Global Information Assurance Certification Paper

GIAC Practical Assignment

GFCW Certification
LevelTwo Firewalls, Perimeter Protection and VPNs

Elton Wright
April 4, 2001

Assignment One

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

You must consider and define access for:

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

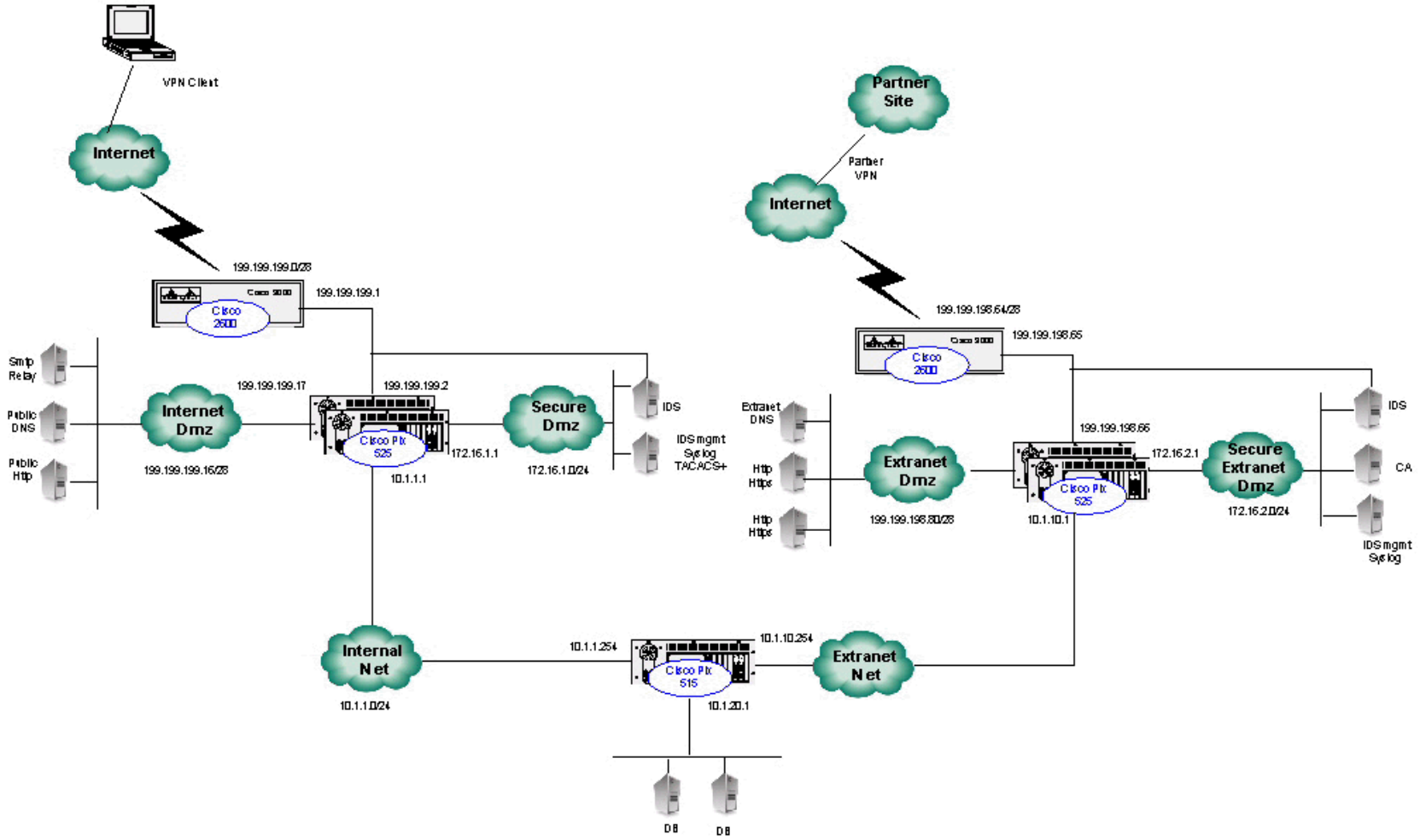
Security Architecture

GIAC Enterprises (GIAC) has recently undergone a network redesign. The new infrastructure has been designed to facilitate efficient and secure exchange of fortune cookie sayings with partners, customers, and suppliers while at the same time offering Internet services to GIAC employees. The infrastructure has been divided into the following two segments:

- Corporate Internet Perimeter
- Extranet Internet Perimeter

The two segments allow GIAC to compartmentalize their infrastructure based on traffic patterns associated with specific business needs. The two perimeter networks are secured by PIX firewalls. A third PIX firewall is located between GIAC's internal network and the Extranet Internet Perimeter. This adds a third layer of security and protects the sensitive information that is stored on the databases from all networks.

The following diagram is a high-level overview of GIAC's infrastructure.



Corporate Internet Perimeter	The purpose of the Corporate Internet Perimeter (CIP) is to provide a secure Internet presence for GIAC. The CIP will serve as the Internet gateway for GIAC employees. The CIP infrastructure will be composed of the following pieces: **IP Information** Network Broadcast Nodes Network Segment 199.199.199.0/27 199.199.199.31 30 ISP issued 199.199.199.0/28 199.199.199.15 14 Perimeter-net 199.199.199.16/28 199.199.199.31 14 Internet-DMZ **Cisco 2600 Router – Item 1** IOS version – 12.1(0) The perimeter router will connect GIAC to the ISP and will serve as the first line of the perimeter defense. The router will be locked down based on the GIAC border router security policy. **Cisco PIX 525 – Item 2** OS version – 5.3(1) Redundant firewalls will be responsible for enforcing the security policy. All TCP/IP traffic will be intercepted at the firewall and routed to one of the following networks: • Internet • Internet DMZ • Secure DMZ • Intranet Function Interface IP Address Subnet Mask External Interface Ethernet0 199.199.199.2 255.255.255.240

Corporate Internet Perimeter

Internet-DMZ – Item 3

The Internet-DMZ will host the typical Internet services that organizations need to in today's business environment. The Internet-DMZ will provide a secure method for sending and receiving SMTP email as well as DNS and web hosting services for GIAC.com.

- The Http servers in the Internet-DMZ will host the web site www.GIAC.com. This will provide the static web pages that include general company information and investor information.
- All public MX records for GIAC.com will point to the email relay located in the Internet-DMZ. This will provide all anti-spam and anti-virus protection before forwarding email to the internal mail host.
- The DNS server will provide primary DNS services for GIAC.com. This name server will only provide name services for publicly accessible devices.

Secure-DMZ - Item 4

The Secure-DMZ will be used by GIAC to monitor the CIP. Intrusion detection and logging systems will be the critical pieces composing this Dmz.

