



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

**SANS GCFW PRACTICAL ASSIGNMENT**  
**Firewall, Perimeter Protection, and VPNs**

**Version 1.7**

**GIAC ENTERPRISES**

By Alfred Ho  
October 5, 2002

Preface .....	4
1. Assignment 1 – Security Architecture.....	5
1.1 Design Principal.....	5
1.2 Access Requirement .....	5
1.2.1 Customers .....	5
1.2.2 Suppliers .....	5
1.2.3 Partners.....	6
1.2.4 GIAC Enterprises employees located internally .....	6
1.2.5 GIAC Enterprises mobile sales force and teleworkers .....	6
1.3 Network Diagram and IP address assignment.....	7
1.4 Individual Components .....	9
1.4.1 Border Router.....	9
1.4.2 Firewall .....	9
1.4.3 VPN.....	9
1.4.4 External Web Server .....	9
1.4.5 External Mail Server .....	10
1.4.6 External DNS.....	10
1.4.7 Internal Netfilter Firewall.....	11
1.4.8 Database Server .....	11
1.4.9 Application Server .....	11
1.4.10 Syslog Server .....	11
1.4.11 Exchange Server.....	12
1.4.12 Internet DNS.....	12
1.4.13 Internal Web Server.....	12
1.4.14 Backup Server/Library .....	12
1.4.15 Proxy Server.....	13
1.4.16 User Desktop.....	13
1.4.17 NTP Server.....	13
1.4.18 Standby/test Servers .....	13
1.4.19 Cisco Switches .....	13
2. Assignment 2 - Security Policy and Tutorial .....	15
2.1 Border Router .....	15
2.1.1 General Configuration .....	15
2.1.2 Access Control List (ACL) .....	19
2.1.3 Create and apply access list to line interfaces.....	20
2.1.4 Create and apply inbound access list to GIAC network and to the router .....	20
2.1.5 Create and apply outbound access list to the internet.....	22
2.2 PIX firewall.....	23
2.2.1 General PIX configuration .....	23
2.2.2 Packet Filter (access list) on the “outside” interface.....	25
2.2.3 Packet filter for interface edmz1 .....	25
2.2.6 Packet filter for interface inside .....	26
2.3 VPN .....	28

2.3.1	General Configuration .....	28
2.3.2	Group and user Configuration .....	34
2.3.3	Policy Management.....	38
2.3.4	Administration setting.....	39
2.3.5	Save VPN 3005 configure .....	40
3.	Assignment 3 – Audit.....	42
3.1	Plan Audit.....	42
3.1.1	Select Audit schedule.....	42
3.1.2	Scope of work - consultant.....	42
3.1.3	Notification.....	43
3.1.4	Tools.....	43
3.2	Implementation.....	43
3.2.1	Setup.....	43
3.2.2	Port scan and OS fingerprint from PIX outside interface .....	43
3.3	Evaluate the audit.....	52
4.	Design Under Fire.....	54
4.1	An Attack against the firewall itself .....	54
4.1.1	Attack #1 .....	54
4.1.2	Attack #2 .....	54
4.2	A denial of service attack.....	55
4.2.1	Attack #1 .....	55
4.3	An attack plan to compromise an internal system .....	56
	References: .....	57

© SANS Institute 2000 - 2002

## **Preface**

GIAC Enterprises is a startup company established in June, 2002, the head office is located in Vancouver, Canada. The primary business is selling Fortune Cookie via internet.

The company vision expands the business expand 40% each year in the first 3 years. In order to support the company vision and support different customers at different time zones, selling online through internet is chosen. It is because internet is almost available everywhere, website can serve our customer 7x24 which is more cost effective than the traditional method. Customers can purchase bulk order online through our web site, or through one of the 2 partners (locate in England and Taiwan) or purchase the cookie through our mobile sales force.

© SANS Institute 2000 - 2002, Author retains full rights.

# 1. Assignment 1 – Security Architecture

## 1.1 Design Principal

- A scalable design that will support the business growth.
- Multi-layer design uses 2 or more different vendors/products to secure the network.
- All servers and user desktops are Intel base machine for ease of support.
- Support 2 OSs, Red Hat Linux 7.2 ([www.redhat.com](http://www.redhat.com)) and Windows 2000 ([www.microsoft.com](http://www.microsoft.com)).
- DMZ servers and VPN concentrator have one NIC facing internet (external) and another NIC facing internal network. Traffic initiate from internet will terminate on the external facing NIC.
- Servers are equipped with CD-RW to facilitate installation and backup.
- No real data is stored in the DMZ's servers except configuration setting.
- All OSs are hardened and install with the latest patches.
- Features and services that are not used in a server will be disabled.
- Application or network change must be tested before implementation.
- 128-bit encryption browser must be used.
- All network equipment and servers are locked in cabinets and stored in the data center with tight access control
- Unused switch Ethernet ports are disabled.

## 1.2 Access Requirement

### 1.2.1 Customers

Customers with internet access with browser that supported 128-bit encryption can visit GIAC external web site to purchase bulk order. The customer web traffic is filtered by the firewall and only allows http (tcp port 80) and SSL (tcp port 443) to pass the firewall and communicate with GIAC external web site. The customer can also contact the GIAC employees via phone or email ([cust@giac.com](mailto:cust@giac.com)).

Customer credit card validation (credit card number, credit, confirmation number) is handled by the applications server which is located in internal network, the application server will forward the information to the bank using SSL and record all transaction records.

### 1.2.2 Suppliers

Suppliers also connect to the same external website as normal customers through http (tcp port 80). Once the GIAC home page is display, click the

“Suppliers” link will redirect the supplier to a secure web page uses SSL (tcp port 443) protocol. It will prompt the supplier for entering username and password. If login correctly, the supplier can submit invoices, view invoices and view his transaction history.

### 1.2.3 Partners

Partners connect to the same external website as customer and suppliers. Once the GIAC home page is display, click the link “Partners” will redirect the partner to a secure web page uses SSL (tcp port 443) protocol. It will prompt the partner for entering username and password. If login correctly, the partner can view special promotion, submit order, check order status and view transaction history.

### 1.2.4 GIAC Enterprises employees located internally

Internal employees require access to email, order process, internet and internal servers.

- Email access  
User uses Microsoft Windows 2000 with Outlook 2002 to access the Microsoft Exchange server. Incoming email from internet will be redirected to the mail gateway (sendmail) in DMZ1, scan for viruses. If it is virus free, it will forward to the internal Exchange server. Outgoing mail will be sent from Exchange server to the mail gateway and the mail gateway will forward the email to the destination.
- Order process  
All order related information can be accessed through the link at the intranet website. Click the “Order” link, the user will be redirected to a secure web page. It will prompt for entering username and password. If login correctly, the user can view, change and add order depends on his/her permission preset by the security officer.
- Internet access  
GIAC standard desktop browser is Microsoft Internet Explorer, it is configured to use proxy server for all web related traffic, no direct internet traffic is allowed. The proxy server is Microsoft proxy server 2.0 running on a Windows 2000 server, it will check and make sure the user is belongs to the “internet users” group in the GIAC Windows’ domain before any traffic will be proxy out to the internet.

