Global Information Assurance Certification Paper

Author: Clay Maney
Date: 11/11/00
Track: GIAC Firewall and Perimeter Protection
Monterey, CA, October 2000

Assignment #1: Security Architecture

Define a security architecture. The goal of your policy is to use filtering routers, firewalls, VPNs and internal firewalls to rapidly implement the VISA "Ten Commandments" to the extent possible at GIAC Enterprises, a new Internet Startup that expects to earn 200 million per year in sales of online fortune cookie sayings. The "Ten Commandments" are listed below:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
2. Keep security patches up-to-date.
3. Encrypt stored data accessible from the Internet.
4. Encrypt data sent across networks.
5. Use and regularly update anti-virus software.
6. Restrict access to data by business "need to know."
7. Assign unique IDs to each person with computer access to data.
8. Track access to data by unique ID.
9. Don't use vendor-supplied defaults for system passwords and other security parameters.
10. Regularly test security systems and processes

The student assignment is to produce a diagram, or set of diagrams with explanatory text defining how to use perimeter technologies to implement as many of the requirements above as possible. For this assignment you are a large and growing E-business that just completed a merger/acquisition you must consider the need for customers, suppliers, and partners.

We shall begin by dividing our security architecture into two distinct pieces: the security policy, and the networking infrastructure itself. The security policy is the piece upon which everything else rests. It will both define how various devices are to be configured, in general terms, as well as how individual users can interoperate with them. The networking infrastructure section of this design will detail specific configuration steps and considerations for all pertinent devices on the network.

The Security Policy:

Any security policy can quickly become a tremendously complex creation, but we will try to keep it closely defined into three broad areas: user education, change management/accountability, and a broad set of guidelines that define configuration of firewalls, routers, servers, etc. This policy needs to, at a minimum, address as many of the "Ten Commandments" as possible in order to provide a reasonably secure network. Any commandments not covered in this section will be discussed in detail in the "Networking Infrastructure" section of this document.

Commandment #1: Install and maintain a working network firewall to protect data accessible via the Internet.

- Firewalls have a tendency to generate an inordinate amount of logs. These logs need to be examined by someone knowledgeable enough to understand them. Further, they need to be secured in such a way that the logs themselves are

considered to be pristine. In an effort to guarantee these two functions, this policy recommends the following: a dedicated server be used for nothing other than syslog functionality which resides in the internal network. This server can be either linux or freebsd and will be configured to have no services running on it other than syslog and Ssh. Trained personnel will be responsible for going through the logs on a daily basis and comparing them with the logs from the IDS systems to watch for potential problems. No other accounts will exist on this machine. Lastly, the firewall administrators will be required to remain up-to-date on firewall related vendor security announcements. More specific configuration information will be given in the networking infrastructure section of this document.

Commandment #2: Keep security patches up-to-date.

- All system administrators/security administrators should be required to monitor vendor security mailing lists as well as reputable third party security mailing lists such as SANS, BUGTRAQ, and CERT. A mechanism should be in place to allow for weekly meetings with other administrators to discuss the relevance of the various vulnerabilities to GIAC Enterprises' networks prior to applying any patches. It should be noted that exceptions can be made at the discretion of the individual system administrator/security administrator for particularly dangerous exploits such as the recent "IIS Unicode Traversal" vulnerability. Further, any patches should first be applied to non-production systems to try to eliminate costly potential downtime of production servers.

Commandment #4: Encrypt data sent across networks.

- The only Internet-originated traffic that will be allowed into the internal network will come via trusted third-party companies and these will be connecting either via Ssh or triple-DES VPN tunnels. It should be noted that the internal network itself must be isolated from other sensitive systems such as the accounting systems. All e-commerce will take place using SSL into the DMZ network.

Commandment #5: Use and regularly update anti-virus software.

- Anti-virus software should be installed at every user workstation, every applicable server, and, when possible, at the firewalls. Auto-updating anti-virus software should be used and configured to pull down new signature files on a bi-monthly basis. Further, these should be configured to pull from a local server which has itself been configured to pull from the vendor's website with at least the same regularity.

Commandment #6: Restrict access to data by business "need to know."

- Establish a firm policy that defines exactly what is required for a person to acquire "need to know" in a department other than his/her own. Using either NTFS or Novell Netware permissions, grant any additional (non-home-group) access on a per-user basis rather than just adding users to additional groups. For example, if Bob is in Engineering and needs access to some Accounting files and has met the criteria, give him access to those files individually; don't just add him to the Accounting group. Further, a weekly audit of these temporary exceptions should be made to prevent unintentional access remaining long after it is no longer necessary.

Commandment #7: Assign Unique IDs to each person with computer access to data.

- Every user on the network is assigned a unique user ID. This includes any off-site users, any business partners coming across a VPN, and absolutely anyone else that ever uses a computer on the corporate network. There will be no "group" id's that more than one person has access to like "guest" or "training". Lastly, administrators will be trained to use their own IDs with programs like "sudo" to elevate their authority unless absolutely required to use root access.