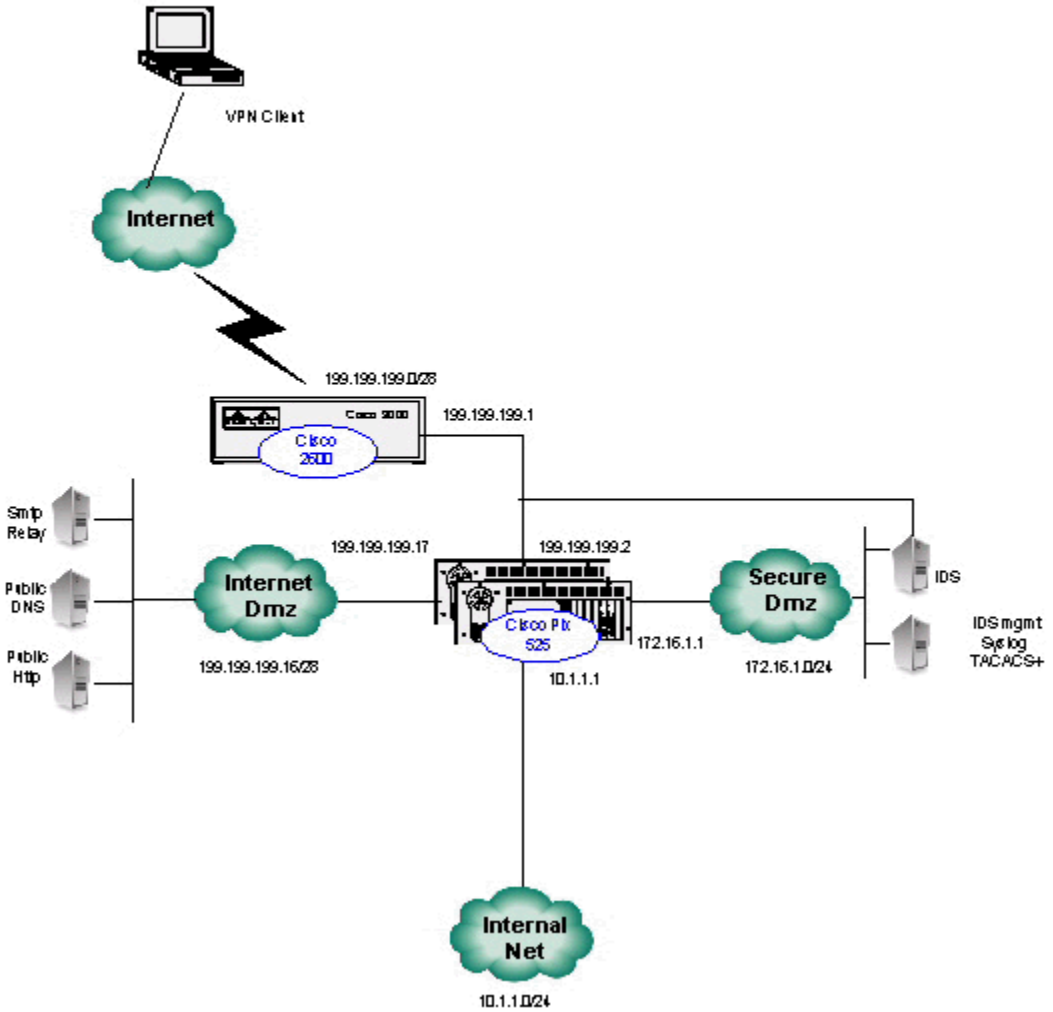
- ISS RealSecure 5.0 will provide intrusion detection for the external network segment. This will alert GIAC security engineers of any malicious TCP/IP signatures.
- A PrivateI syslog server will keep all PIX and router logs. This host will also host the workgroup manager for the RealSecure network engine. The workgroup manager will allow GIAC security associates to customize the IDS system to create a policy to minimize the false positives associated with most IDS. A TACACS+ server will be installed to perform client VPN authentication.

Remote Access - Item 5

GIAC employees will have remote access over the Internet using a VPN connection to the PIX. Cisco's Secure VPN Client will be on each employees laptop to provide them with remote access.

- Client VPN services are provided to all approved GIAC employees requiring remote access.

Corporate Internet Perimeter



Extranet Internet Perimeter	The purpose of the Extranet Internet Perimeter (EIP) is to provide secure e-commerce communications with GIAC customers, suppliers, and partners. The EIP has been created as a separate network to allow GIAC to customize a security solution required for secure e-commerce as well as increase performance and scalability. The foundation for the EIP is a Cisco 2600 series router and redundant Cisco PIX 525 firewalls. **IP Information** Network Broadcast Nodes Network Segment 199.199.198.64/27 199.199.198.95 30 ISP issued 199.199.198.64/28 199.199.198.79 14 Extranet-Net 199.199.198.80/28 199.199.198.95 14 Extranet-DMZ **Cisco 2600 Router – Item 1** IOS version – 12.1(0) The perimeter router will connect GIAC to the ISP and will serve as the first line of the perimeter defense for the EIP. The router will be locked down based on GIAC security standards. **Cisco PIX 525 – Item 2** OS version – 5.3(1) The firewall will be responsible for enforcing the security policy. All TCP/IP traffic will be intercepted at the firewall and routed to one of the following networks: • Extranet Dmz • Extranet VPN Dmz • Secure Extranet Dmz • Extranet Net Function Interface IP Address Subnet Mask External Interface Ethernet0

EIP (cont.) **Extranet-VPN – Item 5**

This will provide a secure connection to GIAC partners. The chosen VPN protocol is IKE and we will be using the 3DES algorithm.

