Global Information Assurance Certification Paper

GIAC LevelTwo Firewalls, Perimeter Protection, and VPNs
Practical Assignment for GCFW Certification.

Submitted By:
Mike Rudenko, Jr.

GCFW PRACTICAL INSTRUCTIONS

Assignment 1 - Security Architecture (25 Points)

Define a security architecture for GIAC Enterprises, a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. 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).

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.

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 ruleset, 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. Keep in mind you are an E-Business with 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 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".

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 Border Router and 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 costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Border Router and Primary Firewall are 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.

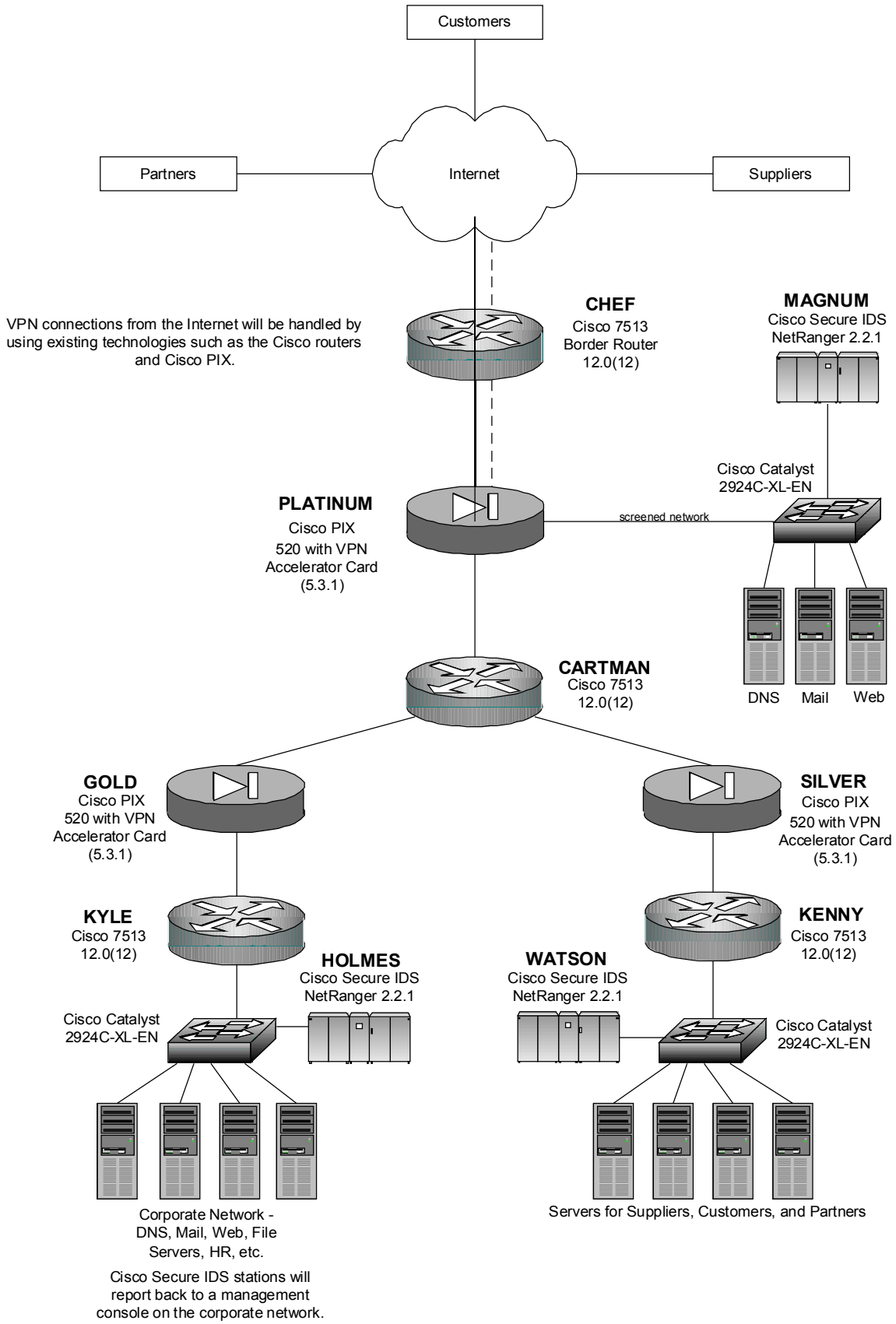
Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

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 paste 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.

ASSIGNMENT 1 – SECURITY ARCHITECTURE



Border router 'CHEF':

The Cisco 7513 running 12.0(12) code will be set up with ACL's, which filter traffic destined for the most commonly probed and attacked ports on the internal network, as well as other pre-defined ports and services as determined by our security policy. This "pre-filtering" of traffic is to keep unnecessary traffic off of the network backbone. Telnet access from this router back through the firewall to inside hosts is denied. The access lists on this router will be adjusted accordingly depending on inbound traffic, this can be done to take some load off of the PIX firewall. This router is connected to the Internet via OC-12 and to the Cisco PIX 520 PLATINUM via 100BaseTX interface.

Cisco PIX 520 'PLATINUM':

Running with the latest code 5.3.1, a VPN Accelerator card, the maximum amount of RAM and Flash memory, this unit will have three interfaces. One interface connects it to the border router CHEF(100BaseTX) and the second interface connects it to the service network (100BaseTX) where the external DNS, Email, and Web servers reside, and the third interface connects it to the edge router of the internal network (100BaseTX). This firewall will secure the screened network to make sure DNS, mail, and web services operate smoothly as well as making sure customers have a secure platform on which to purchase online fortunes by only allowing authorized traffic. It will also aid in securing the rest of the internal network as defined in the security policy. All database applications for customers, suppliers, and partners will reside in the server farm as indicated on the diagram. The VPN Accelerator Card (VAC) for the PIX 520 series provides high-performance, tunneling and encryption services suitable for site-to-site and remote access applications. This hardware-based VPN accelerator is optimized to handle the repetitive but voluminous mathematical functions required for IPsec. Offloading encryption functions to the card not only improves IPsec encryption processing, but also maintains high-end firewall performance. This firewall will terminate the VPN traffic from partners, suppliers, and customers.

Cisco 7513 'CARTMAN':

This edge router, running 12.0(12) code, will route traffic between all segments of the network based on the company's security policy defined later in this document. This router is connected to the firewalls GOLD, PLATINUM, and SILVER via 100BaseTX connections. This router adds an additional level of security between segments as additional ACL's can be applied to it, a defense in depth strategy.

Cisco PIX 520 'GOLD':

Running with the latest code 5.3.1, a VPN Accelerator card, the maximum amount of RAM and Flash memory, this unit will have one interface connected to the edge router CARTMAN (100BaseTX), and the other interface connected to router KYLE (100BaseTX). It will be this firewall that secures the corporate network from the other network segments, again, based on the security policy. This firewall will allow DNS queries to pass from the internal DNS servers, as well as mail and web traffic.

Cisco PIC 520 'SILVER':

Running with the latest code 5.3.1, a VPN Accelerator card, the maximum amount of RAM and Flash memory, this unit will have one interface connected to the edge router CARTMAN (100BaseTX), and the other interface connected to router KENNY (100BaseTX). It will be this firewall that secures the network segment that contains the servers for GIAC Enterprises suppliers, partners, and customers based on the security policy.