Commandment #9: Don't use vendor-supplied defaults for system passwords and other security parameters.

- Ensure that every server has been strictly examined for such accounts as Windows "Guest" account or Irix's "lp" account. Any such accounts should be immediately removed or disabled from login. Also, any default accounts on the systems should have their passwords changed. Further, any user accounts that are created should be configured in such a way as to require the user to change his/her password upon first login. Lastly, if services such as Compaq Insight Manager are present, be sure to configure them to have non-default passwords as well.

Commandment #10: Regularly test security systems and processes.

- This will be covered in more detail later, but it must be noted that any security system must be routinely examined for continuing relevance against new security threats.

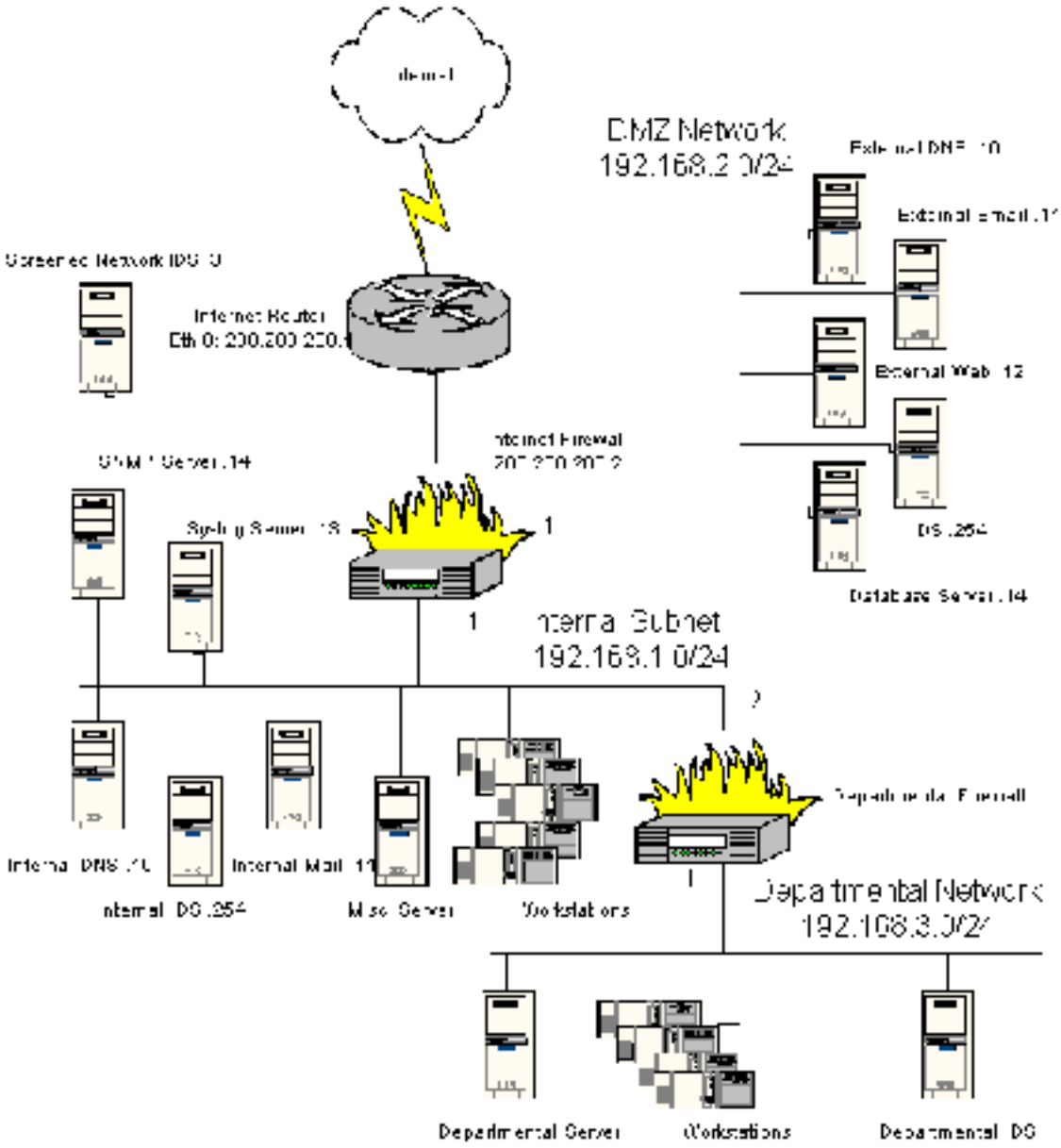
Further, several other things need to be addressed to fully make this policy as all encompassing as we can:

1) Every user must undergo basic security instruction before (s)he is even allowed to log into the network for the first time. This instruction should include how to generate a good password and how to behave securely on the phone, among other things.
2) All passwords should be routinely run against a common hacker password cracking utility such as L0phtCrack. Any passwords that are found within some pre-determined period of time should be added to the dictionary and the accounts set to change passwords on next login. Further, the owners of those accounts should be re-taught how to create secure passwords.
3) Services that pass clear-text passwords, like pop3, should be eliminated whenever possible to help protect from sniffers.
4) Tripwire shall be installed on every server, regardless of where it resides in the network.
5) Human Resources is required to notify IT of any hiring or firing on the day that it happens so that users can be created/deleted/retired as necessary. Under no circumstances shall an ex-employee retain a valid login account after termination… if an account is still needed for some reason, a new account with new privileges can be created.