IKE

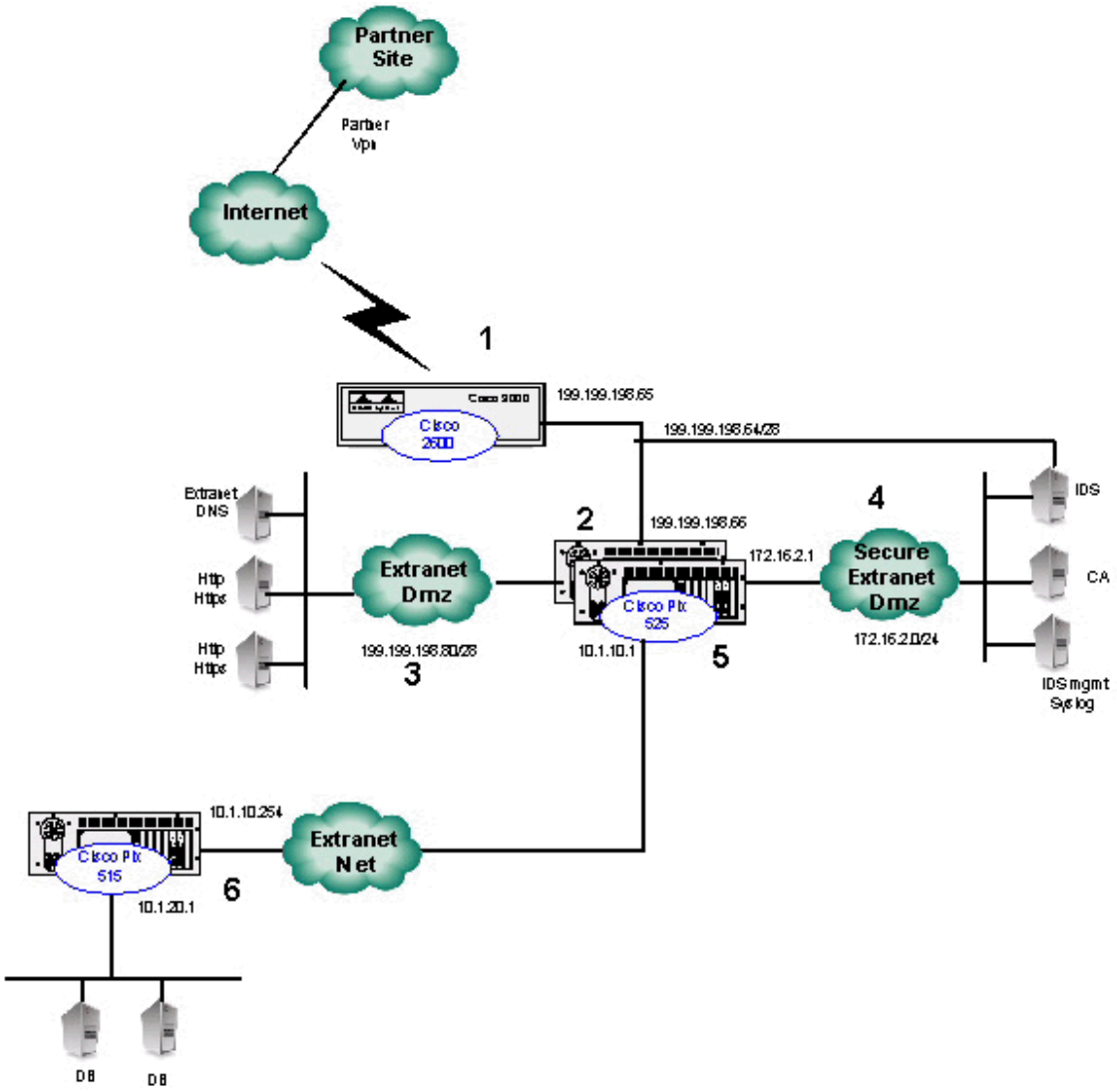
Internet Key Exchange (IKE) is a VPN protocol that allows two VPN end-points to establish communication through an encrypted tunnel. In order to establish this encrypted link, both parties need to configure the VPN end-point using the same VPN policy. GIAC partners must comply with a strict security policy before a VPN can be established. If someone were to compromise a partner site, this would create a backdoor into GIAC's EIP.

NOTE: Each PIX will need an activation key to enable DES and 3DES. Without these activation keys VPN will not work.

Internal Firewall – Item 6

A PIX firewall will be used internally to provide a third layer of security between the CIP and the EIP. The ERP system that the secure web servers communicate with will reside on a network behind the internal firewall. The only network traffic that will be allowed to pass from the CIP to the EIP will be for development and administration purposes.

Extranet Internet Perimeter



Assignment Two

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.

Security Policy	The security policy for GIAC requires a layered security model. A layered security model is composed of multiple security checkpoints throughout the CIP and EIP. Each layer serves to protect corporate information in the event of a security breach at a higher level.

Bordor Router	**Disable TCP/IP Services** Cisco routers have certain services that are enabled by default. These services can be used in a number of attacks and are not necessary on the border router. The following policy should be applied on both the CIP and EIP border routers. Action Reason Interface Disable proxy ARP Can be used to generate insecure routing information. **Command - no ip proxy-arp** All Disable TCP/UDP small services Small services include chargen, discard, and echo. These services can lead to various attacks. **Command – no service tcp-small-servers** **no service udp-small-servers** Global Disable IP source routing IP source routing can be used to spoof the packet origin. IP source should always be turned off. **Command - no ip source-route** All Disable finger replies Can be used to gather user information that could lead to more severe attacks. **Command – no service finger** Global Disable redirect messages Allows ICMP redirect packets that could be used to gather routing information. **Command – no ip redirects** S0 Disable the generation of icmp unreachable messages IP unreachable information can be used to determine the types of protocols allowed on your network. Command – **Command – no ip unreachables** S0 Disable fast and autonomous switching Can be manipulated to exploit routing information. **Commnand – no ip route-cache** Global Disable multicast route caching Multicast routing is not necessary on the perimeter router. **Command – no ip mroute-cache** All Disable maintenance operation protocol MOP can be used to gain administrative access. MOP is generally not required and should be stopped. **Command – no mop enabled**

Border Router (cont.)

Access-List Security

Simple access-lists (acls) provide an extra layer of perimeter security without drastically affecting router performance. Cisco routers have been used throughout this design and offer several types of acls. Two of the most used on border routers are as follows:

- Standard Acls – Are defined by using an Acl number of 1-99. Standard Acls only test IP traffic based on source IP address.
- Extended Acls – Are defined by using an Acl number of 100-199. Extended Acls validate source, destination and protocol.

Defining and Applying Access-Lists - Router

Access lists are composed of several pieces. The purpose of an Acl is to allow the administrator to define what source IP addresses can go to what destination IP address using a specific service. Below are the basic parts of a router Acl.

Access-list <id> <action> <protocol> <source> <destination> <service>

Serial0 Interface

```
Router(config)#Access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
Router(config)#Access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
Router(config)#Access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
Router(config)#Access-list 101 deny ip 172.16.0.0 0.0.255.255 any log
Router(config)#Access-list 101 deny ip host 0.0.0.0 any log
Router(config)#Access-list 101 deny ip 224.0.0.0 0.255.255.255 any log
```

Simply creating an Acl is not enough. The Acl must now be applied to a specific interface. The Access-group command is used to apply the Acl to a specific interface. The following command would apply Acl 101 to the S0 interface in the inbound direction.

```
Router(config-if)#Ip  access-group 101 in
```

The purpose of this Acl is to prevent the routing of RFC-1918 addresses. This Acl has been applied to both perimeter routers. RFC-1918 was developed to create address ranges to be used on private networks. This has allowed ISPs to drastically increase their IP address space because organizations only need public address space for devices accessible via the Internet.

NOTE: Unless an Acl has been applied to an interface all traffic is implicitly allowed. Once an Acl has been applied to an interface, all traffic that is not explicitly allowed is implicitly denied.

PIX The PIX architecture is based on interface security levels. Access through the PIX is configured based on the security levels of the source and destination interfaces. A security level of 0 is low and is treated as the least secure interface. The outside interface or Ethernet0 is always assigned a security level of 0. The inside interface or Ethernet1 is always assigned a security level of 100. This is the most secure interface. The table below illustrates GIAC's PIX interface security levels.