Cisco 7513 'KYLE':

This 7513 running code 12.0(12) will route traffic to and from the corporate network of GIAC Enterprises and provide an addition level of filtering and security in conjunction with he PIX firewall on its upstream side. The 7513 is connected to the PIX 'GOLD' via 100BaseTX, and connected to a Cisco Catalyst 2924C-XL-EN switch via 100BaseFX.

Cisco 7513 'KENNY':

This 7513 running code 12.0(12) will route traffic to and from the suppliers, customers, and partners servers and provide an additional level of filtering and security for this segment if needed. It is connected to a Catalyst 2924C-XL-EN via 100BaseFX and connected to the upstream PIX via 100BaseTX.

Cisco Secure IDS NetRanger MAGNUM,HOLMES,WATSON and Catalyst switches:

The three IDS stations will report findings back to a management console on the corporate network and will be monitoring traffic inbound and outbound from the respective segments as shown on the diagram. Traffic will be compared to known signatures of illegitimate packets and will be handled accordingly based on policy. Besides continually monitoring network traffic, the IDS systems can be used to aid in the verification of the router access lists and firewall policies. Configuration choices and what these devices do is very flexible, they can issue RESETS for example, or simply log the traffic. Business needs will always come first, and security will be tightened as much as possible. The Catalyst switches are put in place to handle extra capacity if and when it is needed. Lastly, the switches serve as a point at which to install additional monitoring equipment such as LAN sniffers, etc.

All PC's and Servers

Outfitted with the latest security patches and hardened operating systems. Audited frequently.

* All devices that are capable will be sending logs to a syslog server. Telnet access to all network devices will only be allowed from secure, trusted hosts within the corporate network. This network architecture is a Defense in Depth type, where, if one layer fails, another will be there as a backup.

ASSIGNMENT 2 – SECURITY POLICY

In this section, we will discuss access lists, router security, and configuration of the VPN.

Security Policy on border router CHEF:

In this section, we list 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. The following list will be used a base policy, it is what CERT and SANS recommend be blocked. ACL's created from this list will be applied to the Internet side interface of the border router CHEF for both inbound and outbound traffic. The following list can be viewed at this URL: http://www.sans.org/infosecFAQ/firewall/blocking_cisco.htm Information and explanatory text are at the end of this section. Telnet access to ALL GIAC router is allowed only from certain trusted internal hosts. Console access only by admins.

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

Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp) **NOTE: telnet, ssh, and ftp will allowed only to certain hosts which are needed to carry out business functions.** Telnet is not secure and it can be sniffed. FTP can potentially carry dangerous payloads and like telnet is only allowed to certain hosts. The firewall will do content checking to prevent deadly payloads.

RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp) Too many exploits to mention here, so we will block these ports.

NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – earlier ports plus 445(tcp and udp) These are potential disasters waiting to happen, there is no need for these ports to be accessed via the Internet to the internal network.

X Windows -- 6000/tcp through 6255/tcp We are not using X-Windows, so we block these. These are dangerous services to be running on unprotected UNIX machines.

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) Zone transfers are allowed only to known internal DNS servers.

Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp). **POP and SMTP will be allowed to only specific addresses.** Mail is only sent from corporate network mail servers to mail servers in the screened network, then out to the Intertnet.

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.)Only screened net web servers are accessed.

"Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)These are unused and can be abused, they will be blocked.

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) **NOTE: BGP will NOT be blocked as the border router uses this protocol.** Again, these ports should not be accessed from the Internet due to abuse.

ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages **except** "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.) **NOTE: ICMP will NOT be blocked at this time BUT will be rate limited at the border router to protect against ICMP floods.**

Shown below is the syntax of the extended access list, and then the access lists themselves that will be applied to the Internet interface side of Cisco router CHEF with supporting text. The syntax for Cisco extended access lists is as follows:

access-list *access-list-number or name* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log | log-input**]

---outbound traffic matched against this access list----------
access-list 108 permit ip x.x.0.0 0.0.255.255 any (allows our network address out)
access-list 108 deny ip any any (denys spoofed addresses)

---inbound traffic matched against this access list----------
access-list 126 permit tcp any certain.giac.host.addresses eq 21 (permits ftp to certain hosts)
access-list 126 permit tcp any certain.giac.host.addresses eq 22 (permits ssh to certain hosts)
access-list 126 permit tcp any certain.giac.host.addresses eq 23 (permits telnet to certain hosts)
access-list 126 permit udp any host giac.external.dns.server eq 53 (permits outside DNS queries)
access-list 126 permit tcp ext.sec.dns.server eq 53 giac.ext.dns.server eq 53 (permits zone transfers)
access-list 126 permit tcp any host giac.external.web.server eq 80 (permits web traffic)
access-list 126 permit tcp certain hosts customer.supplier.partner.webserver eq 80 (permits web traffic)
access-list 126 permit tcp giacs.isp.bgptalking.router giac.border.router.chef eq 179 (permits bgp updates with upstream ISPs router)
access-list 126 permit tcp any giac.external.web.server eq 443 (permits SSL connections to web server)
this above line entry will be duplicated for customer, supplier, and partner addresses.
access-list 126 deny ip 0.0.0.0/8 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 1.0.0.0/8 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 23.0.0.0/8 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 31.0.0.0/8 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 64.0.0.0/3 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 96.0.0.0/4 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 112.0.0.0/5 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 120.0.0.0/6 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 124.0.0.0/7 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 127.0.0.0/8 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 128.0.0.0/24 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 191.255.0.0/16 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 192.0.0.0/16 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 197.0.0.0/8 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 201.0.0.0/8 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip 223.255.255.0/24 any log (denying reserved addresses and ones we don't want coming in)
access-list 126 deny ip any giac.int.network.address 0.0.255.0 log (denying our internal address)
access-list 126 deny ip 10.0.0.0 255.0.0.0 any log (denying private addresses)
access-list 126 deny ip 172.16.0.0 255.255.0.0 any log (denying private addresses)
access-list 126 deny ip 192.168.0.0 255.255.0.0 any log (denying private addresses)
access-list 126 deny udp any any range 1 19 log (denying small services udp)
access-list 126 deny tcp any any range 1 19 log (denying small services tcp)
access-list 126 deny tcp any any eq 21 log (denying ftp not permitted above)
access-list 126 deny tcp any any eq 22 log (denying ssh not permitted above)
access-list 126 deny tcp any any eq 23 log (denying telnet not permitted above)
access-list 126 deny tcp any any eq 37 log (denying time not permitted above)
access-list 126 deny udp any any eq 37 log (denying time not permitted above)

```
access-list 126 deny udp any any eq 53 log (denying dns not permitted above)
access-list 126 deny tcp any any eq 53 log (denying dns not permitted above)
access-list 126 deny udp any any eq 69 log (denying tftp)
access-list 126 deny tcp any any eq 79 log (denying finger)
access-list 126 deny tcp any any eq 80 log (denying web not permitted above)
access-list 126 deny udp any any eq 111 log (denying rpc)
access-list 126 deny tcp any any eq 111 log (denying rpc)
access-list 126 deny tcp any any eq 119 log (denying nntp)
access-list 126 deny tcp any any eq 123 log (denying ntp)
access-list 126 deny udp any any range 135 139 log (denying net-bios)
access-list 126 deny tcp any any range 135 139 log (denying net-bios)
access-list 126 deny tcp any any eq 143 log (denying imap)
access-list 126 deny tcp any any range 161 162 log (denying snmp)
access-list 126 deny udp any any range 161 162 log (denying snmp)
access-list 126 deny udp any any eq 389 log (denying ldap)
access-list 126 deny tcp any any eq 389 log (denying ldap)
access-list 126 deny tcp any any eq 443 log (denying ssl not permitted above)
access-list 126 deny udp any any eq 445 log (denying win2000 file sharing)
access-list 126 deny tcp any any eq 445 log (denying win2000 file sharing)
access-list 126 deny udp any any eq 514 log (denying syslog)
access-list 126 deny tcp any any range 512 515 log (denying rlogin)
access-list 126 deny tcp any any eq 540 log (denying uucpd)
access-list 126 deny tcp any any eq 1080 log (denying socks)
access-list 126 deny tcp any any eq 2000 log (denying open windows)
access-list 126 deny udp any any eq 2000 log (denying open windows)
access-list 126 deny tcp any any eq 2001 log (denying Cisco Aux ports)
access-list 126 deny udp any any eq 2049 log (denying nfs)
access-list 126 deny tcp any any eq 2049 log (denying nfs)
access-list 126 deny tcp any any eq 4001 log (denying Cisco Aux port)
access-list 126 deny tcp any any eq 4045 log (denying Lockd)
access-list 126 deny udp any any eq 4045 log (denying Lockd)
access-list 126 deny tcp any range 6000 6255 any log (denying XWindows)
access-list 126 deny tcp any any eq 8000 log (denying high order http ports)
access-list 126 deny tcp any any eq 8080 log (denying high order http ports)
access-list 126 deny tcp any any eq 8888 log (denying high order http ports)
access-list 126 permit ip any any
```