### 1.2.5 GIAC Enterprises mobile sales force and teleworkers

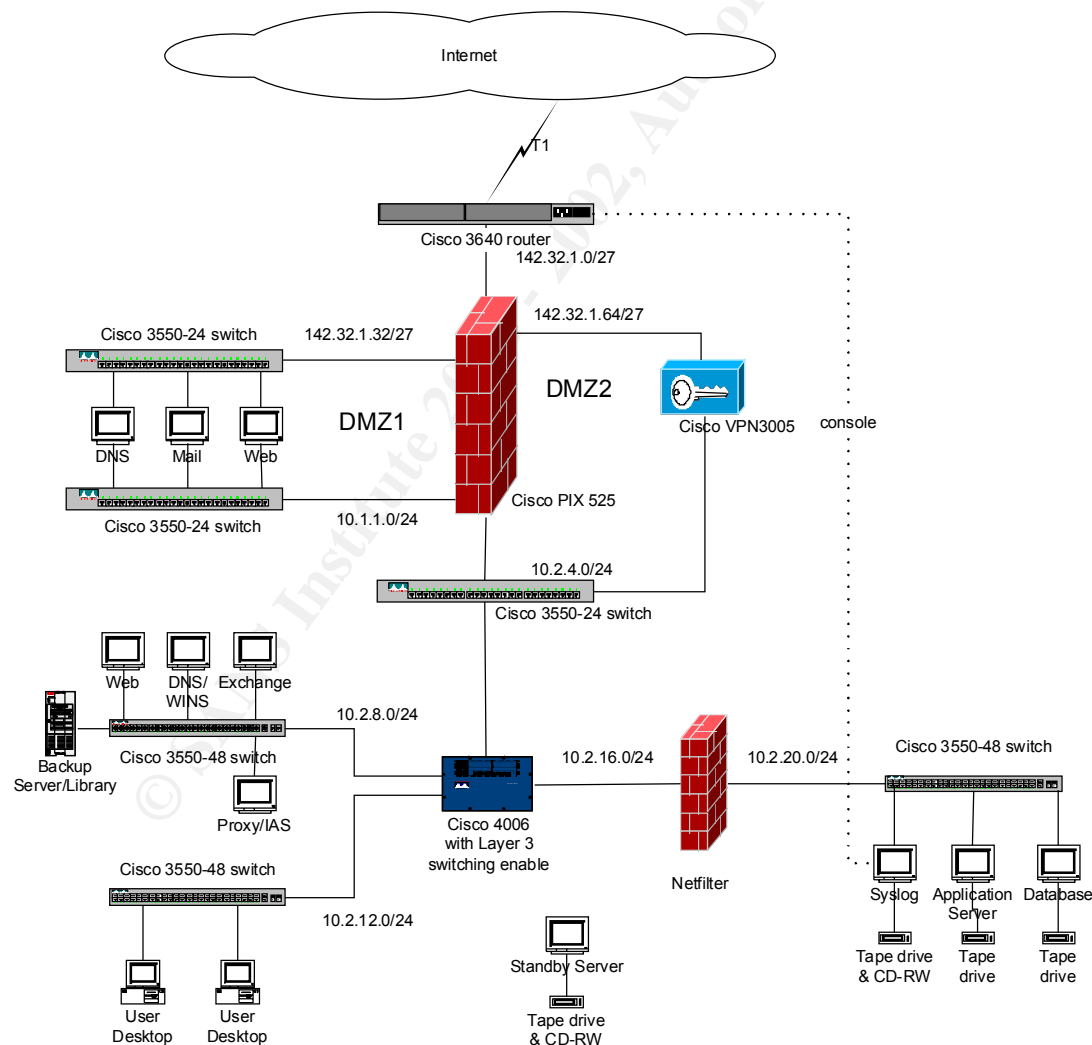
Mobile and teleworkers will be accessing GIAC internal network using the pre-install Cisco VPN client in their laptops via internet. In addition to the Cisco VPN client software, each laptop is protected by McAfee ([www.nai.com](http://www.nai.com)) virus scan software and ISS BlackICE ([www.iss.net](http://www.iss.net)) personal firewall. The virus scan software will protect the laptop from being infected by virus and the BlackICE personal firewall will protect the laptop from unauthorized access from internet.

No VPN split tunnel is allowed because an attacker can hijack the user laptop from internet and gain access to GIAC internal network.

GIAC provides high speed internet access (cable modem or ADSL) for those who need to work from home. Others remote users that do not have high speed internet access will use AT&T internet dial up account.

VPN client software and VPN 3005 concentrator ([www.cisco.com](http://www.cisco.com)) are configured to accept IPSec (ESP-3DES-MD5) protocol only, shared secret password is used plus Windows user id and password to authenticate user. The VPN concentrator will pass the windows user id and password via RADIUS protocol to Microsoft IAS server, if the user belongs to "vpn users" Windows' domain group and password is corrected. The VPN tunnel will establish.

### 1.3 Network Diagram and IP address assignment





IP Address	Subnet mask	Comment
142.32.1.0	255.255.255.224	PIX's external interface subnet
142.32.1.1		Cisco 3640 f0/0 interface
142.32.1.3		PIX's external interface
142.32.1.5		PAT
142.32.1.32	255.255.255.224	DMZ1 external subnet
142.32.1.33		PIX's DMZ1 external interface
142.32.1.35		External Web server's external interface
142.32.1.37		External Mail server's external interface
142.32.1.39		External DNS server's external interface
142.32.1.64	255.255.255.224	DMZ2 external subnet
142.32.1.65		PIX's DMZ2 external interface
142.32.1.67		VPN 3005's external interface
10.1.1.0	255.255.255.0	PIX's DMZ1 internal subnet
10.1.1.1		PIX's DMZ1 internal interface
10.1.1.35		External Web server's internal interface
10.1.1.37		External Mail server's internal interface
10.1.1.39		External DNS server's internal interface
10.1.3.0	255.255.255.0	VPN 3005 internal pool address
10.2.1.0	255.255.255.0	Cisco 4006 management subnet
10.2.1.1		Cisco 4006 management subnet's router ip
10.2.1.10		Cisco 4006 management ip
10.2.4.0	255.255.255.0	Segment between primary firewall and Cisco 4006
10.2.4.1		Cisco 4006 router interface
10.2.4.21		PIX's internal interface
10.2.8.0	255.255.255.0	Servers subnet
10.2.8.1		Cisco 4006 router interface for server subnet
10.2.8.10		Cisco 3550-48 management ip
10.2.8.21		Exchange Server
10.2.8.23		Internal DNS
10.2.8.25		Internal Web
10.2.8.27		Proxy
10.2.8.29		Backup Server/Library
10.2.12.0	255.255.255.0	User subnet
10.2.12.10		Cisco 3550-48 management ip
10.2.16.0	255.255.255.0	Segment between Netfilter and Cisco 4006
10.2.16.1		Cisco 4006 router interface for Netfilter segment
10.2.16.21		Netfilter interface
10.2.20.0	255.255.255.0	Secure servers subnet
10.2.20.10		Cisco 3550-48 management ip
10.2.20.21		Netfilter ip
10.2.20.23		Syslog server
10.2.20.25		Application server
10.2.20.27		Database server

## 1.4 Individual Components

### 1.4.1 Border Router

The border router is a Cisco 2621XM router running IOS version 12.2.12.