Networking Infrastructure:

The physical network can easily be subdivided into four separate areas itself which will be shown in the diagram on the next page. We will cover these areas on an "outside-in"

approach. The first area happens to be the only one of which we have no control over: the Internet. We will not discuss the Internet itself in this paper.



As you can see, we have been assigned the 200.200.200.0/24 Class C address space for our network.

The second subsection of the network is the screened network. The screened network is often mistakenly considered to be a DMZ but it is not. The screened network is nothing more than a small network that exists between the Internet router and the Internet firewall that is protected by access-lists on the router. This network is an ideal location for an IDS as it can tell you when someone is knocking at the doors. There will be no production systems in this network at all.

Because the Internet router is our first point of contact with non-secure systems, we will attempt to filter out as much "noise" as possible before allowing data to the firewall. Any data that is dropped due to our filtering rules will be logged via the internal syslog that was mentioned earlier in the paper so that it can be examined for errors on the network or potentially malicious activity. Some of the things that will be filtered at this point will include inbound or outbound spoofed source addresses, inbound traffic to unknown service ports, and DNS zone transfers. Management of this router shall be done via telnet and shall be configured to only accept connections from the internal network. A detailed configuration for the Internet router will be discussed later in this paper.

The DMZ network will only contain such servers as are needed to run the services required for business and nothing more. In the case of GIAC Enterprises, this includes a web server, a database server, an external DNS server, an external E-mail server, and an IDS. All of the servers will be configured with the minimum amount of services running that will allow them to function properly. The DNS server will be configured with only those machines listed that actually exist within the DMZ. As for the E-mail server, it will be configured to prevent mail relaying. The database server will be configured to run on an encrypted filesystem such as Microsoft's Encrypted File System or the Linux or BSD CryptFS so that no customer information is exposed unnecessarily. Further, administration of these boxes will only be allowed via Ssh from the internal network or direct console access. Lastly, any sample scripts will be removed from all of the servers before they are brought online.

The Internal Network will hold enterprise-wide common file servers, the internal e-mail server, the internal DNS server, and another IDS that will be from a different vendor than the ones in the DMZ or screened network. It will also be subdivided so that departments that require increased protection such as Accounting and Human Resources can be segregated from the rest of the network. Subdivision of the networks will be accomplished by putting Cisco Pix 506 firewalls in place between the networks.

As should be expected, no unnecessary services will be running on any of the servers in any of the networks. This will be verified by running port scans against each host before they are placed on the net. Any open ports of unknown origin will be thoroughly investigated before the systems are open for production work. Further, Tripwire shall be loaded on all servers to help notify us of anything changing without approval.

Finally, any vendor or third-party supplied patches should first be applied to test systems and tested as rigorously as possible in order to reduce the risk of downtime or new vulnerability. The test systems should not be on the same network as any production system.

Assignment #2: Security Policy

Develop a security policy (implemented as a firewall filtering policy) that focuses on requirement #1, above: "Install and maintain a working network firewall to protect data accessible via the Internet". Use the Base Security Policy listed below as a starting point; you DO NOT need to repeat this information. Instead, focus on what ADDITIONAL

filtering you would recommend and why. Keep in mind that you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything. Your policy should implement your security architecture design from Assignment 1, above.

For each ADDITIONAL filtering recommendation in your policy, write a tutorial on how to implement that recommendation on your firewall or perimeter defense solution. Be explicit about the brand and version of perimeter defense. Screen shots, network traffic traces, firewall log information, and URLs to find further information should all be used. Be certain to include the following:

1. The reason these services might be considered a vulnerability.
2. Relevant information about the behavior of the protocol or service on the network.
3. Syntax of the filter.
4. Description of each of the parts of the filter.
5. Explain how to apply the filter.
*6. If this filter is order-dependent, what other rules should this filter precede and follow.***
7. Explain how to test the filter.

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

*** You may find it easier to create a section of your practical that describes the order in which you would apply all of the rules, rather than trying to do it with each policy cluster. Be certain to explain your reasons for the order you choose - we cannot read your mind.*

Base Security Policy

The Base Security Policy contains the filtering recommendations from Appendix B of the SANS Top Ten document located at http://www.sans.org/topten.htm. Please note, we are NOT asking you to write a tutorial to explain how to block the services from the Top Ten, only for the ADDITIONAL filters you recommend. Student practicals from July - August 2000 focused on how to block the services described below; you may wish to reference one of these practicals in your work. They can be found at http://www.sans.org/giactc/gcfw.htm.

In this section, we list the Base Security Policy so you know what additional services to recommend blocking. This Policy lists ports that are commonly probed and attacked.

Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts.