The 108 access list, will allow all IP traffic outbound to the Internet only from valid source addresses within our network range (Class B address with a Class C mask). It will deny all other traffic. The 126 access list will be applied to all traffic coming into GIAC Enterprises network from the Internet. The services and protocols are shown above in the security policy. Both access lists are applied to the interface by entering enable mode on the router by typing in the enable password, then typing **conf t** to get in configuration mode, then enter what interface you wish to configure, in this case, the OC-12 interface.

```
CHEF>en
Password:xxxxxxxxx <enter>
CHEF# conf t
CHEF(config)#int OC-12 1/0
CHEF(config-if)#access-group 108 out
CHEF(config-if)#access-group 126 in
```

Shown below, is what the interface configuration will look like after both access lists 108 and 126 have been applied. Only one access list per direction per interface is allowed. Certain other configuration parameters have been excluded from view due to relevance i.e.: BGP.

```
CHEF# sho int OC-12 1/0

interface OC-12 1/0
description GIAC Enterprises Internet Connection
ip address x.x.1.254 255.255.255.0
ip access-group 108 in
ip access-group 126 out
no ip redirects
no ip directed-broadcast
```

no ip proxy-arp
no ip unreachables

Once the access lists have been applied to the correct interface, and viewed or proper application to that interface, their effectiveness can be tested by issuing a **sho ip access-list** command:

CHEF# sho ip access-list 126
access-list 126 deny tcp any any eq 21 log (2350930660 matches)
access-list 126 deny udp any any eq 69 log (1200983 matches)
access-list 126 deny tcp any any eq 79 log (33460 matches)
access-list 126 deny tcp any any eq 80 log (9988665 matches)
access-list 126 permit ip any any (234523366 matches)

This is only a portion of what would be displayed if this command where issued. Only a few lines shown here, but you will see how many packets have been matched to each entry meaning the router is permitting or denying traffic based on the access list. Specifically, we see here a fair amount of ftp, tftp, finger, and web traffic that has been dropped by the router. Also, an IDS box, like Cisco's NetRanger can be placed behind the router to see what traffic is coming through to test the effectiveness of the access lists.

***Note the following additional statements that have been applied to this and ALL router interfaces within GIAC Enterprises and what they do. These statements have been configured into the routers to secure the routers themselves. Certain services have been turned off on the router to prevent them from being exploited:

no ip redirects - The Cisco router sends an ICMP Redirect message to the originator of any datagram that it is forced to resend through the same interface on which it was received, since the originating host could presumably have sent that datagram to the ultimate destination without involving the router at all. The router ignores Redirect messages that have been sent to it by other routers. We will not be sending redirects, so we disable this service.

no ip directed-broadcast - This prevents your network from being used as a smurf amplifier, you need to filter packets sent to the broadcast address of your network. This is very important as we have seen in the news lately. You don't want your site being a smurf reflector.

no ip proxy-arp - By default, IOS enables proxy ARP on all interfaces. Since we don't need the service, we will disable it.

no ip unreachables - By default, when an access list drops a packet, the router returns a type 3, code 13 ICMP (administratively prohibited) message. This allows potential attackers to know that the router implements access list filters. Also, most UDP scans rely on the target sending back unreachable messages. To thwart UDP scans we can prevent the router from sending any ICMP type 3 (unreachable).

no mop enabled – disables the maintenance protocol. We aren't doing DECnet.

The following statements are applied to this, and ALL GIAC routers in global configuration mode:

no ip subnet-zero – disables the use of subnet zero addresses and routing updates.
no ip source-route – disables source routing.
no ip finger – disables finger service.
no ip bootp server – stops bootp requests
no ip http server – turns off the router web interface
no snmp – turns off snmp service on the router

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

The follwing banner message is applied to all devices. It appears upon telnet, ftp, and any type of remote access:

This system is for the use of authorized users only.

Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

A final word on access lists – Traffic is matched to the line in an access list from top to bottom, in an order dependant way, so when a packet enters the router it is either permitted or denied based on what line in the list it matches. If the packet does not match any line in the list, then the implicit 'deny all' at the end handles it accordingly if there is no 'permit ip any any' before it. The access lists should be written to block out bulk traffic first, then move on to more specific traffic types.

Tips, Tricks, and Gotchas:

- If you intend to deny all unmatched packets, it is better to use an explicit deny and log it, that way you know immediately if there is an error in an access-list.

-Never write access lists to NVRAM until you have thoroughly tested them.

-Once the ACL has been proven to work DON'T forget to issue a 'write mem' command to save it incase the router gets reloaded.

-You can't just add lines to a extended numbered access list, you have to re-write the whole list.

-Conduit statements on the PIX firewall -- the source and destination addresses are placed in different postions within the command syntax, different from the ACL.

