the over all box.

Perhaps setting up natting on the firewall to help hide the external service network a little more could be done as well. This would provide a method of hiding the actual address of the box and make it somewhat harder to find and hack.

Since we know that http servers and smtp servers as well as DNS servers are always open for attack we know that we have to expect that these boxes on the external service network will eventually be attacked and broken into and thus a review should be conducted periodically to ensure they are not compromised.

NOTE: Since I don't have a live network to run these 'attacks' against I can't provide some of the information that normally would be provided at this level. (i.e. screen shots, true results of scans etc. etc.)

ASSIGNMENT 4 – DESIGN UNDER FIRE (25 POINTS)

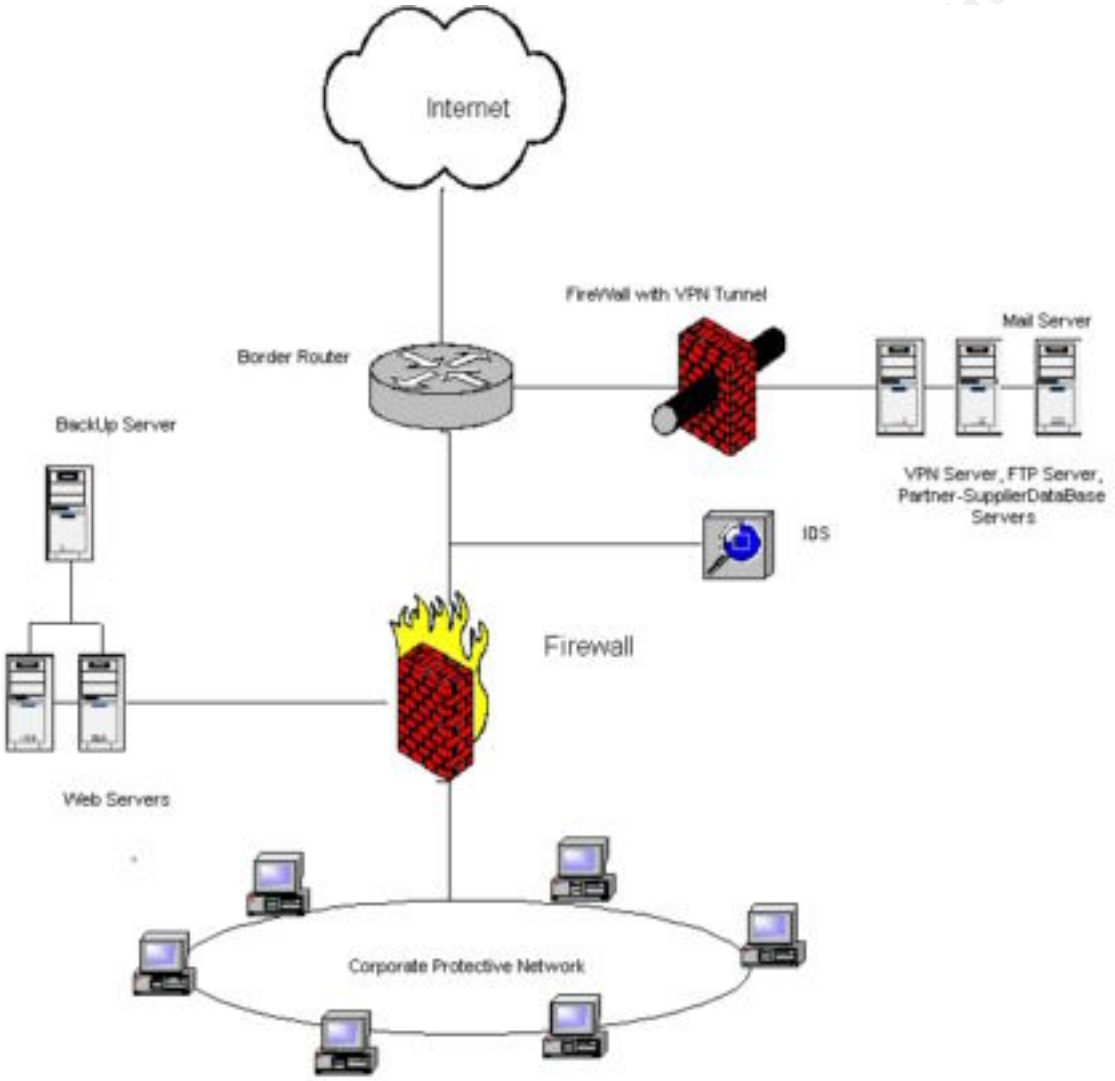
The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!

Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and past the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target and describe the process to compromise the target.

SOLUTION – ASSIGNMENT 4

For this portion of the assignment I chose to perform my attacks against Deepak Midhas' design (http://www.sans.org/y2k/practical/deepak_midha_GCFW.doc).



1. Attack against the firewall itself:

For this attack I choose the FTP vulnerability that affects the PIX firewall (http://www.cisco.com/warp/public/784/packet/jan01/p75-cover.html). Running this attack against the PIX firewall that Deepak used in his design allows an encapsulated command to open a new session through the firewall thus allowing the transmission of unauthorized data through the firewall. Deepak used a PIX 515. Without, applying the patch offered by Cisco, the firewall wall is left vulnerable to this attack. This is a fairly straightforward attack.

2. DoS attack:

For this attack I decided to use the TCP SYN attack. Simply put this attack would flood the router and/or firewall with SYN packets and reduce the bandwidth of the available resources (i.e. the CPU) as well as leaving the connection partially open until it times out waiting for the response to the SYN ACK. Implementing the TCP intercept mode on the firewall could prevent this. This should force the router into aggressive mode once it hits the appropriate limit to help reduce the number of open connections as well as help reduce the load on the resources. A review of the log file would confirm if this is working or not.

Since I wanted to make sure I was through in my DoS attack, I decided to toss in an ICMP flood attack as well. Since the firewall and router should be dropping the packets for all ICMP protocols, the best I could hope for here was a simple bandwidth reduction.

3. Attack of internal system:

Let's go after the DNS server, since it tends to be one of the easiest to attack. I would start with the DNS BIND issue (http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57056,00.html), which would allow a 'blackhat' to redirect web traffic. Or worse yet, poison the DNS services that a company may often publish out to the rest of the world.

One other system that has recently come to light and may allow a hacker to exploit is the new Cisco IOS attack against routers. (http://www.computerworld.com/cwi/stories/0,1199,NAV47_STO58279,00.html) By compromising the configuration of the router, the hacker could have complete control to roam the internal network of a company. Since most often than not the passwords on the routers tend to be the same as those on the firewall, accessing this could be extremely damaging.

---

[i] This information was provided by David J. Huggins, Director of Operations – Telecommunications, Full-Duplex Communications Corporation. (813) 818-9852 Dhuggins@full-duplex.net