CIP

Outside
0

Inside
100

InternetDmz
20

SecureDmz
50

EIP

Outside
0

Inside
100

ExtranetDmz
20

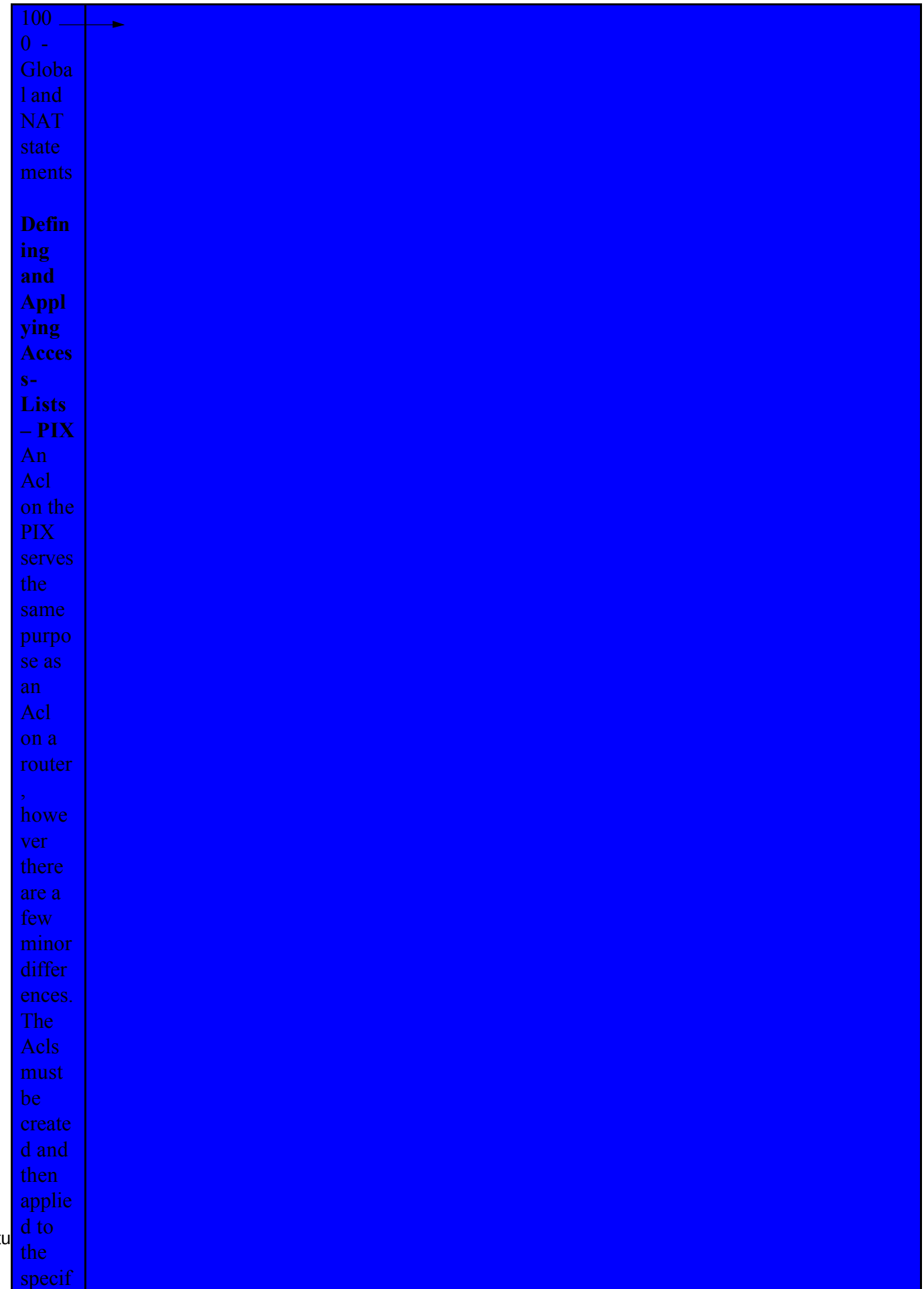
SecureExtDmz
80

All traffic is denied by default in the PIX architecture. In order for traffic to pass through the firewall from a lower security level to a higher security level both access lists and static NAT must be configured.

0 ⟶

100 - Access-list and Static NAT statements

In order for traffic to pass from a higher security level to a lower security level, global and NAT statements must be configured. Once these two statements have been configured, all traffic is by defaul



VPN

Client VPN

The client VPN will be created using an IPSec VPN tunnel from the remote client to the PIX firewall. Cisco Secure VPN is a client based software package that will facilitate the VPN communication between the VPN termination points. The remote client will need to be configured using the following VPN policy:

Authentication Method – TACACS+
Encryption Algorighm = 3DES
Hash Algorighm – MD5

The CIP PIX will need to be configured to allow the remote VPN clients to establish a VPN.

The **sysopt** command will allow all validated VPN traffic to bypass all access-list and conduit statements.

- *Sysopt connection permit-ipsec*

A **transform set** will also need to be defined. The transform set is how you configure the hash level and encryption method.

- *Crypto ipsec transform-set clientvpn esp-3des esp-md5-hmac*

A **dynamic crypto map** will need to be created. Dynamic crypto maps are used for instances when the source is not always known such as with a remote user. The dynamic crypto map will cause certain VPN credentials to be determined after VPN establishment. The map has to be associated with a transform-set.

- *crypto dynamic-map client 1 set transform-set clientvpn*

A **crypto map** must be defined to reference the dynamic crypto map that was previously defined. This allows the administrator to define multiple crypto maps with different weights. This allows the PIX to function in a site-to-site VPN as well as client-to-PIX VPN.

- *Crypto map dynamic 10 ipsec-isakmp dynamic clientvpn*

Now an **isakmp** policy must be defined similar to the policy defined on the VPN client.

- Isakmp policy 10 authentication pre-share
  Isakmp policy 10 encryption 3des
  Isakmp policy 10 hash md5
  Isakmp policy 10 group 10
  Isakmp policy 10 lifetime 500
  Isakmp enable outside
  Isakmp key fortunesrus address 0.0.0.0 netmask 0.0.0.0

VPN (cont.)

Partner VPN

The EIP PIX will be configured using the following VPN policy:

The **sysopt** command will allow all validated VPN traffic to bypass all access-list and conduit statements.

- *Sysopt connection permit-ipsec*

A **crypto map** will need to be created. The crypto map is where all the VPN properties will be configured

- *crypto map partner* 1 *ipsec-isakmp*

An **access-list** will be referenced under the crypto map to define what networks are in the encryption domain. VPN is the access-list in this example.

Crypto map giac 1 match address VPN

- *Access-list VPN permit ip {partner network} {mask} 10.1.10.0 255.255.255.0*

A VPN **peer** will need to be defined so that the PIX will have a VPN termination end-point. Multiple partner sites will be created by using multiple set peer instances.

- *Crypto map partner 1 set peer {partner VPN device IP}*

A **transform set** will also need to be defined. The transform set is how you configure the hash level and encryption method.

- *Crypto ipsec transform-set partnervpn ah-md5-hmac esp-3des*

The transform set previously created must now be **assigned to a crypto map**.

- *crypto map partner 1 set transform-set giacvpn*

The last thing that needs to be done is to associate the crypto map giac, to an interface.

- *crypto map partner interface outside*

By using isakmp (IKE) for VPN establishment we will still be using IPSec as the protocol. The key difference between Manual-IPSec and IKE is the method in which keys are exchanged. Manual-IPSec requires that a pre-shared key be negotiated manually. IKE uses dynamic key negotiation.

Assignment Three

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

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.

2. Implement the assessment. Validate that the Primary Firewall is actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.

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

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

Information Security Audit

Purpose

GIAC Enterprises (GIAC) is an online firm that provides fortune cookie sayings and paraphernalia to a wide range of organizations. GIAC has just completed a network redesign that will facilitate communication while at the same time maintaining a secure e-commerce environment. It is imperative that GIAC maintain the level of security that has been established. In order to comply with this requirement, GIAC will undergo a routine security audit to validate their perimeter network security.