- 2621XM provides a cost effective solution that can support future growth, maximum throughput is 30K pps (packet per second) and with the current traffic, the CPU utilization is running at 4%.
- Cisco is chosen because of its reputation in the router market and its technical support is one of the best in the networking industry.
- GIAC has 2 network specialists with at least 3 years experienced in Cisco router, switch and VPN products. No training is required.
- Router cost is \$4,700

### 1.4.2 Firewall

Cisco PIX 515UR running 6.2.6 software is chosen.

- Again, PIX is one of the leading firewall in the market. Price and performance are competitive with other vendors' product.
- Our 2 network specialists have experienced (setup and support) with the PIX.
- It is easier to maintain a hardware based firewall (not susceptible to attack on the underlying operating system).
- Our Design Principal defined in section 1.1 recommends multi-layer design. Although both router and PIX are Cisco products, the underlying design is different (Cisco acquired Network Translation in 1995).
- Firewall cost is \$9,000.

### 1.4.3 VPN

Cisco VPN 3005 concentrator running 3.5.6 software is chosen.

- It can handle 100 simultaneous sessions which is 3 times the current user base.
- Build-in load balancing and failover features. A second VPN 3005 can be easily added to share the load. Availability is higher than relying on one single device to handle all the traffic.
- Authenticated VPN users are only allowed to access the internal server subnet (10.2.8.0).
- Our design principal recommends multi-layer products, therefore, PIX is not used for VPN. Although PIX and VPN 3005 are Cisco products, the underlying design is also different (Cisco acquired Altiga Network which made the VPN 3000 series).
- VPN 3005 cost is \$4,500.

### 1.4.4 External Web Server

The external web server is running Apache 2.0.40 on a Redhat 7.2 Linux machine.

- Hardened OS

- VeriSign certificate ([www.verisign.com](http://www.verisign.com)) is installed.
- Only accept http (tcp port 80) and ssl (tcp port 443) with 128-bits encryption. For those customers that do not have 128-bits browser, they can contact GIAC or partner to order the cookie.
- WebLogic ([www.bea.com](http://www.bea.com)) plug-in is installed to communicate with the application server (WebLogic Server) using "http tunnel".
- Two NICs. One NIC handles internet traffic and the other NIC handles traffic between the web server and application server. The design is better than using one interface because it segregates the internet traffic and the internal traffic which makes troubleshooting easier.
- The external interface uses PIX edmx1 interface as default gateway. Multiple static routes are used in the server to control the traffic route towards the internal hosts via the PIX's idmx1 interface as gateway. The internal hosts include application server, internal NTP server and syslog server.
- Server does not contain real data except the static web pages. CD-RW driver is used to backup and update Apache configuration files and web pages. Daily backup is not required.

#### 1.4.5 External Mail Server

The external mail server is running Sendmail 8.12.6 ([www.sendmail.org](http://www.sendmail.org)) on Redhat 7.2 Linux machine.

- It acts as a gateway for all inbound and outbound email messages.
- McAfee virus scan software is installed.
- The external interface uses PIX edmx1 interface as default gateway. Multiple static routes are used in the server to control the traffic route towards the internal hosts via the PIX's idmx1 interface as gateway. The internal hosts include Exchange server, internal NTP server and syslog server.
- The server also does not contain real data. CD-RW driver is used to backup and update Sendmail configuration files. Daily backup is not required.

#### 1.4.6 External DNS

The external DNS is running BIND 9.2.2rc1 ([www.isc.org](http://www.isc.org)) on a Redhat 7.2 Linux machine.

- Primary and authoritative DNS server for the giac.com domain.
- It allows any host from internet to do query using udp port 53. TCP port 53 is limited for zone transfer between our External DNS server and the ISP DNS server. The ISP DNS server is acted as the secondary DNS server for giac.com.
- Responsible for providing non-recursive name resolution on behalf of the internal DNS. It uses udp port 53 to query other external DNS servers.
- No entry for any internal host except those in the DMZ (external web, external mail, external DNS and VPN concentrator).

- The external interface uses PIX edmz1 interface as default gateway. Multiple static routes are used in the server to control the traffic route towards the internal hosts via the PIX's idmz1 interface as gateway. The hosts include internal DNS server, internal NTP server and syslog server.
- Since the server has a few static DNS records, CD-RW driver is used to backup the BIND configuration files. Daily backup is not required.

#### 1.4.7 Internal Netfilter Firewall

The internal Netfilter firewall is running Netfilter Iptables 1.2.7a on a Redhat 7.2 Linux machine.

- Acts as a second layer firewall to protect mission critical applications and data.
- Prevent unauthorized access to critical server segment.
- Low cost solution which also meet the GIAC's Design Principal (multi-layer products).

#### 1.4.8 Database Server

The database server is running Oracle 9 ([www.oracle.com](http://www.oracle.com)) on a Redhat 7.2 Linux machine.

- RAID 5 design.
- External tape backup drive which supports up to 256GB (incremental backup from Monday to Saturday and full backup on Sunday).

#### 1.4.9 Application Server

The database server is running BEA version 7 ([www.bea.com](http://www.bea.com)) on Redhat 7.2 Linux machine. The server only accepts the "http tunnel" traffic from the internal and external web server with WebLogic plug-in to the Apache application.

#### 1.4.10 Syslog Server

The syslog server is running SL4NT 3.0 ([www.netal.com](http://www.netal.com)) on a Windows 2000 workstation.

- Responsible to capture syslog messages collects from network devices and servers except the Border Router and the Ethernet switch in the external side of DMZ1.
- The SL4NT software is configured to write captured messages to different log files. There are 5 different log files setup - ALL, router, switch, server and firewall. The setup helps to troubleshoot network, security and application problem more easily. The "ALL" log provides centralized view of all messages which is particular useful for network wide security problem.
- Daily log is setup (new log file everyday).
- If any message matches a predefine pattern and threshold, SL4NT sends an email alert to the network group.
- Terminal emulation software Tera Term Pro (<http://hp.vector.co.jp/authors/VA002416/teraterm.html>) is installed to

capture Border Router console messages remotely. Script is used to save the capture into a daily log file every mid-night.