A warning is also in order: blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

1) Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.

2) Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)

3) RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)

4) NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)

5) X Windows -- 6000/tcp through 6255/tcp

6) Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)

7) Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)

8) Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)

9) "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

10) Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

11) ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages.

Before we can begin to build the access-lists and firewall configurations for our Internet router and external firewall, we need to have a list of what ip addresses are viewable to the outside world. This list will, of necessity, be as short as possible and will be listed once again using an "outside-in" approach for simplicity.

Our public address space: 200.200.200.0/24
Internet router: WAN address 199.199.199.2/30
LAN address 200.200.200.1/24
Internet Firewall external interface: 200.200.200.2
Screened-subnet IDS: 200.200.200.3

DMZ address space: 192.168.2.0/24
Internet Firewall DMZ interface: 192.168.2.1
External DNS: 192.168.2.10 (DMZ) - 200.200.200.10 (NAT)
External Mail: 192.168.2.11 (DMZ) – 200.200.200.11 (NAT)
External Web (http and https): 192.168.2.12 (DMZ) – 200.200.200.12 (NAT)
DMZ IDS: 192.168.2.254
DMZ Database Server: 192.168.2.20

Internal main address space: 192.168.1.0/24
Internet Firewall internal interface: 192.168.1.1
Internal Syslog Server: 192.168.1.13 (internal) – 200.200.200.13 (NAT)
Internal SNMP Server: 192.168.1.14 (internal) – 200.200.200.14 (NAT)
Internal DNS: 192.168.1.10
Internal Mail: 192.168.1.11
Internal IDS: 192.168.1.254

Internal Networks will be provisioned using PIX 506 firewalls and will not offer any services to the outside world.

Access-lists in the Cisco world are configured as following:

standard access-lists
access-list <list #> <permit/deny> <from ip address> < from inverse mask>

OR

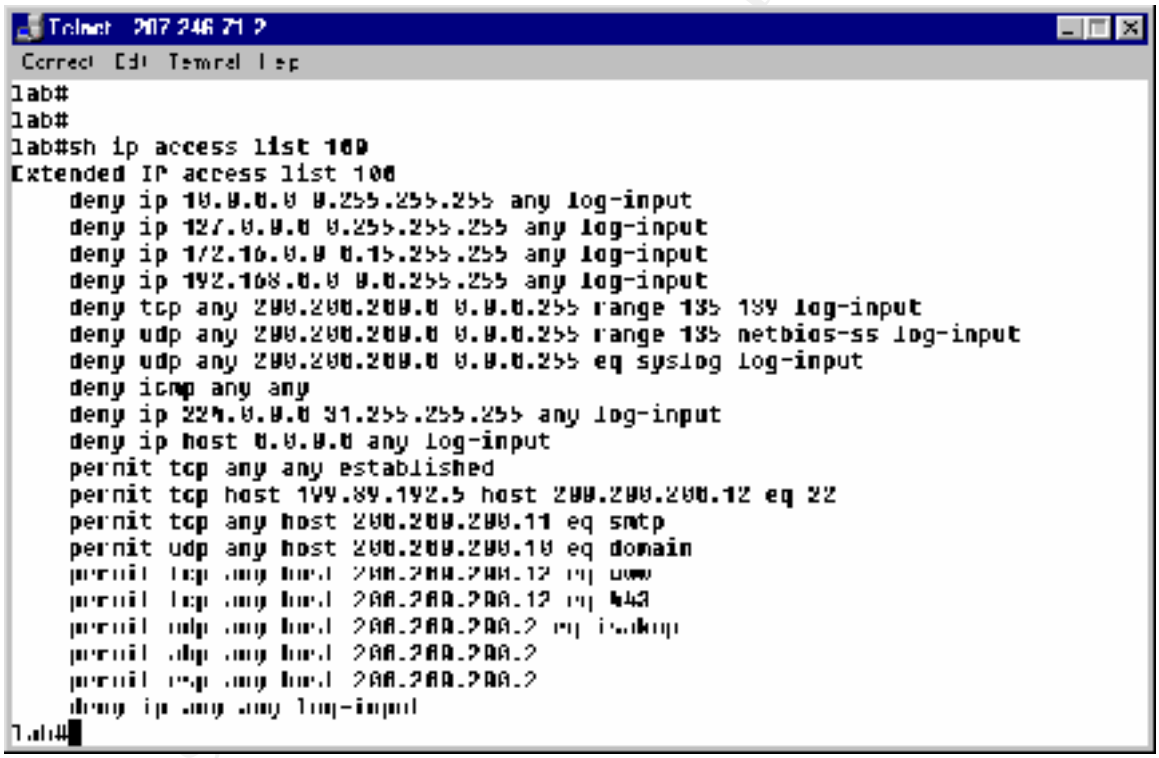
extended access-lists

access-list <list #> <permit/deny> <protocol> <opt. keyword host> <from ip address> < from inverse mask> <opt. “eq port #”> <opt. keyword host> <to ip address> <to inverse mask> <opt. “eq port #”>

After the access-lists are configured, they are applied to one or more interfaces on the router. Access-lists can be applied on traffic either inbound or outbound. Any interface can only hold one inbound and one outbound access-list.