Security Policy on Cisco PIX 520 with VPN Accelerator Card PLATINUM

A Virtual Private Network is a way of employing encryption and integrity protection so that a public network such as the Internet can be used for data transport, as if it were a private network. That reduces the cost significantly over leased circuits and is very secure. The traffic that traverses this VPN is encrypted, data integrity is protected, and encapsulated into new packets which are sent across the Internet to a device that tears the packet apart and does does the decrypting. IPSec is becoming the standard protocol used by VPN devices to communicate with each other. IPSec is actually a collection of protocols used to wrap around the data sent between two devices. The IPSec protocols are the Internet Key Exchange(IKE), Authentication Header(AH), and the Encapsulating Security Protocol(ESP). IKE is used to negotiate which encryption and authentication methods will be used between two IPSec devices and how long they will last. These negotiated methods between devices are called Security Associations (SA). After each device has been properly identified, either via a pre-shared key or public key exchange, the IKE negotiations begin.
IPSec supports two encryption or authentication modes: Transport and Tunnel. Transport mode encrypts and authenticates only the payload of the IP packet, leaving the header untouched. Tunnel mode encrypts and authenticates both the header and the payload giving the added benefit of protecting the real source and destination of the packet. If the use of AH is negotiated during the IKE process the data transmission can be protected using these methods - data origin authentication, connectionless integrity and protection against replay attacks. Please note that the data payload is not encrypted when using AH. If ESP is negotiated, then the following security services are offered: payload encryption, data origin authentication, connectionless integrity, protection against replay attacks, and limited traffic flow confidentiality. The VPN Accelerator Card, encrypts data using the 56-bit Data Encryption Standard (DES) or 168-bit 3DES algorithms at speeds up to 100 Mbps. A PIX equipped with a VAC supports as many as 2,000 encrypted tunnels for concurrent sessions with mobile users or other sites. In addition to encryption, the card handles a variety of other IPsec-related tasks—hashing, key exchange, and storage of security associations—which free the PIX main processor and memory to perform other perimeter security functions.

- Encryption—DES and 3DES encryption are very CPU intensive, potentially impacting firewall performance in high-throughput configurations. The VAC makes it possible to send DES or 3DES encrypted data at high speed while still providing the full range of perimeter security services available from the Cisco Secure PIX Firewall.
- Authentication—RSA and Diffie-Hellman are CPU-intensive protocols that are used when a new IPsec tunnel is established. RSA authenticates the remote device while Diffie-Hellman exchanges keys that will be used for DES or 3DES encryption. The VPN Accelerator Card implements these protocols in specialized hardware ensuring fast tunnel setup and high overall encryption throughput.
- Tunneling—The PIX and VAC support IPsec tunneling protocol enabling high-performance, flexible network designs for both remote access and site-to-site VPNs. Site-to-site solutions can be designed with PIX or combinations of PIX with Cisco VPN appliances or VPN-enabled multi-service routers. Remote access solutions can utilize Cisco's VPN client or other 3rd party clients supporting the IPsec tunneling protocol.

The security policy on this device will be fairly straight forward, for the traffic destined to and from the screened network. This PIX will also handle the VPN connections coming in from partners, resellers, customers, and administrators from the Internet through the router CHEF. The Cisco Firewall has IPSEC encryption built-

in, permitting both site-to-site and remote access VPN deployments, and operate on a hardened operating system focused on protecting both the security of the device and the networks its protects. In addition to having the ability to be managed by the PIX Configuration Manager, the Cisco Secure PIX Firewalls also may be centrally managed by the Cisco Secure Policy Manager, which can manage up to 500 PIX Firewalls, Cisco Secure Integrated Software deployments, and site-to-site VPN installations. For more information on why GIAC Enterprises chose PIX, go here:

http://www.cisco.com/warp/customer/cc/pd/fw/sqfw500/tech/nat_wp.htm

As a dedicated, stateful appliance, the Cisco Secure PIX Firewall is easy to install and highly stable. The Cisco Secure PIX Firewall Series is cost effective both in cost and maintenance, and provides unmatched security and performance.

For the screened network, the PIX will only allow DNS, mail, and Web traffic to access the servers on the screened network for the purpose of viewing the company's web page, sending email, and resolving DNS queries. Secondly, the PIX will allow the DNS, mail servers, and a few administrative hosts on the corporate network access the screened network as well. All other traffic to the screened network will be denied.

Here are the configuration examples from the PIX and it's VPN portion configuration and explainatory text:

Interfaces on the PIX:

The interfaces on the PIX need names, so, we name them:

```
Nameif Ethernet0 outside security 0
Nameif Ethernet1 screened-network security 50
Nameif Ethernet2 inside 100
```

The interfaces also need addresses:

```
ip address outside x.x.outside.interface 255.255.255.0
ip address inside x.x.inside.interface 255.255.255.0
ip address screened-network x.x.screened.network 255.255.255.0
```

The static commands map inside and outside addesses to the screened network. Since traffic will be coming from a less secure interface to a more secure one, we need to use **static** statements:

```
static (screened-network,outside) giac.screened.net.address netmask 255.255.255.0 0 0
static (outside,inside) outside.addresses.from.internet giac.int.net.address netmask 255.255.255.255 0 0

conduit permit tcp host giac.ext.dns.server eq domain any
conduit permit tcp host giac.ext.mail.server eq smtp any
conduit permit tcp host giac.ext.web.server eq 80 any
conduit permit tcp host giac.ext.web.server eq 443 partner.address
conduit permit tcp host giac.ext.web.server eq 443 customer.address
conduit permit tcp host giac.ext.web.server eq 443 supplier.address
```

Access lists decide who and what get through:

```
access-list 111 permit tcp any host giac.ext.dns.server eq domain
access-list 111 permit tcp any host giac.ext.mail.server eq smtp
access-list 111 permit tcp any host giac.ext.web.server eq 80
access-list 111 permit tcp giac.partner.net.address host giac.ext.web.server eq 443
access-list 111 permit tcp giac.supplier.net.address host giac.ext.web.server eq 443
access-list 111 deny ip any any
```

The access list and conduit statements below insure that only web, mail, and DNS traffic are allowed to pass. All other traffic destined for the screened network is implicitly denied.

The following shows the syntax for Cisco PIX conduit statements:

conduit permit | **deny** *protocol global_ip global_mask* [*operator port* [*port*]] *foreign_ip foreign_mask* [*operator port* [*port*]]

The VPN configuration:

IPSec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPSec will be especially useful for implementing virtual private network and for remote user access through dial-up connection to private networks. A big advantage of IPSec is that security arrangements can be handled without requiring changes to individual user computers.

IPSec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

GIAC Enterprises wishes to take advantage of ESP's authentication and encryption feature rather that just the authentication piece that AH has to offer.

Cisco recommends the following order when configuring your IPSec:

If you will implement interoperability with a CA, Cisco recommends that you perform your IPSec configuration in the following order:

1. CA
2. IKE
3. IPSec
4. (Optional) IKE Extended Authentication---applies only if you are configuring user authentication for remote VPN clients.
5. (Optional) IKE Mode Configuration---applies only if you are configuring dynamic IP addressing for remote VPN clients.

If you will not implement interoperability with a CA, and you will implement IKE, Cisco recommends that you perform your IPSec configuration in the following order:

1. IKE
2. IPSec
3. (Optional) IKE Extended Authentication---applies only if you are configuring user authentication for remote VPN clients.
4. (Optional) IKE Mode Configuration---applies only if you are configuring dynamic IP addressing for remote VPN clients.