- Tape drive is used to backup the log files every night. Monthly backup is written to CD and will be kept for one year.
- Accept standard udp port 514 only.

#### 1.4.11 Exchange Server

The Exchange server is running Microsoft Exchange 2000 on a Windows 2000 Advanced Server machine.

- Exchange 2000 is chosen because of better integration with other Microsoft software that GIAC is using (e.g. Microsoft Office, NetMeeting).
- ScanMail for Exchange 2000 from Trend Micro Inc. is installed. Different virus scan software from the user desktop and external mail gateway to maximized protection.
- All outgoing email will be forwarded to the mail gateway in DMZ1 uses standard SMTP (tcp port 25) protocol.
- Employees use Outlook 2002 to connect to the Exchange 2000 server.
- Veritas client software is used for backup the data to the Backup Server.

#### 1.4.12 Internet DNS

The internal DNS is running Microsoft DNS on a Windows 2000 Advanced Server machine.

- Only contains internal host entries.
- Unresolved name will forward to external DNS server in DMZ1.
- WINS is also enable on the same machine to reduce the cost of acquire another machine.
- Veritas client software is used for backup the data to the Backup Server.

#### 1.4.13 Internal Web Server

The internal web server is running Apache 2.0.40 ([www.apache.org](http://www.apache.org)) on Redhat Linux 7.2 machine.

- Same hardware, OS, applications that runs in the external web server for ease of support.
- WebLogic plug-in is installed to communicate with the application server (WebLogic Server) using "http tunnel".
- Accept tcp port 80 and 443 traffic.
- Serve as an intranet web site for employee.
- Veritas client software is used for backup the data to the Backup Server.

#### 1.4.14 Backup Server/Library

The backup server is running Veritas NetBackup 4.5 ([www.veritas.com](http://www.veritas.com)) on a Windows 2000 Advanced Server machine with 512GB tape library.

#### 1.4.15 Proxy Server

The proxy server is running Windows Proxy 2.0 on a Windows 2000 Advanced Server machine.

- Internet Explore 5.5 is the current supported browser in GIAC and is configured to use proxy server for all browser related traffic. The proxy server accepts client traffic uses tcp port 8080.
- Employee's user id must belongs to "Internet users" Windows domain group in order to gain access to internet.
- User id, timestamp and URL are logged in the proxy log.
- Content caching is enable to improve response time.
- Microsoft Internet Authentication Server (IAS) is installed on the same server to handle RADIUS authentication requests from VPN 3005 concentrator, PIX 515UR firewall and internal network devices (router and switches except Border Router and the switch on the external side of the DMZ1). The IAS uses RADIUS authentication port 1645 and accounting port 1646.

#### 1.4.16 User Desktop

Desktops are running Windows 2000 workstation. The standard GIAC desktop image includes Windows Office XP, Veritas client, McAfee anti-virus software 4.5.1 and IE 5.5 proxy set to port 8080 (bypass proxy server for local address enable). The virus scan software different from the Exchange server to maximize virus protection.

#### 1.4.17 NTP Server

The core backbone switch, Cisco 4006, is acted as the NTP server to serve internal and DMZ devices except Border Router and external switch in DMZ1 which require manual synchronization. The core switch synchronizes with two external clocks uses udp port 123 to increase accuracy.

#### 1.4.18 Standby/test Servers

There are two standby servers, a RedHat 7.2 Linux and a Windows 2000 Advanced Server. There are two test servers, a RedHat 7.2 and a Windows 2000 Advanced Server. Applications changes and patches are tested before applying to production system.

#### 1.4.19 Cisco Switches

In view of GIAC enterprise network is still pretty small and a good SNMP management software will cost a lot of money. Therefore, SNMP management is not really required at this stage. Switches configuration are captured via console and store in the syslog server uses PGP (<http://web.mit.edu/network/pgp.html>) to encrypt the files.

The external switch in DMZ1 is specially configured with 2 VLANs and all remote management services are disabled. VLAN1 is assigned to "interface vlan 1" and VLAN2 is assigned to all Fast Ethernet interfaces "interface fastethernet 0/1 to

interface fastethernet 0/24". Therefore, any configuration change must be done via console.

© SANS Institute 2000 - 2002, Author retains full rights.

## 2. Assignment 2 - Security Policy and Tutorial

This section will walk through how to configure the Border Router, Primary Firewall and VPN to meet our security policy plus some background information of why they are needed.

### 2.1 Border Router

The border router is a Cisco 2621XM running IOS 12.2.12 with 64M DRAM, 16M Flash memory, two fast Ethernet ports (part #: NM-2FESW) and two serial WAN interfaces (part #: WIC-2T).

Before we start configuring a router, we are going to use a Windows 2000 laptop with Tera Term Pro terminal emulation software, then connects the laptop to the router console port using the provided DB-9 connector and console cable. Power on the router, Tera Term Pro will display the router's bootup messages which include IOS software version, installed module, memory, etc. When the router completes the bootup sequence, it will display a message "Press RETURN to start". By hitting the RETURN key, we will enter the non-privileged mode.

```
router>
```

The non-privileged mode is used to view router status and statistical information. The next mode is called Privileged mode which is used to view the router status, statistical information and router configuration. Type **enable** at the non-privileged mode's router prompt, the router will enter the privileged mode (please note the router prompt has changed).

```
router#
```

Now, we can view the router current configure by using **show running-config** or view the configuration stores in the memory by using **show startup-config**. The next mode is called Global Configuration mode which is used to edit router configure. Type **configure terminal** at privilege mode to enter the Global Configuration mode.

```
router(config)#
```

#### 2.1.1 General Configuration

Router host name is set by **hostname** command. We pick the one of the local mountain's names (no hint that it is a router) which we believe it will reduce the risk of attracting Denial-of-Service (DOS) attack to our router.

```
router(config)# hostname seymour
```



Assign unique login name and password to each administrator for audit purposes.

```
seymour(config)# username jjone password haV8ingfun
```

In order to reduce the risk that someone can easily login to our router by viewing the clear text password stores in the configuration files, we turn on password encryption to encrypt the password. The encrypted password uses a simple Vigenere cipher which is not designed to protect the router configuration file from experience attackers.

```
seymour(config)# service password-encryption
```

Privileged mode access is protected by enable password which can be setup by using `enable password <password>` or `enable secret <password>`. The latter command is more secure because it uses MD5 to encrypt the password.