An access-list can be readily tested via knowledgeable usage of a port scanning tool such as nmap. It is trivial to compare the output of nmap’s “found” ports with the list of those ports that we are trying to show.

The Internet router is a Cisco 2600 series router with one Serial and one Ethernet interface. The following image shows the access-list in place on the Serial interface (WAN interface) that was enabled with the “ip access-group 100 in” command.



Here is a breakdown of exactly what is happening with this configuration:

Lines 1-4) These lines are in place to block “spoofed” addresses from the RFC 1918 list of private addresses as well as the loopback network. These addresses aren’t supposed to be routable at all so they should never get to our network from the world so let’s just drop them.

Line 5-6) These lines are in place to block access to NetBIOS services from the Internet. This hardly needs to be explained… Windows File Sharing = BAD.

Line 7) Here we are simply blocking any inbound syslog messages. We shouldn't be seeing any and it might be interesting to see if someone tries to target our syslog server so let's log it.

Line 8) Let's block all icmp messages. This helps slow down people that are trying to map our network.

Line 9) Let's block all inbound multi-cast traffic. Management hasn't told us to allow them so let's just kill them here.

Line 10) Let's block traffic heading for the 0.0.0.0 broadcast.

Line 11) Let's permit any established traffic (e.g., started from the inside) to flow back into our network.

Line 12) Let's allow a single trusted host to use Ssh to connect to our web server in case remote administration is needed.

Line 13) Let's allow anyone to connect to port 25 on our email server in the DMZ

Line 14) Let's allow anyone to connect to port 53 on our external DNS server in the DMZ. This is UDP traffic only to help prevent Zone Transfers.

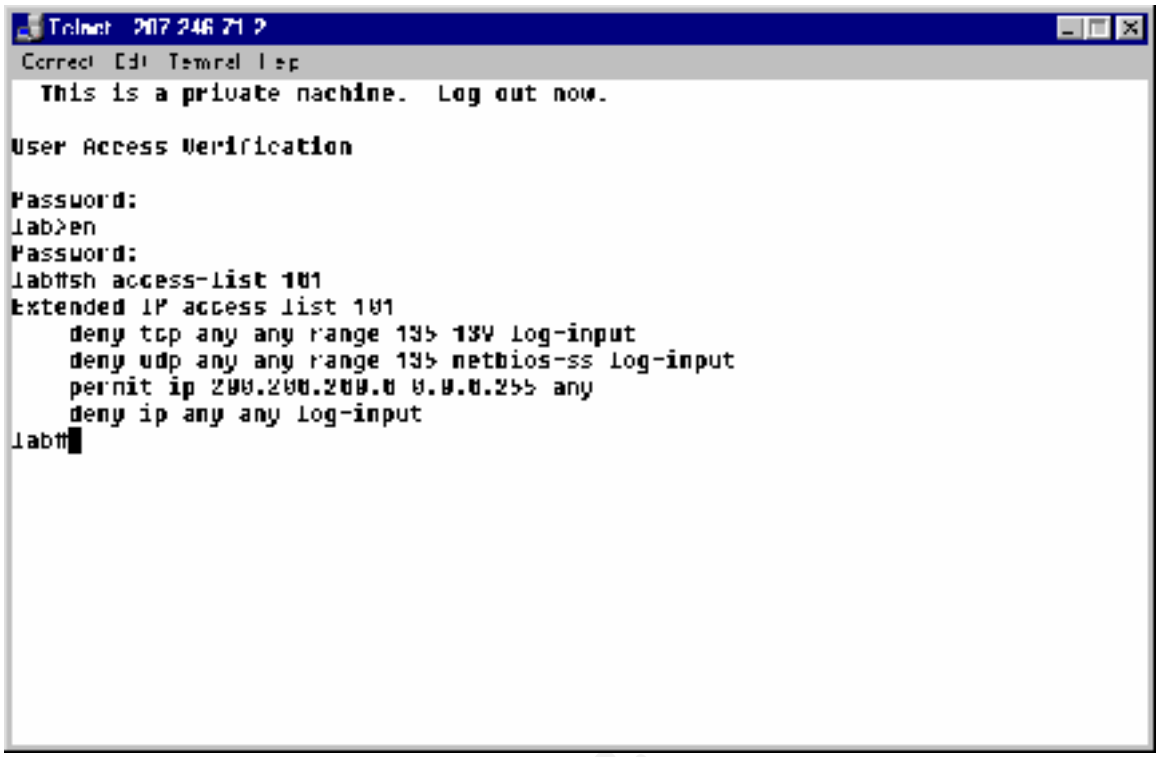
Lines 15-16) Let's allow the world to connect to either http or https on our web server in the DMZ

Lines 17-19) Let's allow inbound VPN traffic from anywhere to connect to the Firewall for VPN tunnels.

Line 20) Deny all other traffic.

It should definitely be noted that *all* denied traffic is logged to the syslog server via the "log-input" keyword at the end of each deny rule.