Security Audit

Plan the Assessment

The security audit will be performed on the Extranet Internet Perimeter (EIP) firewall. The EIP firewall is responsible for protecting the extranet segment, which is used to communicate with customers, suppliers and partners. The security audit will be composed of three components.

- Pre-audit planning
- Information gathering
- Vulnerability identification and exploitation

Pre-audit Planning

Due to the nature of the audit it is important to plan the security audit before hand. The following measures should be taken to ensure a smooth and risk free security audit.

- **Notify all parties** that could be affected by the assessment. This includes your ISP, network administrator, security administrators. Notifying these associates will alleviate the anxiety any hacking attempt will cause an unsuspecting associate. Also schedule the audit during a time period that customers, suppliers and partners will not be affected.

- **Prepare diagrams** for the audit. This particular audit will be to validate the security currently in place, not to map the network. It will be important to have information regarding services, operating systems, etc. to conduct a complete security audit.

- **The estimated costs** for the security audit will be in the range of $3,500 - $4,500. This estimate is a fixed price estimate that allows for 2-3 days to complete the audit and document the findings. **NOTE:** The security audit scope includes a PIX audit and documentation. This security audit does not include any security validation of operating systems, application layer security, etc.

Security Audit (cont.)

Information Gathering

The first step in conducting the security audit is to gather as much information as possible about the targeted network and hosts. This is the reconnaissance phase of the audit. It is a good idea to know what kind of information is available to the Internet community about your network. NOTE: GIAC is a fictitious organization and a real lab could not be created. All of the examples below are for educational purposes.

Nmap is a port-scanning tool that is invaluable for gathering network information. Nmap has many options that can be useful depending on the purpose of the scan.

Nmap –sP 199.199.198.64/27 – This is a ping scan that will tell us every device on the given network that responds to a ping request. This is useful information that will help in more refined attacks.

- -sP – This option indicates a ping scan

Nmap – sT 199.199.198.64/27 –p 1-65535 –O – This is a Tcp port scan that will tell us the Tcp ports that are open on the targeted network range. This will be a critical scan to validate proper Acl configuration.

- *–p* – This allows us to enter the designated port range to scan
- *–sT* – This option indicates a Tcp port scan
- *–O* – This will give us Tcp fingerprinting information to identify operating systems.

Nmap – sU 199.199.198.64/27 –p 1-65535 – This will tell us all of the Udp ports that are allowed through the PIX firewall.

- –sU – This option indicates a Udp port scan.

The output from the Nmap scans can now be used to validate the Acls implemented on the PIX firewall.

- Are the appropriate Tcp ports being allowed through?
- Are the appropriate Udp ports being allowed through?
- Are all other packets being dropped?

Security Audit (cont.)

Vulnerability Identification and Exploitation

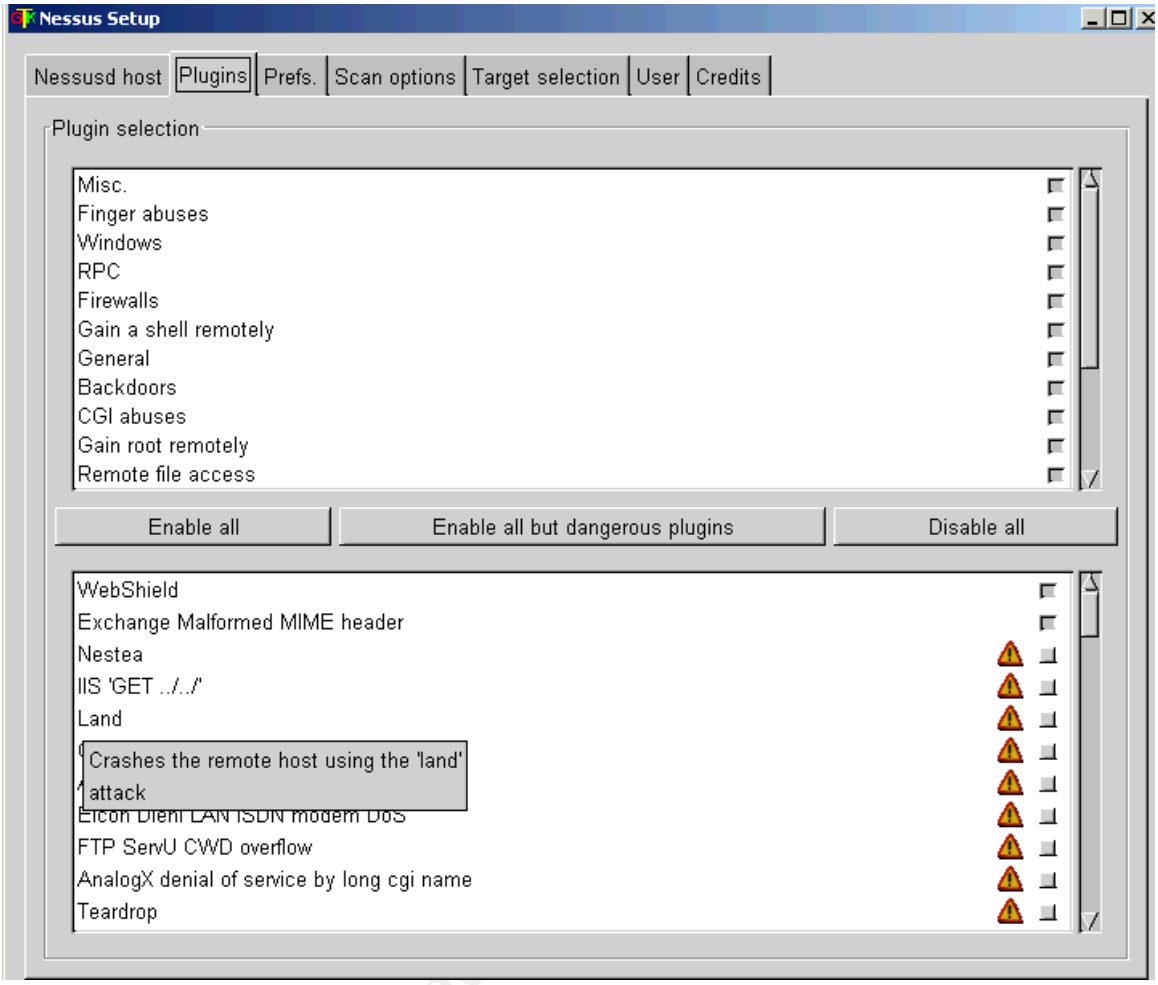
Once the initial reconnaissance has been performed a more efficient attack plan can be developed to target specific devices for vulnerabilities.

Nessus is an excellant tool that will scan the network and simulate a large number of attacks on the targeted network devices. After conducting the scans, Nessus provides reports stating what vulnerabilities were found and Common Vulnerability and Exposure (CVE) http://cve.mitre.org/.

- CVE – A common vulnerabilitiy that has been researched and determined to be a valid concern. The CVE describes the problem and usually offers a problem resolution.

Nessus

Nessus is a security auditing tool that incorporates plugins to simulate approximately 630 attacks. The plugins allow the administrator/cracker to update the attack signatures routinely as new exploits are developed. The following link shows the current exploit database http://cgi.nessus.org/plugins/dump.php3.