<sup>1</sup> Disable enable password first, then use enable secret  

```
seymour(config)# no enable password  
seymour(config)# enable secret s8cur8Giac
```

Configure login banner that warns user against unauthorized access. It is wise not to include any router information (router name, model, etc.) in the banner because the information may help attacker to attack the router.

```
seymour(config)# banner motd *WARNING: Unauthorized Access Is Prohibited*
```

Cisco Discovery Protocol (CDP) is used to discover other Cisco devices' model, IOS version and ip addresses which is directly connected in the same segment. To minimize the chance that attacker can get hold with these information from CDP, we will disable CDP in our configuration.

```
seymour(config)# no cdp run
```

Standard TCP and UDP implementation comes with some small services (echo, chargen, discard and daytime services) which are never required in GIAC network and are disabled.

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

Unix like finger service will also be disabled to avoid releasing user information to the attacker.

```
seymour(config)# no ip finger  
seymour(config)# no service finger
```

---

<sup>1</sup> "!" means comment

HTTP and SNMP can be used to remote manage a router but our security policy defines Border Router can only be accessed via console. Therefore, HTTP and SNMP are be disabled. **no snmp-server** will shutdown all SNMP processes but the original SNMP configuration may still be there but not appear in the running-config. It is better to disable snmp-server and related services individually.

```
seymour(config)# no ip http server  
seymour(config)# no snmp-server  
seymour(config)# no snmp-server enable traps  
seymour(config)# no snmp-server system-shutdown  
seymour(config)# no snmp-server trap-auth  
seymour(config)# no snmp-server tftp-server-list  
seymour(config)# no snmp-server trap-source
```

Cisco router can act as a bootp server for other Cisco hardware but this is not required.

```
seymour(config)# no ip bootp server
```

Cisco router is capable to load startup configuration from local memory or from the network. It is less secure to load the configuration through the network and is disabled.

```
seymour(config)# no boot network  
seymour(config)# no service config
```

Source routing bit in IP header will allow sender to specify the routing path of a packet. If a router allows source-route packet to pass through, spoofed packets will able to route back to the attacker. Some old machine may even crash because it cannot handle source route packet properly. Therefore, this feature is disabled.

```
seymour(config)# no ip source-route
```

Cisco router can use domain name lookup to resolve unknown host name but there is no need to resolve name in the Border Router and is disabled.

```
seymour(config)# no ip domain-lookup
```

Disable **ip classless** routing stops a router forwarding packet to the best available supernet route if it has no default route setup. It is a good practice not to route unknown route's packet to internet.

```
seymour(config)# no ip classless
```

Router with proxy ARP turn on will respond to ARP requests for hosts that it knows about but are not directly reachable by the host that makes the ARP request. If it is enabled, transparent access between multiple subnets is allowed and traffic may be able to bypass our access control. Disable this service in each interface

```
seymour(config-if)# no ip proxy-arp
```

An attacker can send illegitimate traffic to target subnet's broadcast address to create denial-of-service attack. By disable directed-broadcast service in each of the interfaces will stop router from forwarding such traffic.

```
seymour(config-if)# no ip directed-broadcast
```

When a router receives non-broadcast message for a protocol or subnet that it does not recognize, it returns an ICMP unreachable message back to the source host. Therefore, an attacker uses UDP scan will be able to find out what services are active in target router. Use **no ip unreachables** in each interface to disable sending ICMP unreachable message.

```
seymour(config-if)# no ip unreachables
```

Redirect message is normally sent by a router to a host to indicate which router it can use. An attacker can use a host to send out redirect message to confuse the router and host. Use **no ip redirects** on each interface will stop router from forwarding such traffic.

```
seymour(config-if)# no ip redirects
```

NTP is used to automatically synchronize time between network devices. There is no need for NTP because Border Router's clock is set manually everyday.

```
seymour(config)# no ntp  
seymour(config-if)# no ntp disable
```

Timestamp log messages use router's local time will help to review when and what happened locally to the router and it can also be used to correlate events with other devices.

```
seymour(config)# service timestamps debug datetime msec localtime  
seymour(config)# service timestamps log datetime msec localtime
```

Border Router uses both console logging for long term and buffer logging for short term record.

```
seymour(config)# logging on
seymour(config)# logging console informational
! set the buffer to 16384 bytes and severity equals to informational
seymour(config)# logging buffered 16384 informational
```

### 2.1.2 Access Control List (ACL)

Access list is a sequential collection of permit and deny conditions used to control each packet that is allowed or disallowed to access a router or passing through a router to another network. The router tests addresses against the conditions in an access list one by one, it stops testing conditions when a first match condition is found. The first match will determine whether the router accepts or rejects the packet. Therefore, the order of the conditions is critical. If no conditions match, the router rejects the packet.

There are ACL for IP, IPX and AppleTalk in Cisco router but we focus on IP ACL because Border Router will only route IP packet. Two most commonly used IP ACLs are Standard and Extended, the other kind such as Reflexive ACL which is not going to be used in our configuration and won't be discussed in this document.

Standard access list checks each packet source ip and/or wildcard for a match condition, it uses access list number 1 to 99 and each access list number can have more than one condition. The syntax for defining access list is:

```
access-list access-list-number { deny | permit } { source [source-wildcard] | any }
```

The syntax for apply access list to an interface in configuration mode:

```
ip access-group access-list-number { in | out }
```

The syntax for apply access list to terminal lines:

```
access-class access-list-number { in | out }
```

Extended access list checks each packet protocol type, protocol source and destination port number, source and destination addresses for a match condition. It uses access list number 100 to 199 and each access list number can have more than one condition.

The syntax for defining access list for IP:

```
access-list access-list-number { deny | permit } ip {source source-wildcard | any} {destination destination-wildcard | any} [protocol-specific options]
```

The syntax for defining access list for ICMP:

```
access-list access-list-number { deny | permit } icmp {source source-wildcard | any} {destination destination-wildcard | any} [icmp-type [ icmp-code] | icmp-message]
```

The syntax for defining access list for TCP:

```
access-list access-list-number { deny | permit } tcp (source source-wildcard | any) [operator source-port | source port] {destination destination-wildcard | any} [operator destination-port | destination-port] [established]
```

The syntax for defining access list for UDP:

```
access-list access-list-number { deny | permit } udp (source source-wildcard | any) [operator source-port | source port] {destination destination-wildcard | any} [operator destination-port | destination-port]
```

The syntax for applying access list to an interface in configuration mode:

```
ip access-group access-list-number { in | out }
```

### 2.1.3 Create and apply access list to line interfaces

The router access policy only allows console access, telnet and AUX access needs to be disabled.

```
seymour(config)# access-list 10 deny any  
seymour(config)# line vty 0 4  
seymour(config-line)# access-class 10 in  
! executive timeout is one second  
seymour(config-line)# exec-timeout 0 1  
! use local username database to login  
seymour(config-line)# login local  
! no transport protocol is allowed  
seymour(config-line)# transport input none  
! switch to AUX line  
seymour(config-line)# line aux 0  
! Disable login  
seymour(config-line)# no exec  
! Switch to CON line  
seymour(config-line)# line con 0  
! Set executive idle timeout to 5 minute  
seymour(config-line)# exec-timeout 5 0  
! Use local username database to login  
seymour(config-line)# login local
```