A much simpler rule-set is applied to outbound traffic at the Internet router. A graphic of it with accompanying explanation follows.



Line 1-2) Let's deny all outbound TCP and UDP Windows NetBIOS traffic. This traffic should not occur and is a significant security risk because it most likely indicates a Windows Share to the world or an internal person attempting to access one on the Internet which might open us up to litigation.

Line 3) We will allow any outbound traffic as long as it says it is coming from my network. In other words, let's not allow anyone to spoof traffic coming *from* us.

Line 4) Let's drop any other packets.

As before, all other attempted traffic is logged to the syslog server.

This access-list has been applied to the same interface as the previous access-list but has been applied with the "out" keyword in place of the "in" keyword. Notice also that there is a login banner that specifically notifies anyone attempting to log into the machine that this is a private router and they are not welcome.

One more access-list will be applied to this router to limit who is capable of actually connecting to the router itself. Here is the command snippet (it is not large enough to warrant a separate graphic).

```
access-list 1 permit 200.200.200.13
line vty 0 4
        access-class 10
        login
```

```
password 74bs82k0
exec-timeout 5
```

Here's what it does:

Line 1) This specifies exactly who is allowed to connect directly to me

Line 2) Enter into the "line vty" config section for all vty's (0-4)

Line 3) Apply the access-list to the vty's

Line 4) Enable login

Line 5) Set the password. This password will be encrypted later.

Line 6) Make the session disconnect after 5 minutes of inactivity.

Now that we are through with the access-lists, we have to apply some additional commands to the router to make sure that there are no brain-dead default security options set.

no cdp run

This command is used to turn off Cisco's built-in CDP protocol that is used to find and identify other Cisco devices on the network. This protocol gives out a surprising amount of information and is rarely useful once a network is setup.

no service finger

This command turns off the finger service on the Cisco router.

no ip http server

This disables the http server if it has been turned on. It is off by default on nearly every Cisco router above the 1000 series.

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

These commands disable the basic services like echo and chargen.

service password-encryption

This command is used to encrypt the passwords in the config file of the router to avoid them being displayed if anyone managed to get a copy of the router config. This is *not* strong encryption but is better than nothing.

service tcp-keepalives-in

This command generates keepalives on idle incoming network connections to help protect from orphaned sessions.

enable secret <password>

This should be used instead of enable password. The enable secret password is actually an MD5 hash and is much more secure.

access-list 2 permit 200.200.200.14
snmp-server community X7h6bsd2 RO 2
snmp-server community 07Hbad2m RW 2

These commands allow only the host 200.200.200.14 to connect via SNMP using the relatively non-intuitive SNMP community strings X7h6bsd2 and 07Hbad2m.

logging buffered
logging 200.200.200.13

These commands set where log messages are sent. They stipulate that messages are held in the buffer (until the buffer is filled and then it is aged out) and also to an external syslog server.

scheduler interval 500

This command helps make sure that the router can still handle process-level tasks even when being flooded with packets. It specifies that the router must handle these tasks at least every 500 milliseconds.

no ip source-route

This command simply drops any inbound packets that have the source-route flag set. There should be no reason why this should be allowed in a functioning network.

no ip directed-broadcast
no ip redirects
no ip proxy-arp

These commands are all done at the interface layer and do exactly what they appear to. They block incoming packets heading for broadcast addresses, icmp redirects, and requests for proxy-arp, respectively.

That should wrap up the Internet router configuration.

Now it's time to address the Internet Firewall. Since we're using a Cisco PIX 520, this should be pretty easy. By default, a PIX looks like a brick wall to the network because you have to specifically allow the traffic that you want as opposed to blocking what you don't want.

First things first, we need to name the interfaces on the PIX so we can easily access them. We will also go ahead and name the PIX itself. This is done with the following commands:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
hostname lab
```

We also need to set the telnet and enable passwords for the PIX. Both passwords are encrypted after you enter them so you will not be able to read them in the config.

```
passwd 2kjh23ds
enable password jKh42hd8
```

The following lines are used to actually inspect the following ports to make sure the data is as expected. For example, let's make sure that port 25 traffic really is smtp traffic. It should be noted that these are all on by default at least since PIX version 4.2. There is a bug with the ftp monitoring that has been fixed by either upgrading to the latest version or not having a conduit for ftp.