GIAC PIX:

The following configuration lines define the crypto map transforms, specify ISAKMP access, map the match to the access list (both use ID 80 to be associated), set the tunnel peer to be the outside interface IP address of the remote PIX firewall, and apply the crypto map to the outside interface.

```
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map newmap 10 ipsec-isakmp
crypto map newmap 10 match address 100
```

```
crypto map newmap 10 set peer remote.pix.firewall.address
crypto map newmap 10 set transform-set myset
crypto map newmap interface outside
```

This portion of the configuration defines the ISAKMP policy:

```
isakmp enable outside
isakmp key cisco123 address remote.pix.firewall.address netmask 255.255.255.255
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 1000
```

Configuration on remote PIX firewall:

The following configuration lines define the crypto map transforms, specify ISAKMP access, map the match to the access list (both use ID 80 to be associated), set the tunnel peer to be the outside interface IP address of the GIAC PIX firewall, and apply the crypto map to the outside interface.

```
crypto ipsec transform-set myset ESP-Des esp-md5-hmac
crypto map newmap 10 ipsec-isakmp
crypto map newmap 10 match address 100
crypto map newmap 10 set peer giac.pix.firewall.address
crypto map newmap 10 set transform-set myset
crypto map newmap interface outside
```

This portion of the configuration defines the ISAKMP policy:

```
isakmp enable outside
isakmp key cisco123 address 192.68.0.10 netmask 255.255.255.255
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 1000
```

Go here for a great IPSec overview:
http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/prodlit/ipsec_ov.htm

ASSIGNMENT 3 – AUDIT YOUR SECURITY ARCHITECTURE

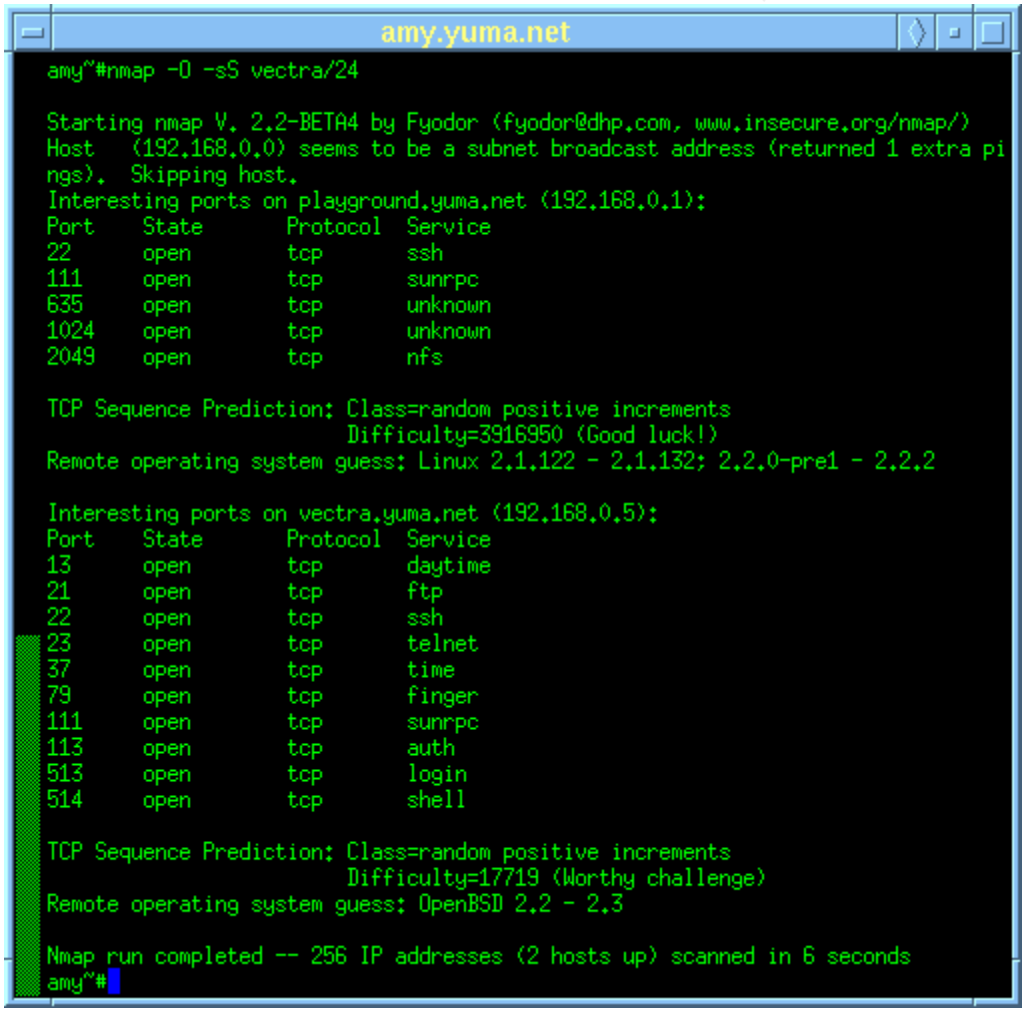
Plan the Assessment

Auditing our security architecture will establish whether or not the security policy that we have established and implemented actually works. The security assessment of GIAC Enterprises will take place on a weekend, after normal business hours, and after mission critical systems have been backed up. GIAC Enterprises will hire two security analysts at a cost of $175/per hour per analyst. Estimated time to complete the assessment is 8 hours for the assessment itself and another 24 hours to write up the security evaluation. Total cost is estimated at $2,800 for the assessment and $4,200 for one engineer to write up the assessment, so a total of $7,000.

Implement the Assessment

We need to determine whether our border router and firewall are allowing the proper traffic to pass in and outbound and whether the two devices are filtering the traffic we want to disallow. The tools that will be used to perform this assessment are:

Nmap – http://www.insecure.org/nmap



Nmap is designed to scan large networks to determine which hosts are up and what services they are offering. Nmap supports a large number of scanning techniques such as: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, and Null scan. Nmap also offers a number of advanced features such as remote OS detection via TCP/IP fingerprinting, stealth scanning, dynamic delay and retransmission calculations, parallel scanning, detection of down hosts via parallel pings, decoy scanning, port filtering detection, direct (non-portmapper) RPC scanning, fragmentation scanning, and flexible target and port specification.

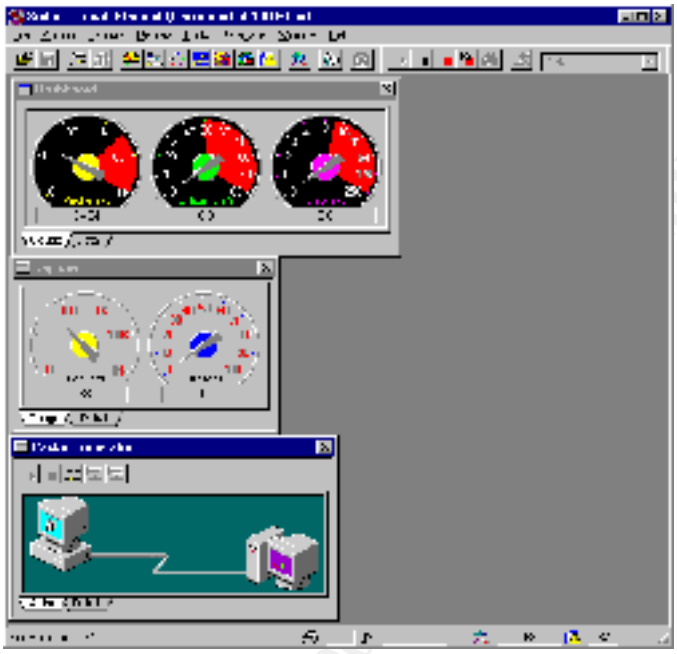
Fport – http://www.foundstone.com

```
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
154   RpcSs          ->  135   TCP   C:\WINNT\system32\RpcSs.exe
2     System         ->  135   TCP
2     System         ->  139   TCP
2     System         ->  1026  TCP
154   RpcSs          ->  1026  TCP   C:\WINNT\system32\RpcSs.exe
154   RpcSs          ->  1028  TCP   C:\WINNT\system32\RpcSs.exe
273   aim            ->  2932  TCP   D:\AIM95\aim.exe
2     System         ->  2934  TCP
273   aim            ->  2934  TCP   D:\AIM95\aim.exe
70    ICQ            ->  3152  TCP   E:\ICQ\ICQ.exe
2     System         ->  3152  TCP
2     System         ->  3209  TCP
273   aim            ->  3209  TCP   D:\AIM95\aim.exe
2     System         ->  3552  TCP
2     System         ->  3554  TCP
70    ICQ            ->  3849  TCP   E:\ICQ\ICQ.exe
73    blackd         ->  1102  UDP   G:\blackice\blackd.exe
2     System         ->  3857  UDP
198   iexplore       ->  3857  UDP   C:\PROGRA~1\INTERN~1\iexplore.exe
```