### 2.1.4 Create and apply inbound access list to GIAC network and to the router

Anti-spoofing means nobody from the internet should be sending packets to our network with the source address of either our network address or certain well-known and reserved addresses. We will configure an access list to drop and log those packets.

```
! drop source address that is the same as our public ip address  
seymour(config)# access-list 101 deny ip 142.32.1.0 0.0.0.63 any log  
! drop source address with first octet all zeros, all ones and loopback network.  
seymour(config)# access-list 101 deny ip 0.0.0.0 0.255.255.255 any log  
seymour(config)# access-list 101 deny ip host 255.255.255.255 any log  
seymour(config)# access-list 101 deny ip 127.0.0.0 0.255.255.255 any log  
! drop class D multicast and class E addresses  
seymour(config)# access-list 101 deny ip 224.0.0.0 15.255.255.255 any log  
seymour(config)# access-list 101 deny ip 240.0.0.7 7.255.255.255 any log
```

```

! drop RFC 1918 addresses
seymour(config)# access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
seymour(config)# access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
seymour(config)# access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
! drop end node autoconfig
seymour(config)# access-list 101 deny ip 169.254.0.0 0.0.255.255 any log

```

New conditions are added to allow customers, partners, suppliers and remote workers to access GIAC applications. These users can access from anywhere, therefore, we will allow all valid ip addresses (after the anti-spoofing conditions) to access our applications. No log is required because PIX will log.

```

! Allow incoming http and ssl traffic to the external web server
seymour(config)# access-list 101 permit tcp any host 142.32.1.35 eq 80
seymour(config)# access-list 101 permit tcp any host 142.32.1.35 eq 443
! Allow incoming SMTP to the external mail server
seymour(config)# access-list 101 permit tcp any host 142.32.1.37 eq 25
! Allow incoming DNS query to the external DNS server
seymour(config)# access-list 101 permit udp any host 142.32.1.39 eq 53
! Allow incoming DNS zone transfer between ISP's DNS 142.32.100.99
! which is the secondary DNS of giac.com (external DNS is the primary server)
seymour(config)# access-list 101 permit tcp host 142.32.100.99 host 142.32.1.39 eq 53
! Allow ISAKMP traffic to the VPN 3005, it goes first because more ISAKMP traffic than ESP
seymour(config)# access-list 101 permit udp any eq 500 host 142.32.1.67 eq 500
! Allow ESP traffic to the VPN 3005
seymour(config)# access-list 101 permit esp any host 142.32.1.67

```

The following conditions allow return traffics/sessions which are initiated from internal network to internet. No log is required because PIX will log.

```

! Return http packet to the PAT address
seymour(config)# access-list 101 permit tcp any eq 80 host 142.32.1.5 ge 1024
! Return ssl packet to PAT address
seymour(config)# access-list 101 permit tcp any eq 443 host 142.32.1.5 ge 1024
! Return NTP packet to PAT address
seymour(config)# access-list 101 permit udp host 192.5.41.40 eq 123 host 142.32.1.5 ge 1024
seymour(config)# access-list 101 permit udp host 129.7.1.66 eq 123 host 142.32.1.5 ge 1024
! Return SMTP packet to external mail server in DMZ1
seymour(config)# access-list 101 permit tcp any eq 25 host 142.32.1.37 ge 1024
! Return DNS response to external DNS server in DMZ1
seymour(config)# access-list 101 permit udp any eq 53 host 142.32.1.39 ge 1024

```

Log everything that does not match any conditions

```

seymour(config)# access-list 101 deny ip any any log

```

Apply access list 101 to the serial interface connects to ISP.

```

seymour(config)# interface s0/0
seymour(config-if)# ip access-group 101 in

```

### 2.1.5 Create and apply outbound access list to the internet.

In order to provide good response to business related traffic, the return packets from external web server to internet will be added right after the spoofed addresses.

```
! Stop well-known and reserved addresses that may send out to internet
seymour(config)# access-list 151 deny ip 0.0.0.0 0.255.255.255 any log
seymour(config)# access-list 151 deny ip host 255.255.255.255 any log
seymour(config)# access-list 151 deny ip 127.0.0.0 0.255.255.255 any log
! drop class D multicast and class E addresses
seymour(config)# access-list 151 deny ip 224.0.0.0 15.255.255.255 any log
seymour(config)# access-list 151 deny ip 240.0.0.7 7.255.255.255 any log
! drop RFC 1918 addresses
seymour(config)# access-list 151 deny ip 10.0.0.0 0.255.255.255 any log
seymour(config)# access-list 151 deny ip 172.16.0.0 0.15.255.255 any log
seymour(config)# access-list 151 deny ip 192.168.0.0 0.0.255.255 any log
! drop end node autoconfig
seymour(config)# access-list 151 deny ip 169.254.0.0 0.0.255.255 any log
! drop destination address that is the same as our public addresses
seymour(config)# access-list 151 deny ip any 142.32.1.0 0.0.0.63 log
! allow return http traffic from external web server
seymour(config)# access-list 151 permit tcp host 142.32.1.35 eq 80 any
! allow return ssl traffic from external web server
seymour(config)# access-list 151 permit tcp host 142.32.1.35 eq 443 any
! allow return ISAKMP traffic from VPN 3005
seymour(config)# access-list 151 permit udp host 142.32.1.67 eq 500 any eq 500
! allow return ESP traffic from VPN 3005
seymour(config)# access-list 151 permit esp host 142.32.1.67 any
! allow return SMTP traffic from external mail server
seymour(config)# access-list 151 permit tcp host 142.32.1.37 eq 25 any
! allow retrun DNS traffic from external DNS
seymour(config)# access-list 151 permit udp host 142.32.1.39 eq 53 any
```

Allow outbound internet traffic from internet users.

```
! allow outbound http traffic from internal users, 142.32.1.5 (NAT address for internal users)
seymour(config)# access-list 151 permit tcp host 142.32.1.5 any eq 80
! allow outbound ssl traffic from internal users.
seymour(config)# access-list 151 permit tcp host 142.32.1.5 any eq 443
! allow outbound SMTP traffic from external mail server
seymour(config)# access-list 151 permit tcp host 142.32.1.37 any eq 25
! allow outbound DNS query from external DNS server
seymour(config)# access-list 151 permit udp host 132.32.1.37 any eq 53
```

Allow outbound ICMP message types Parameter Problem, Packet Too Big, and Source Quench. Parameter Problem and Source Quench packets improve connections by informing problems related to packet headers and by slowing down traffic when it is necessary. Packet Too Big is necessary for Path MTU discovery.

```
seymour(config)# access-list 151 permit icmp 142.32.1.0 0.0.0.63 any parameter-problem
seymour(config)# access-list 151 permit icmp 142.32.1.0 0.0.0.63 any packet-too-big
seymour(config)# access-list 151 permit icmp 142.32.1.0 0.0.0.63 any source-quench
```

Log everything that does not match any conditions

```
seymour(config)# access-list 151 deny ip any any log
```

Apply access list 151 to the Fast Ethernet interface f0/0.

```
seymour(config)# interface f0/0
```

```
seymour(config-if)# ip access-group 151 in
```

## 2.2 PIX firewall

The firewall is a PIX 515UR running software version 6.2.6 with six Fast Ethernet ports (part #: PIX-4E) installed.