```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

The following lines protect from TCP SYN-flood attacks and fragmented packet attacks respectively.

```
floodguard
sysopt security fragguard
```

Now let's setup where the syslog messages go. While we are at it, let's specify the SNMP server and where the traps go.

```
logging host inside 192.168.1.13
snmp-server host inside 192.168.1.14
snmp-server community 7B%bcV09
snmp-server enable traps
```

Let's make sure that there are no routing protocols running on the PIX.

```
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
```

Finally, let's set the ip addresses for the various interfaces on the PIX.

```
ip address inside 192.168.1.1 255.255.255.0
ip address outside 200.200.200.2 255.255.255.0
ip address dmz 192.168.2.1 255.255.255.0
```

Now it is time to setup the NAT pools and the static mappings for all of the devices that need to be seen from the Internet.

```
global (outside) 1 200.200.200.20 netmask 255.255.255.0
global (outside) 1 200.200.200.21-200.200.200.250 netmask 255.255.255.0
global (dmz) 1 192.168.2.10 netmask 255.255.255.0
nat (inside)  1 0.0.0.0 0.0.0.0 0 0
nat (dmz) 1 192.168.2.0 255.255.255.0 0 0

static (dmz,outside) 200.200.200.10 192.168.2.10 255.255.255.255 0 0
static (dmz,outside) 200.200.200.11 192.168.2.11 255.255.255.255 0 0
static (dmz,outside) 200.200.200.12 192.168.2.12 255.255.255.255 0 0
static (inside,outside) 200.200.200.13 192.168.1.13 255.255.255.255 0 0
```

A little explanation: the global command is used to create the NAT pool itself and the nat command is used to determine who "matches" and can be NAT'ed. The static command is used to associate a public address with one of the addresses in the internal private address space.

Now let's build some conduits so that we know what will be allowed through. If we don't stipulate that traffic can come in, it won't. Due to this fact, we don't have to do anything to block ping from working at this level.

The syntax for the following commands is as follows:

conduit <permit/deny> <protocol> <optional keyword host> <dest. ip> <optional keyword "eq port#"> <optional keyword host> <source ip> <optional keyword "eq port#">

```
conduit permit tcp host 200.200.200.12 eq 80 any
conduit permit tcp host 200.200.200.12 eq 443 any
conduit permit udp host 200.200.200.12 eq 443 any
conduit permit tcp host 200.200.200.11 eq 25 any
conduit permit udp host 200.200.200.10 eq 53 any
conduit permit udp host 200.200.200.13 eq 514 any
conduit permit tcp host 200.200.200.14 eq 161 any
conduit permit udp host 200.200.200.14 eq 161 any
conduit permit tcp host 200.200.200.12 eq 22 host 199.89.192.5
```

The "any" keyword means, obviously, any host.

We still have to setup some routes since we disabled all routing protocols.

```
route outside 0.0.0.0 0.0.0.0 200.200.200.1 1
route inside 192.168.3.0 0.0.0.255 192.168.1.2 1
```

Now for the fun stuff. Let's setup the VPN information since we are using the PIX to terminate it. We will be using a pre-shared key and only allowing a specified host to connect (100.100.100.100).

```
ip local pool clients 10.0.0.1-10.0.0.100
access-list vendor_a permit ip 192.168.1.0 255.255.255.0 172.16.1.0
255.255.255.0
sysopt connection permit-ipsec
sysopt ipsec pl-compatible
crypto ipsec transform-set vendor esp-des esp-md5-hmac
crypto dynamic-map  roadwarrior 1 set transform-set vendor
crypto map vpn 1 ipsec-isakmp
crypto map vpn 1 set peer 100.100.100.100
crypto map vpn 1 set transform-set vendor
crypto map vpn 1 match address vendor_a
crypto map vpn 199 ipsec-isakmp dynamic roadwarrior
crypto map vpn client configuration address initiate
crypto map vpn client configuration address respond
crypto map vpn interface outside
isakmp enable outside
isakmp key Hd9.J~l3! address 100.100.100.100 netmask 255.255.255.255
isakmp key ab&8dNba address 0.0.0.0 netmask 0.0.0.0
isakmp identity hostname
isakmp client configuration address-pool local clients outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
```

The "crypto map" and isakmp key" sections should simply be repeated for additional VPN tunnels.

The last thing we need to configure is a way to log into the PIX via remote. This is *not* allowed by default. This is done with one simple command.

```
telnet 192.168.1.14 255.255.255.255 inside
```

Unlike some other firewalls, the order that any of these commands are entered does not matter in the least. (The obvious exception being that if you try to use a NAT pool that hasn't been defined yet or something similar, there will be a complaint.)

Assignment #3: Audit your security architecture

For the purposes of this assignment please assume that you have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises, a electronic commerce facility that is the largest supplier of electronic fortune cookie sayings in the world. The firewall analyst has set their firewall up according to their base + recommended enhancements security policy that happens to mirror your assignment 1 security policy exactly. Your assignment is:

- *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 costs and level of effort. Identify risks and considerations.*
- *Implement the assessment. Validate that the firewall or perimeter router is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Screenshots when possible should be included in your report.*
- *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: Assignment 3 should be primarily focused on VISA requirement number 1, "Install and maintain a working network firewall to protect data accessible via the Internet." and your base + recommended security policy. Credit towards honors status will be given to students that are able to design an audit that can test all or a good deal of the VISA requirements.

Network security audits have to, at a minimum, be performed both from the inside of the network and from outside of the network. With the layout that we have for GIAC Enterprises, we will also need to run nmap scans from the DMZ to see if we have more access from there than we want.

The timing of the audits is also important. In the case of internal audits, they should be scheduled whenever new servers or services are put in, whenever patches are applied, and, barring any changes, on a recurring basis to make sure that something hasn't changed without your notice.