Fport reports all open TCP/IP and UDP ports and maps them to the owning application. The program contains five (5) switches. The switches may be utilized using either a '/'
or a '-' preceding the switch. The switches are;

```
/h - Help
/a - sort by application
/i - sort by process ID
/ap - sort by application path
/p - sort by port
```

Network Associates Sniffer Basic – http://www.networkassociates.com



Sniffer Basic captures all packets at near-wire speed. To help focus troubleshooting, you can quickly develop filters using standard Windows drag-and-drop functionality. Once captured, protocols are decoded and displayed in color-coded summary, detail, and hex windows. Sniffer Basic's traffic generator is ideal for application developers who need to test network hardware and software components. Sniffer Basic can play back captured packets one at a time or in a batch, and can vary the time between packets to control the load placed on the network. Individual packets may be edited before transmission. Sniffer Basic also supports simultaneous traffic generation and packet capture.

First we will run Fport on all mission critical, and a sampling of other hosts on the network. Fport shall report back what ports are open and tied to what application or service. This is one way to ensure that if a Trojan was installed on a machine, it will be caught, and secondly, if we find a service running on a host that shouldn't be, we can shut it off. i.e.: port 111 sunRPC

From outside of GIAC Enterprises network, we run Network Associates Sniffer Basic packet generator feature. We generate packets based on what we know about our rulesets and send these packets to the border router, firewalls, and certain targeted hosts inside GIAC Enterprises network. While these packets are being generated externally, we have the Sniffer Basic product running internally capturing packets. This capture file is then analyzed to see whether our perimeter defenses are doing what they are supposed to be doing.

We run Nmap against the border router, firewalls, and certain targeted host inside GIAC Enterprises network. Lets go ahead and run Nmap against the firewall and border router in the following way:

```
nmap -v -sS -g(source port) -P0 giac.border.router.address
nmap -v -sS -g(source port) -P0 giac.PIX.firewall.address
```

The -sS switch will run a what is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection. The **-v**, tells nmap to run in verbose mode, **-P0** tells nmap not to ping the host. The switch **-g**(source port) is great to use because you can vary this number so it looks like traffic is coming from a certain port that you specify. This is a good way to test and determine whether the firewall or the border router is blocking based on source port such as ftp, DNS zone transfers, etc. During this whole process we are capturing packets for analysis with Sniffer Basic so that we may be able to monitor packet payload as well.

Example output from Nmap:

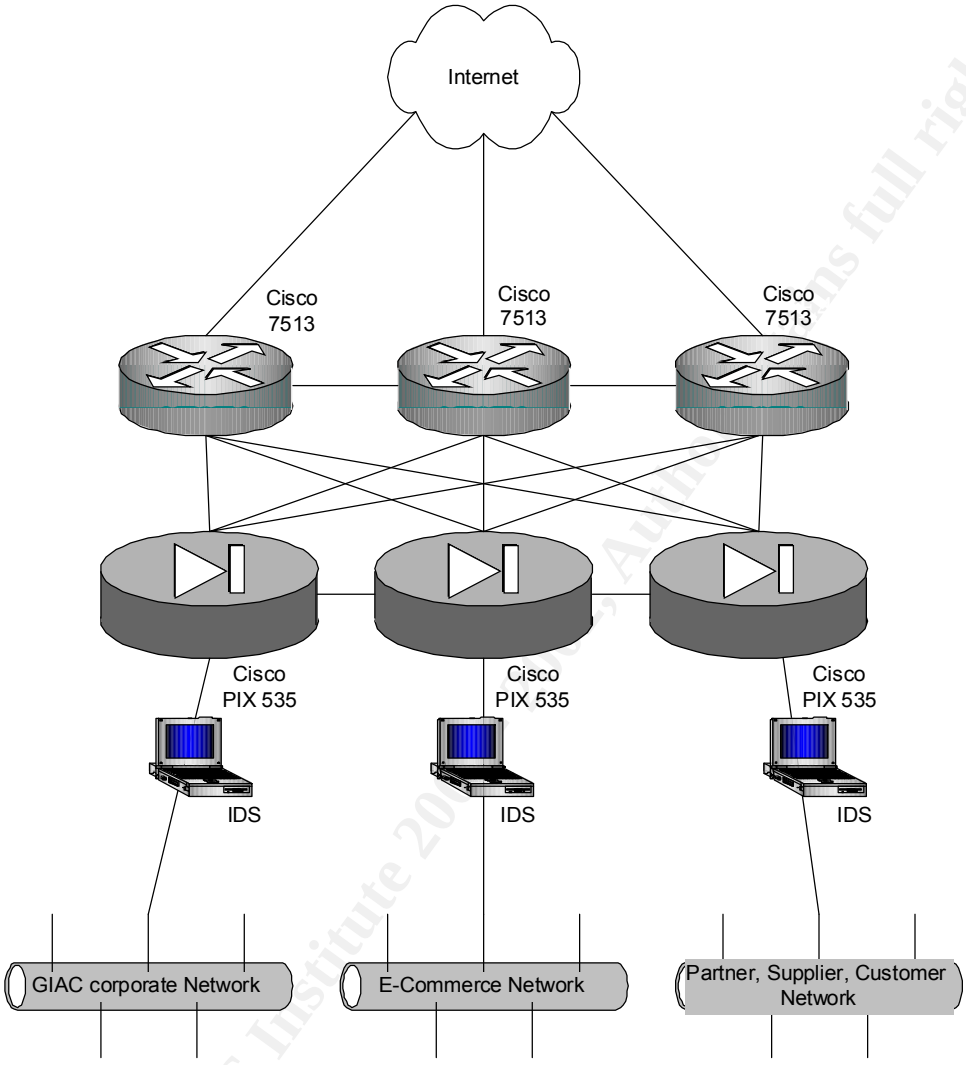
```
Starting nmap V. 2.53 by fyodor@insecure.org
www.insecure.org/nmap

Initiating SYN half-open stealth scan against giac.int.host.address (x.x.x.x)
The SYN scan took 79 seconds to scan 1523 ports.
Interesting ports on giac.int.host.address (x.x.x.x):
(The 1489 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
21/tcp     filtered    ftp
22/tcp     filtered    ssh
23/tcp     filtered    telnet
25/tcp     closed      smtp
53/tcp     filtered    domain
79/tcp     open        finger
80/tcp     open        http
```

From this output we can tell our rulesets are working because of the filtered state of certain ports. The result of running nmap is usually a list of interesting ports on the machine(s) being scanned (if any). Nmap always gives the port's "well known" service name (if any), number, state, and protocol. The state is either 'open', 'filtered', or 'unfiltered'. Open means that the target machine will accept connections on that port. Filtered means that a firewall, filter, or other network obstacle is covering the port and preventing nmap from determining whether the port is open. Unfiltered means that the port is known by nmap to be closed and no firewall/filter seems to be interfering with nmap's attempts to determine this. Unfiltered ports are the common case and are only shown when most of the scanned ports are in the filtered state.