Perimeter Analysis

The overall perimeter security for both the CIP and EIP is very good. However, there are a number of things that could be added to strengthen security.

Host based Intrusion Detection

To complement the network sensors on the perimeter, host based intrusion detection could be added to increase security at the host level. ISS RealSecure has host based IDS modules as well as network sensors. The host-based modules can be managed from the same workgroup manager which would fit nicely into this environment. The RealSecure host based modules are suppoted on a number of operating systems including Solaris, HP-UX and NT. The purpose of these modules is to monitor for malicious activity as the system level as opposed to the network level. A malicious user trying to log on to a server would not be detected at the network layer. The host based IDS would detect an excessive amount of failed logon attempts.

Terminal Server

A terminal server is an excellent way to increase perimeter security for all devices on the Internet perimeter. A Cisco 2600 serious router should be used as a terminal server for each Internet perimeter. This will allow the security administrator to completely disable telnet on the border routers and the PIX firewalls. The terminal server will provide console access from the internal network.
To disable telnet on the Cisco router type the following:

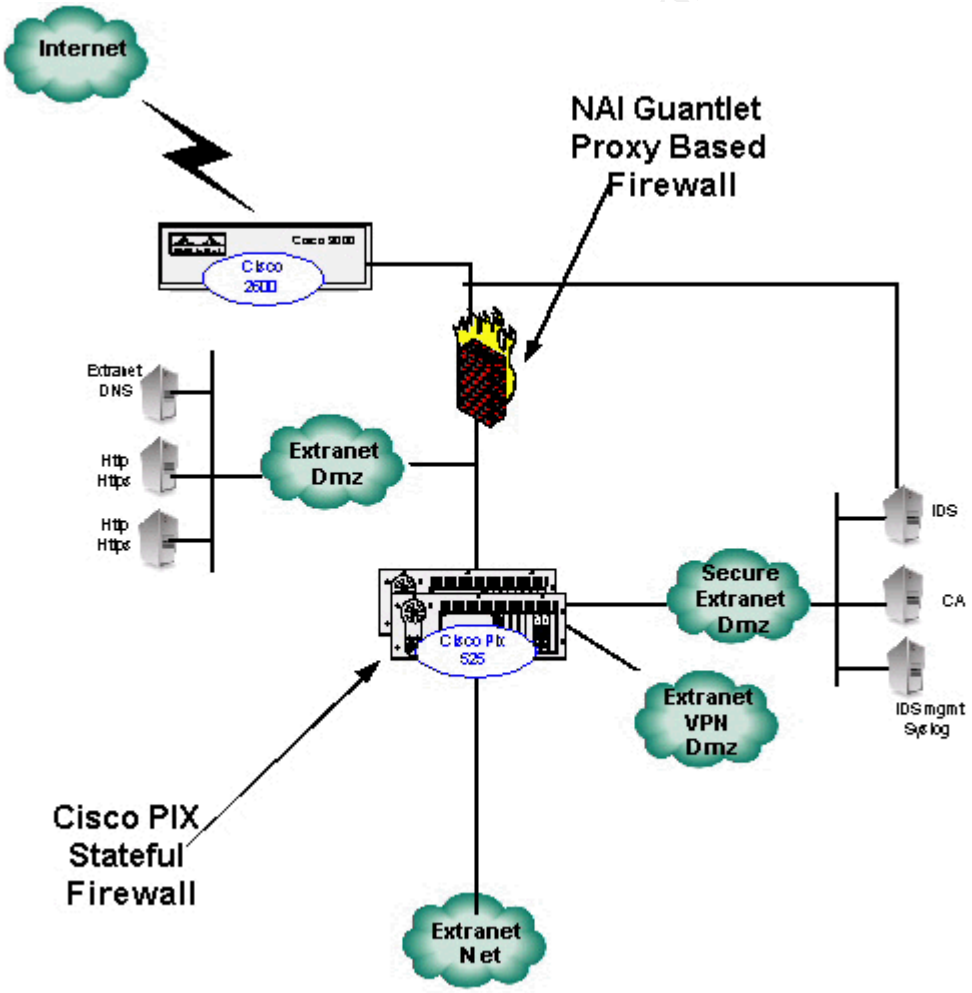
Cisco#(config)line vty 0 4
Cisco#(config-line)transport input none

By default telnet is not allowed on the PIX, however on most occasions the administrator will enable telnet for administrative purposes. The terminal server would alleviate this requirement.

Perimeter Analysis (Cont.)

Incorporate a Proxy based firewall

A way to strengthen the network perimeter would be to incorporate a proxy based firewall into the perimeter architecture on the EIP network segment. I would recommend placing the proxy-based firewall on the EIP segment only. One of the key principles for a security engineer to keep in mind is that all of this "stuff" is done not to give security engineers and consultants something to do, but to facilitate business communication and improve business processes. The security that accompanies these networks is an insurance policy and one must gauge the level of security that is needed based on the perceived value of information that could be exposed. It would certainly be more secure to add a proxy based firewall to the CIP network segment, however based on the perceived level of risk I don't think this would be advantageous.



Perimeter Analysis (Cont.)

Incorporate a Proxy based firewall (cont.)

The traditional difference between stateful and proxy firewalls are becoming less significant in newer firewall software. Today, many stateful firewalls have proxy capabilities for protocols such as http, smtp and ftp. The primary advantage of adding a proxy based firewall into the EIP infrastructure is to add another layer of security and to incorporate a different brand and type of firewall.

Assignment Four

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.

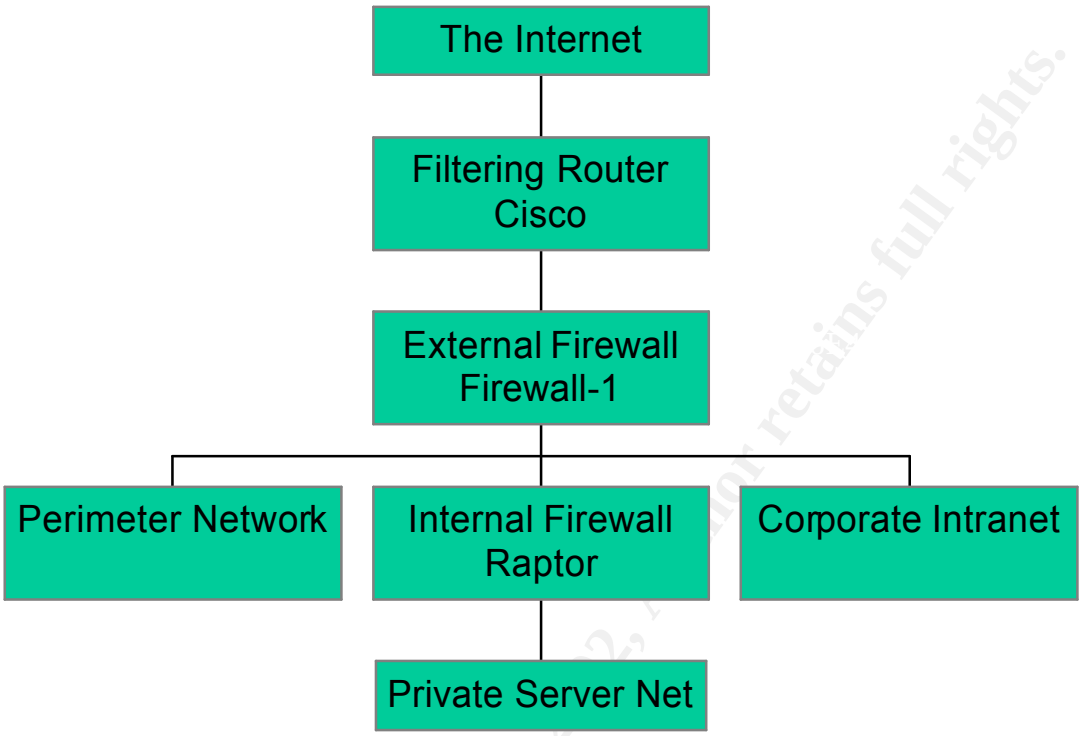
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Note: this is the second time this assignment has been used. The first time, a number of students came up with magical "hand-waving" attacks. You must supply documentation (preferably a URL) for any vulnerability you use in your attack, and the exploit code that you use to accomplish the attack. The purpose of this exercise is for the student to clearly demonstrate they understand that firewall and perimeter systems are not magic "silver bullets" immune to all attacks.