To configure PIX, use the same laptop via console connection to the PIX's console port. PIX has the same configuration modes as the router, non-privileged, privileged and configuration modes.

Non-privileged:

```
pixfirewall>
```

Privileged:

```
pixfirewall#
```

Configuration:

```
pixfirewall(config)#
```

### 2.2.1 General PIX configuration

PIX's commands are very similar to router's commands but some are different. If the command is the same as router, detail description will not be provided.

Set the PIX host name to cypress.

```
pixfirewall(config)# hostname cypress
```

Set the non-privileged mode password.

```
cypress(config)# passwd noManz0n8
```

To set the privileged mode password, we use enable password command.

```
cypress(config)# enable password haggyXdaY
```

Since the firewall has 6 interfaces, we need to define the security level of each interface. Higher the number, the more secure. 100 is the maximum and 0 is the minimum. We set the inside interface to 100 (the most secure), inside interface of DMZ1 to 60, outside interface of DMZ2 to 40, outside interface of DMZ1 to 20 and outside firewall interface to 0.

```
cypress(config)# nameif ethernet0 outside security0
```

```
cypress(config)# nameif ethernet1 inside security100
```

```
cypress(config)# nameif ethernet3 idmz1 security 60
```

```
cypress(config)# nameif ethernet4 edmz2 security 40
```



```
cypress(config)# nameif ethernet5 edmz1 security 20
```

By default, all Ethernet interfaces are shutdown. We need to enable each interface and set the speed to auto negotiation.

```
cypress(config)# interface ethernet0 auto
cypress(config)# interface ethernet1 auto
cypress(config)# interface ethernet3 auto
cypress(config)# interface ethernet4 auto
cypress(config)# interface ethernet5 auto
```

Static route is used to route packet from one network to another. Default route is used to route all outbound traffic to the Border Router, a static route routes traffic to internal hosts via PIX's inside interface to the Cisco 4006 switch.

```
cypress(config)# route outside 0.0.0.0 0.0.0.0 142.32.1.1 1
cypress(config)# route inside 10.0.0.0 255.0.0.0 10.2.4.1 1
```

In view of PIX has limited memory, syslog message (severity level "error" and above) is temporary stored in the buffer and uses syslog server to store the message permanently (severity "informational" and above).

```
cypress(config)# logging on
cypress(config)# logging timestamp
cypress(config)# logging buffered errors
cypress(config)# logging host inside 10.2.20.23 udp/514
cypress(config)# no logging console
cypress(config)# no logging monitor
cypress(config)# no logging standby
```

There are 4 remote access methods for administrator to remotely access PIX – Telnet, SSH, Web and IPSec. Telnet and Web access are not recommended because both protocol transport information in clear text. On the other hand, there is no real advantage to use IPSec with DES (3DES license was not purchased) compares with SSH. Therefore, GIAC has adopted to use SSH and RADIUS authentication for remote PIX administration.

! Allow all internal machines use ssh to access PIX.

```
cypress(config)# ssh 10.0.0.0 255.0.0.0 inside
```

! configure RADIUS authentication to internal IAS server to control who can login to PIX

```
cypress(config)# aaa-server sshconsole (inside) host 10.2.8.27 p1xRadius timeout 10
```

```
cypress(config)# aaa-server sshconsole protocol radius
```

```
cypress(config)# aaa authentication ssh console sshconsole
```

! If **show http** shows http server is enabled, disable it by:

```
cypress(config)# no http server enable
```

! If show telnet indicates telnet is setup, disable it by:

```
cypress(config)# show telnet
```

```
10.0.0.0 255.0.0.0 inside
```

```
cypress(config)# no telnet 10.0.0.0 255.0.0.0 inside
```

To enable ntp synchronization, follow the steps below:

```
cypress(config)# ntp authenticate
```

! set the authenticate key to make sure it is not a spoofed ntp source

```
cypress(config)# ntp authenticate-key 101 md5 pacTime
```

! set the NTP server ip address and use inside interface to access the server

```
cypress(config)# ntp server 10.2.4.1 key 101 source inside
```

```
cypress(config)# ntp trusted-key 101
```

To enable Port Address Translation for internal traffic going out to internet that does not have static mapping.

```
cypress(config)# global (outside) 1 142.32.1.5  
cypress(config)# nat (inside) 1 10.0.0.0 255.0.0.0
```

### 2.2.2 Packet Filter (access list) on the “outside” interface

In general, access list is created for each interface and is applied to the inbound traffic. Addresses and/or protocols do not match any condition will be drop except the return packets. In order to let traffic from lower security level interface to the higher security interface, **static** is used to map the higher security ip to a low security ip.

On the “outside” interface, it allows traffic initiated from internet traffic to the external web server, external mail server, external DNS server and VPN.

! Allow web traffic from internet, use **static** to map the web traffic to external web server in DMZ1

```
cypress(config)# static (edmz1, outside) 142.32.1.35 142.32.1.35
```

! Only allow tcp port 80 and 443 to reach the external web server's external interface.

```
cypress(config)# access-list acl_out permit tcp any host 142.32.1.35 eq 80
```

```
cypress(config)# access-list acl_out permit tcp any host 142.32.1.35 eq 443
```

! Allow SMTP from internet to external mail server

```
cypress(config)# static (edmz1, outside) 142.32.1.37 142.32.1.37
```

```
cypress(config)# access-list acl_outside permit tcp any host 142.32.1.37 eq 25
```

! Allow DNS request from internet and Zone transfer from our ISP's DNS server 142.32.100.99

```
cypress(config)# static (edmz1, outside) 142.32.1.39 142.32.1.39
```

```
cypress(config)# access-list acl_out permit udp any host 142.32.1.39 eq 53
```

```
cypress(config)# access-list acl_out permit tcp host 142.32.100.99 host 142.32.1.39 eq 53
```

! Allow VPN traffic (ESP and ISAKMP) to the VPN 3005

```
cypress(config)# static (edmz2, outside) 142.32.1.67 142.32.1.67
```

```
cypress(config)# access-list acl_out permit 50 any host 142.32.1.67
```

```
cypress(config)# access-list acl_out permit udp any eq 500 host 142.32.1.67 eq 500
```

! Apply access-list acl\_out to outside interface

```
cypress(config)# access-group acl_out in interface outside
```

### 2.2.3 Packet filter for interface edmz1

External DNS server and external mail server allows to initiate traffic to internet on behalf of the internal clients, access list will be created to permit the specific traffic to go through the firewall. The external web server does not need to initial outgoing traffic to internet, no permit condition is required.