Conduct a perimeter analysis

Our perimeter analysis shows us exactly what is being blocked at what device and what is let through. The results are what we expected to see in the data we analyzed. If for some reason, we saw something that shouldn't have happened, we could go back and install a patch or modify an access list or a ruleset. Sure, improvements could be made to tighten security on the network, but that may infringe on our business needs. No network in TOTALLY secure. The reason for this comes from the basic question of "What are my companies business needs?", there is a cost of doing business, an 'exposure' if you will. One of those exposures is network security. Certain services must be opened and certain traffic must be allowed to pass unhindered. Is this dangerous? Yes, it can be, but we simply have to make sure that our security policy is driven by our business needs and keep a vigilant eye out for trouble. We have to work with what we have. Security can only be tightened up to a point, it can't be tightened so much that it hinders our business performance. Click here for more information regarding security that applies to GIAC Enterprises, there

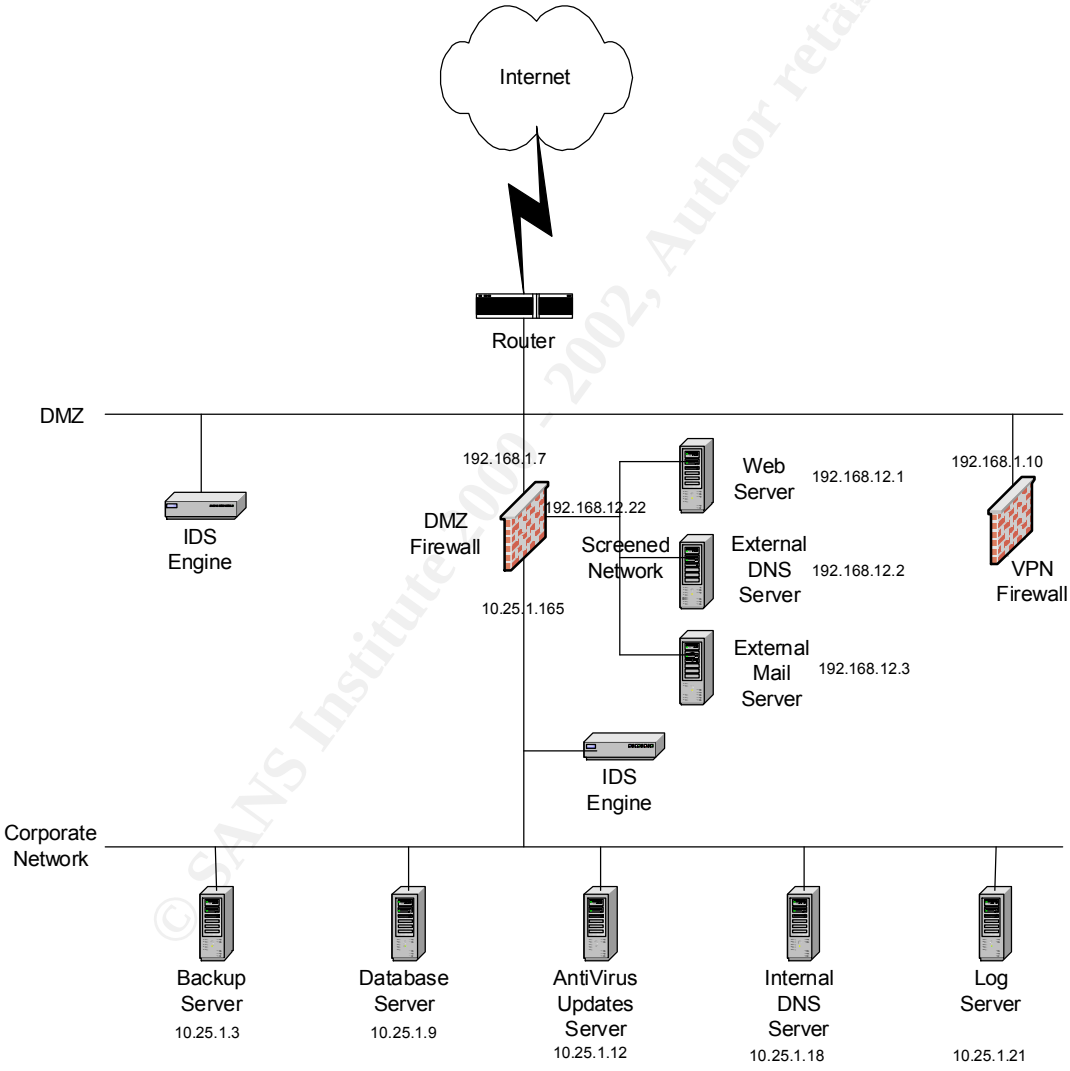
is information here that is often overloked:
http://www.cisco.com/warp/public/126/secpol.html An alternate network architecture for GIAC Enterprises is shown on the next page.



This alternative architecture for GIAC Enterprises is like one shown above. Each of the three PIX 535's are connected to each of the Cisco 7513's as well as being daisy chained to themselves with failover cables. The Cisco 7513 are also connected to one another and are running HSRP (Hot Standby Routing Protocol). IDS boxes are placed behind the firewall for monitoring purposes which can detect and stop attacks. Normally, the GIAC Corporate Network, The E-Commerce Network, and the Partner, Supplier, and Customer network are separate networks, having only one path out to the Internet.
In the case of a failure in one of the six harware devices, network connectivity for that segment will not be lost. This redundancy buys us time, and this time keeps revenue coming in. Downtime for an E-Commerce network can be very, very costly. Lost customers equal lost revenue. Customers must feel they are doing business in a safe environment.
Better hardware support contracts can also be purchased, like Cisco's SmartNet contracts. Training employees to be vigilant with their computing practices helps keep security tight. For example, changing passwords frequently and making them at least eight characters in length and alpha numeric.

ASSIGNMENT 4 – DESIGN UNDER FIRE

For our Design Under Fire section, we will be using the network diagram that was submitted by Janice Southerland. The practical that was submitted can be found here: http://www.sans.org/giactc/gcfw.htm



GIAC Enterprises
Nework Diagram

Janice chose Checkpoint Firewall-1 4.1 for her design, which, has several vulnerabilities. We will be designing a Fragment based attack.
The vulnerabilities of Firewall-1 are listed here:

http://www.checkpoint.com/techsupport/alerts/index.html

An attack against the firewall itself:

IP Fragment-driven Denial of Service Vulnerability

Summary: It has been determined that a stream of large IP fragments can cause the FireWall-1 code that logs the fragmentation event to consume most available host system CPU cycles thereby denying legitimate traffic. For security reasons (e.g., overlay attacks) FireWall-1 reassembles all IP fragments of a datagram prior to inspection against the security policy. After reassembly, the packet is processed by the FireWall-1 Stateful Inspection engine, and if allowed by the security policy to proceed, the packet is refragmented and forwarded. To identify and audit attacks such as Ping of Death, Check Point added a mechanism to FireWall-1, outside of its standard logging capability, to log certain events that occur during the FireWall-1 virtual reassembly process. This fragmentation logging takes place on the gateway itself and not on the management station (relevant for distributed management deployments).