Targeted Network

The network I have chosen can be found at http://www.sans.org/y2k/practical/Jeffery_Roth_GCFW.doc and has been developed by Jeffery Roth.

GIAC Enterprises Security Architecture



The border router is a Cisco 3660 router running IOS 12.1. The Internet firewall is a Sun Ultra 60 running Check Point Firewall-1 4.1, also known as Check Point 2000, on Solaris 2.6. The Internal firewall is a Sun Ultra 10 running (Axent, now Symantec) Raptor 6.5 on Solaris 2.6. Intrusion detection systems are 300 MHz Pentium III Microsoft Windows NT 4.0 workstations running ISS Real Secure 5.0. Host based intrusion detection is also deployed on critical servers including all servers on the perimeter network, all servers on the private server network, all NT domain controllers and all DNS servers.

Firewall Attack

The firewall attack will be against the perimeter firewall. The perimeter firewall is running Check Point Firewall-1 on Solaris 2.6. One of the problems with the Check Point Firewall is that it is a software package that must run on top of an operating system. Configured properly this is just as secure as a hardware-based firewall. However, many organizations lack the personnel to secure the operating system properly.

Known Vulnerabilities

- Check Point Firewall-1 4.1
  - Fragmented Packets DoS vulnerability
  - Denial of service vulnerability
  - Unauthorized RSH/REXEC connection vulnerability
  - SMTP resource exhaustion vulneratility

http://www.securityfocus.com/
http://rootshell.com/
http://www.cert.org/vul_notes/VN-2000-02.html
http://www.checkpoint.com/techsupport/alerts/ipfrag_dos.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0482

- Solaris 2.6
  - Buffer overflow in Sun Solstice AdminSuite daemon sadmind

http://www.cert.org/advisories/CA-1999-16.html

I will demonstrate an attack using the Fragmented Packet DoS vulnerability. Lance Spitzner discovered this vulnerability. An excellent problem description can be found http://www.enteract.com/~lspitz/fwtable.html. The following excerpt was taken from the discussion of the vulnerability directly from http://www.securityfocus.com.

"By sending illegally fragmented packets directly to or routed through Check Point Firewall-1, it is possible to force the firewall to use 100% of available processor time logging these packets. The Firewall-1 rule base cannot prevent this attack and it is not logged in the firewall logs."

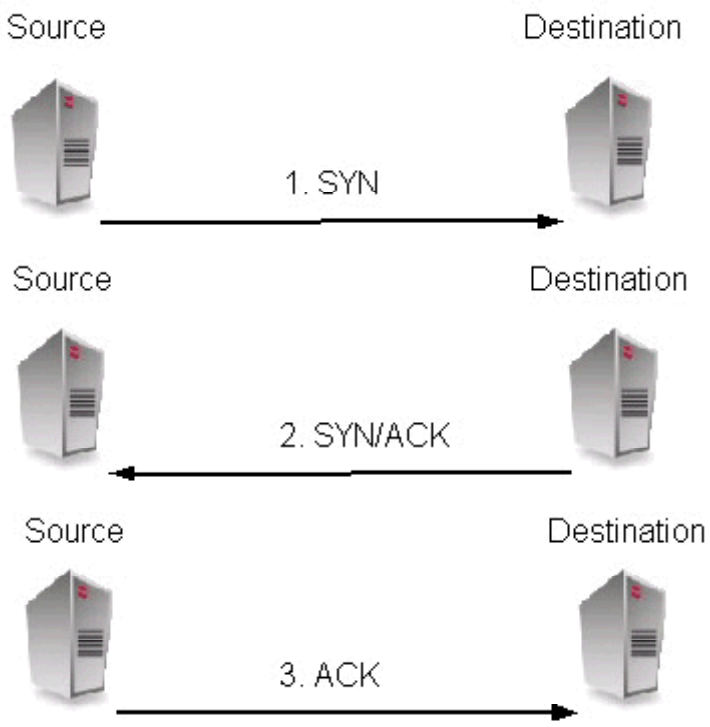
The vulnerability is a result of the software architecture and the way Firewall-1 manages its state table and TCP/IP reassembly. This exploit can't be defended against without disabling console logging. Firewall-1 does not log packets until they have been reassembled. Since the firewall has been sent a large amount of malformed fragmented packets, it spends most if not all of it processing time trying to reassemble these fragmented packets. This vulnerability can be exploited by downloading and compiling Jolt2.c. Running this script will send thousands of fragmented packets at the targeted Checkpoint firewall causing it to stop responding.

Denial of Service Attack

TCP Syn Flood

A TCP Syn flood is a specific type of denial of service (DoS) attack. To completely understand this attack, it is important to understand TCP connection establishment.

TCP is a connection-oriented protocol that uses a three-way handshake to establish a connection. Connection-oriented means that TCP is a reliable protocol and requires an acknowledgement before any data can be transmitted. The purpose of the three-way handshake is to prepare both the sending and receiving device for the communication that is about to occur. Below is an illustration of the three-way handshake.