Internal Audits:

For the sake of this document, internal audits are merely audits that are performed by GIAC Enterprises staff, whether they be from the Internet or local origin.

Several different people should also perform audits. In an attempt to keep a fresh eye open for problems, the System Administrator that is responsible for a given machine should not be the one to audit that same machine if at all possible. Also, peer reviews should be conducted on the findings to determine what problems actually exist in the mass of data that is collected in any audit. Note that these audits are completely separate from the day-to-day monitoring of syslog and IDS logs. This day-to-day part will be handled later in the paper.

Port scans should be run at varying times of the day as soon after install of the network as possible in an attempt to get a "feel" for how the network should look. After that baseline has been established, these scans should be run no less than twice a month to make sure that nothing new has popped up. These scans should reveal any listening services or, barring that, at least machines that report themselves in an up state. These

scans should be run from outside of the Internet Router in order to test as much as possible. We can play with the options that Nmap has in an effort to bypass the access-lists on the router and firewall and also in an effort to remain undetected. Possible options that might produce interesting results are: -P0 (to get around the lack of icmp), -sF (FIN scan, might get around some rules), -sU (UDP port scan), -T Paranoid (in an attempt to get past the IDS… this will cause the scan to take a *long* time because of the slow scan rate. Similar scans should also be run from the DMZ to see if perhaps more access than necessary is available to machines in that area to the internal network. Once again, these scans should be run at varying times of the day. One caveat: particularly intensive scans should be scheduled for off-peak hours to reduce the costs of accidental crashing of machines.

While these scans are being run, the IDS systems should be monitored to make sure that they are responding in the desired fashion.

Another simple yet effective audit technique that should be employed is to simply put a sniffer in each of the different networks. Apply a ruleset slowly that tells the sniffer to ignore the traffic that you *expect* to have present and then watch what remains. This might turn up mystery packets that require more in-depth research. An excellent sniffer for this type of work is either the standard unix tcpdump or the freeware Snort utility with it's IDS functionality disabled.

Service specific audits should also be performed. For example, using nslookup or dig we can try to perform Zone Transfers off of our external DNS server. We can also attempt to use our external mail server as a mail relay agent. If either of the above tests succeeds, we obviously have a misconfiguration that needs to be addressed.

Finally, user passwords should be routinely checked via utilities like l0phtcrack for Windows NT or Crack for Unix.

Daily Review of Log Files:

Log files should be reviewed on a daily basis. This is an extremely tedious task and, in an effort to prevent people from making mistakes due to boredom, the task should be rotated on a per server basis between the qualified personnel. Further, any discrepancies found in the log files should be flagged to be reviewed by co-workers as soon as possible. Finally, all log files should be archived to write-once media to preserve it for possible future research.

External Audit:

For the purposes of this document, an external audit is any audit that is performed by non-GIAC Enterprises staff at the request of said staff. Every attempt should be made to make sure that the auditing company has a reputable presence and demonstrated experience in the field. Deliverables from the audit should include a complete mapping of the network with a breakdown of any vulnerabilities found on specific machines.

An external audit should be performed no less than once per calendar year. This audit should cover both external and internal penetration testing. During the external penetration testing phase, the internal security staff should be completely unaware that a legitimate audit is going on unless they can find it out from logfiles.

Recommendations for Improving the Security of this Network:

1) The Internet router should be configured to only allow Ssh access for configuration purposes. The Cisco 2600 series router now supports this functionality. This will prevent anyone from snooping the administrative passwords on the wire.
2) The http and https server should be configured to be on two separate machines. This will isolate the "secure" traffic from the "insecure" traffic a bit more.
3) The VPN configuration on the PIX currently will allow anyone to use the "roadwarrior" set if they have the proper password regardless of from where they are connecting. Consider tightening this down by removing this generic template.
4) Look for a replacement for syslog that can tighten down the security a little more by specifying on the server side which hosts it will accept syslog messages from. Inbound syslog messages from the internet are already blocked but this might be possible to get around.
5) Invest in RSA's token technology to help eliminate the weakness of relying upon user passwords for security.
6) Consider throwing an application proxy firewall into the mix for increased security to the internal network

List of Utilities and Related Web Sites:

Snort can be found at www.snort.org
L0phtCrack can be found at www.l0pht.com
Tripwire can be found at www.tripwire.com
Nmap can be found at www.insecure.org
Ssh can be found at www.ssh.com
OpenSSH can be found at www.openssh.com
Several good utilities can be found at www.foundstone.com/resources/tools.html

An excellent article on configuring Cisco routers for security resides at:
www.cisco.com/warp/public/707/21.html
Cisco maintains their security advisories page at:
www.cisco.com/warp/public/707/advisory.html
Microsoft can be found at www.microsoft.com
RSA can be found at www.rsasecurity.com

Numerous excellent sites exist for listing new vulnerabilities and discussing old ones:
www.securityfocus.com
www.sans.org
www.wiretrip.net (This is RainForestPuppy's site)