Attack: Jolt2 can be used to send a stream of extremely large IP fragments to a FireWall-1 gateway, which in some cases can cause the write mechanism to grab all host CPU resources thereby bring the firewall down and not letting traffic pass. There is no fragmentation tracking resource that is exhausted; it is the case that the fragmentation logging process is the cause of this issue.

Fix: As workaround, disabling the console logging, thereby mitigating this issue by using the following command line on their FireWall-1 module(s): $FWDIR/bin/fw ctl debug -buf Installing new binaries will also solve this issue. Also, make sure the latest patches have been applied to the operating system.

Denial of Service Attack:

We will be subjecting Janice's network design to an attack from 50 compromised cable modem and DSL users using the **Stacheldraht DDoS Attack Tool** to send a TCP SYN flood. We will then describe countermeasures to prevent such attacks.
A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Since these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing e-mail, using FTP service, and so on. Since cable modems and DSL users have a pretty good amount of bandwidth at their disposal, attacks from those systems can be fairly vicious.

Since Janice has a Cisco 7206 border router running IOS 12.0, we will use the TCP Intercept feature of the Cisco IOS. We will now describe how the TCP Intercept feature works, how it's implemented, and a configuration example:

Description: The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP synchronization (SYN) packets from clients to

servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests. When establishing your security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. You can choose to operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt. TCP options that are negotiated on handshake (such as RFC 1323 on window scaling, for example) will not be negotiated because the TCP intercept software does not know what the server can do or will negotiate.

Implementation:

On the Cisco router we will need to perform the following tasks to configure TCP intercept. The first task is required; the rest are optional.

1. Enable TCP Intercept

Define an IP extended access list on the router using the following syntax in global configuration mode:

access-list access-list-number {deny | permit} tcp any destination destination-wildcard

Enable TCP intercept with this command syntax:

ip tcp intercept list access-list-number

You can define an access list to intercept all requests or only those coming from specific networks or destined for specific servers. Typically the access list will define the source as any and define specific destination networks or servers. That is, you do not attempt to filter on the source addresses because you don't necessarily know who to intercept packets from. You identify the destination in order to protect destination servers. If no access list match is found, the router allows the request to pass with no further action.

2. Set the TCP Intercept Mode

The TCP intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode. In intercept mode, the software actively intercepts each incoming connection request (SYN) and responds on behalf of the server with an ACK and SYN, then waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is set to the server and the software performs a three-way handshake with the server. When this is complete, the two half-connections are joined. In watch mode, connection requests are allowed to pass through the router to the server but are watched until they become established. If they fail to become established within 30 seconds (configurable with the ip tcp intercept watch-timeout command), the software sends a Reset to the server to clear up its state.

To set the TCP intercept mode, issue the following command in global configuration mode. The syntax for which is:

ip tcp intercept mode {intercept | watch}

3. Set the TCP Intercept Drop Mode

When under attack, the TCP intercept feature becomes more aggressive in its protective behavior. If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last one minute exceeds 1100, each new arriving connection causes the oldest partial connection to be deleted. Also, the initial retransmission timeout is reduced by half to 0.5 seconds (so the total time trying to establish a connection is cut in half). By default, the software drops the oldest partial connection. Alternatively, you can configure the software to drop a random connection. To set the drop mode, issue the following command syntax in global configuration mode:

ip tcp intercept drop-mode {oldest | random}

4. Change the TCP Intercept Timers

By default, the software waits for 30 seconds for a watched connection to reach established state before sending a Reset to the server. To change this value, issue the following command syntax in global configuration mode:

ip tcp intercept watch-timeout seconds

By default, the software waits for 5 seconds from receipt of a reset or FIN-exchange before it ceases to manage the connection. To change this value, issue the following command syntax in global configuration mode:

ip tcp intercept finrst-timeout seconds

By default, the software still manages a connection for 24 hours after no activity. Change the time the software will manage a connection after no activity. To change this value, issue the following command syntax in global configuration mode:

ip tcp intercept connection-timeout seconds

5. Change the TCP Intercept Aggressive Thresholds

Two factors determine when aggressive behavior begins and ends: total incomplete connections and connection requests during the last one-minute sample period. Both thresholds have default values that can be redefined. When a threshold is exceeded, the TCP intercept assumes the server is under attack and goes into aggressive mode. When in aggressive mode, the following occurs: Each new arriving connection causes the oldest partial connection to be deleted. (You can change to a random drop mode.) The initial retransmission timeout is reduced by half to 0.5 seconds, and so the total time trying to establish the connection is cut in half. (When not in aggressive mode, the code does exponential back-off on its retransmissions of SYN segments. The initial retransmission timeout is 1 second. The subsequent timeouts are 2 seconds, 4 seconds, 8 seconds, and 16 seconds. The code retransmits 4 times before giving up, so it gives up after 31 seconds of no acknowledgment.)If in watch mode, the watch timeout is reduced by half. (If the default is in place, the watch timeout becomes 15 seconds). The drop strategy can be changed from the oldest connection to a random connection with the ip tcp intercept drop-mode command.

Note - The two factors that determine aggressive behavior are related and work together. When either of the high values is exceeded, aggressive behavior begins. When both quantities fall below the low value, aggressive behavior ends.

You can change the threshold for triggering aggressive mode based on the total number of incomplete connections. The default values for low and high are 900 and 1100 incomplete connections, respectively.

To change these values, perform the following tasks in global configuration mode:
Set the threshold for stopping aggressive mode.

ip tcp intercept max-incomplete low number

Set the threshold for triggering aggressive mode.

ip tcp intercept max-incomplete high number

You can also change the threshold for triggering aggressive mode based on the number of connection requests received in the last 1-minute sample period. The default values for low and high are 900 and 1100 connection requests, respectively. To change these values, perform the following tasks in global configuration mode:

Set the threshold for stopping aggressive mode.

ip tcp intercept one-minute low number

Set the threshold for triggering aggressive mode.

ip tcp intercept one-minute high number

6. Monitor and Maintain TCP Intercept

To display TCP intercept information, perform either of the following tasks in EXEC mode:

Display incomplete connections and established connections.

show tcp intercept connections

Display TCP intercept statistics.

show tcp intercept statistics

TCP Intercept Configuration Example:

The following configuration defines extended IP access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

An attack plan to compromise an internal system:

For this section we will select our target, that target will be the web server. This web server, like many other web servers are targeted for the following reasons. The web server is not protected by the border router or firewall. It also may be running without the proper security patches to the web server software itself (like so many web servers are) which will leave it open to attack, and may also be running with other poorly programmed software as well.

A first step in attempting to compromise this system would be to run Nmap against it to reveal the operating system running on the machine and open ports if there are any open other that port 80, 443, etc, - also much information can be gathered from the http headers revealed by the system. Sometimes poorly configured machines will show you complete directories on their hard disks!

Once the reconnaissance portion of the attack plan has been completed, it's time to gather all this information and research any vulnerabilities that exist with the type of system and software that is running. Once vulnerabilities have benen found, it is up to the attacker as to what they want to do to the system, either defacing the web site, launching a DoS attak against it, or completely crashing the system.