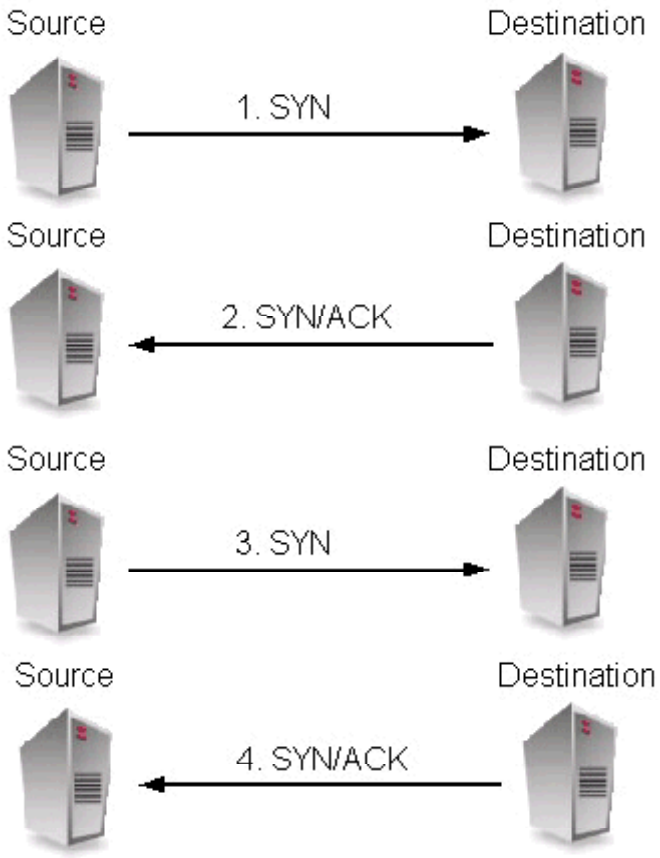
1. A SYN is sent from the source device to the destination device. A SYN is a TCP flag that lets the destination device know that something is about to communicate with it. The SYN flag also alerts the destination device to synchronize its TCP sequence numbers.
2. The destination device in turns sends a SYN/ACK packet back to the source device. The ACK is in acknowledgement of the original SYN. The SYN is sent so the source will synchronize its sequence numbers.
3. The final ACK packet is an acknowledgement of the SYN.

Denial of Service Attack (cont.)

TCP Syn Flood (cont.)

The SYN flood DoS attack can be performed by running a simple tool called Synflood.c. This tool can be pointed at an IP address and used to flood the target with half open requests. The script can be found at the link below. A SYN flood attack could be performed against the CIP firewall by compiling this utility on 50 + Linux hosts and sending thousands of half-open connections to the external IP address of 199.199.199.2.

http://www.hackersclub.com/km/files/c_scripts/



1.
2. The firewall will respond normally with the SYN/ACK flag set and will keep the session open expecting to see a final packet with the ACK bit set.
3. The malicious host running the synflood.c script will create thousands of simultaneous half open connections.
4. The firewall will continue returning a packet with the SYN/ACK flag without ever receiving a final ACK bit to completely establish the session. This activity coming from 50 + malicious hosts on the Internet will easily exceed the firewalls listen queue. Once the firewalls listen queue is filled up, it will no longer accept new

connections.

Denial of Service Attack (cont.)

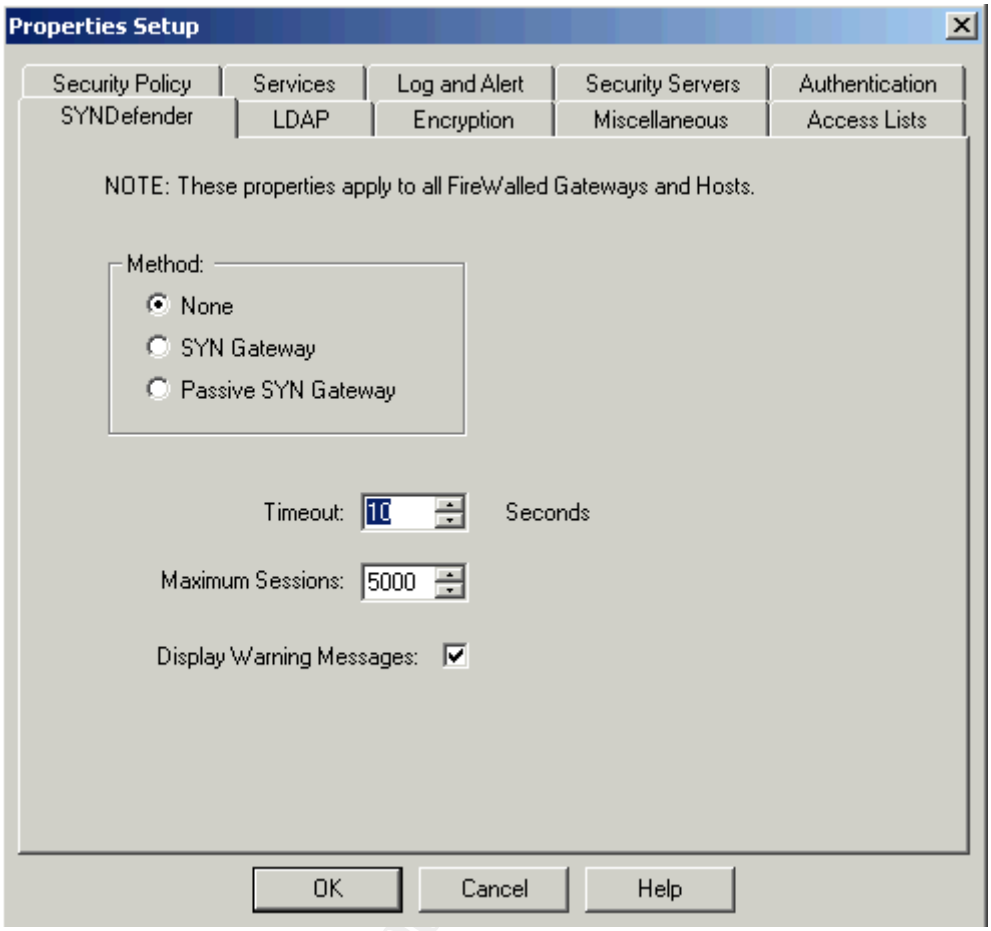
Countermeasures

Checkpoint Firewall-1 has an option called SynDefender that will allow the firewall to proactively watch for SYN packets without the final ACK to create an established session. This is performed by the INSPECT engine and will a RST to the source before it can reach the kernel and fill up the listen queue.

SynDefender is configured through the properties tab of the firewall properties.

SYN Gateway – The SYN Gateway option will cause the Firewall to act as a proxy for the initial TCP three-way handshake. The firewall will not allow any communication to the destination device until the three-way handshake has been completed.

Passive SYN Gateway - Using this option the firewall will allow all connection to the destination device, but will watch all connections for a SYN flood signature.



Internal Compromise

A good way to compromise an internal network is to do so using one of the most widely used services available to a corporate network. , Smtp is used by most, if not all corporate networks connected to the Internet. The following commentary show that steps that could be taken to compromise GIAC's internal network. The primary advantage of using Smtp is because this service is commonly allowed through the firewall and any compromise using SMTP will be undetected by IDS and logging.

Note: The following attack assumes that the VBS script has already been created. However, this attack is identical in theory to the worm viruses such as Melissa and the I Love You virus.

1. An email with the attachment of thisisfunny.jpg would be sent to an internal user at GIAC. Unbeknownst to the user (and there will always be one user to open this), the ".jpg" attachment would actually be a VBS script that would be executed once the user opened the .jpg using Internet Explorer.
2. At this point the host system is compromised and is subject to the actions of the VBS script.

- This script could forward itself to the accounts located in the users address book, much like the recent worm viruses.
- This script could execute a batch file to erase the contents of the users hard drive.
- This script could install a malicious service that could be used for more in-depth attacks.

More information about the vulnerabilities associate with Internet Explorer and VBS scripts reference the following links:

- http://www.nsclean.com/psc-vbs.html
- http://www.sans.org/infosecFAQ/malicious/VBS.htm

The best way to protect against this type of attack is to disable VBS scripting on the browser, if using Internet Expoler.