! Allow DNS traffic out from external dns server, udp port 53 only (no zone transfer)

```
cypress(config)# access-list acl_edmz1 permit udp host 142.32.1.39 any eq 53
```

! Allow SMTP traffic out from external mail server, tcp port 25

```
cypress(config)# access-list acl_edmz1 permit tcp host 142.32.1.37 any eq 25
```

! Apply access-list acl\_edmz1 to interface edmz1

```
cypress(config)# access-group acl_edmz1 in interface edmz1
```

#### 2.2.4 Packet filter for interface edmz2

Since VPN 3005 will not initiate any outbound traffic, no permit condition is required.

#### 2.2.5 Packet filter for interface idmz1

- The 3 servers in DMZ1 need to synchronize their time with the internal NTP server (Cisco 4000 switch) and send syslog message to syslog server.
- External web server requires access to application server.
- External mail server requires access to Exchange server.
- External DNS server does not require access to internal DNS server.

! Map the NTP server (Cisco 4000 switch's router interface) 10.2.4.1 to internal DMZ1

```
cypress(config)# static (inside, idmz1) 10.2.4.1 10.2.4.1
```

! Allow external web, external mail and external dns servers to access internal ntp server

```
cypress(config)# access-list acl_idmz1 permit udp host 10.1.1.35 host 10.2.4.1 eq 123
```

```
cypress(config)# access-list acl_idmz1 permit udp host 10.1.1.37 host 10.2.4.1 eq 123
```

```
cypress(config)# access-list acl_idmz1 permit udp host 10.1.1.39 host 10.2.4.1 eq 123
```

! Map Syslog server 10.2.20.23 to internal DMZ1

```
cypress(config)# static (inside, idmz1) 10.2.20.23 10.2.20.23
```

! Allow external web, external mail and external dns servers to send syslog message to internal syslog server

```
cypress(config)# access-list acl_idmz1 permit udp host 10.1.1.35 host 10.2.20.23 eq 514
```

```
cypress(config)# access-list acl_idmz1 permit udp host 10.1.1.37 host 10.2.20.23 eq 514
```

```
cypress(config)# access-list acl_idmz1 permit udp host 10.1.1.39 host 10.2.20.23 eq 514
```

! Map Application server 10.2.20.25 to internal DMZ1 and only allows external web uses tcp port 80

```
cypress(config)# static (inside, idmz1) 10.2.20.25 10.2.20.25
```

```
cypress(config)# access-list acl_idmz1 permit tcp host 10.1.1.35 host 10.2.20.25 eq 80
```

! Map Exchange server 10.2.8.21 to internal DMZ1 and only allows external mail uses tcp port 25

```
cypress(config)# static (inside, idmz1) 10.2.8.21 10.2.8.21
```

```
cypress(config)# access-list acl_idmz1 permit tcp host 10.1.1.37 host 10.2.8.21 eq 25
```

! Apply access-list acl\_idmz1 to the interface idmz1

```
cypress(config)# access-group acl_idmz1 in interface idmz1
```

#### 2.2.6 Packet filter for interface inside

There are few services will be allowed to pass-through the firewall from internal hosts or users.

- Internet related web traffic originated from internal users will use the proxy server to proxy the traffic to internet.
- Outgoing SMTP traffic to external mail server from Exchange is allowed.
- Internal DNS server will forward unresolved host name to external DNS server uses udp port 53.

- Synchronize internal NTP server clock with 2 external NTP sources – us navy and university of Houston
- SSL session between Application server to the bank for credit card validation is allowed.

! Allow internet web traffic from proxy out to internet

cypress(config)# **access-list acl\_inside permit tcp host 10.2.8.27 any eq 80**

cypress(config)# **access-list acl\_inside permit tcp host 10.2.8.27 any eq 443**

! Allow SMTP from Exchange to external mail server

cypress(config)# **access-list acl\_inside permit tcp host 10.2.8.21 host 10.1.1.37 eq 25**

! Allow internal DNS request forwards to external DNS server

cypress(config)# **access-list acl\_inside permit udp host 10.2.8.23 host 10.1.1.39 eq 53**

! Allow Cisco 4000 switch's router interface to synchronize time with 2 external sources.

cypress(config)# **access-list acl\_inside permit udp host 10.2.4.1 host 192.5.41.40 eq 123**

cypress(config)# **access-list acl\_inside permit udp host 10.2.4.1 host 129.7.1.66 eq 123**

! Allow SSL session from Application server to the bank at 159.12.59.233

cypress(config)# **access-list acl\_inside permit tcp host 10.2.20.25 host 159.12.59.233 eq 443**

! Apply the access-list acl\_inside to interface inside

cypress(config)# **access-group acl\_inside in interface inside**

© SANS Institute 2000 - 2002. All rights reserved. Author retains full rights.

## 2.3 VPN

This section walks through the configuration steps of setting up Cisco VPN 3005 concentrator for GIAC network.

### 2.3.1 General Configuration

The simplest way to start the configuration is using console port. The console setup is very similar to router and PIX except it is using a straight through cable between the laptop and the VPN 3005. After booting up the VPN 3005, we will add the private (internal) ip address. Login user id is **admin** and password is **admin**, choose 1 for "Configuration" and then 1 again for "Interface configuration". Follow the following screen capture to configure the ip address.

```
This table shows current IP addresses.

  Intf          Status      IP Address/Subnet Mask      MAC Address
-----
Ether1-Pri|Not Configured|    0.0.0.0/0.0.0.0          | 00.03.A0.88.BA.94
Ether2-Pub|Not Configured|    0.0.0.0/0.0.0.0          |
-----

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Power Supplies
4) Back

Interfaces -> 1

1) Interface Setting (Disable, DHCP or Static IP)
2) Set Public Interface
3) Select IP Filter
4) Select Ethernet Speed
5) Select Duplex
6) Set Port Routing Config
7) Back

Ethernet Interface 1 -> 1

1) Disable
2) Enable using DHCP Client
3) Enable using Static IP Addressing

Ethernet Interface 1 -> [ 3 ] 3

This table shows current IP addresses.

  Intf          Status      IP Address/Subnet Mask      MAC Address
-----
Ether1-Pri|Not Configured|    0.0.0.0/0.0.0.0          | 00.03.A0.88.BA.94
Ether2-Pub|Not Configured|    0.0.0.0/0.0.0.0          |
-----

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

** An address is required for the private interface. **

> Enter IP Address

Ethernet Interface 1 -> [ 0.0.0.0 ] 10.2.4.5
```

Waiting for Network Initialization...

> Enter Subnet Mask

Ethernet Interface 1 -> [ 255.0.0.0 ] **255.255.255.0**

- 1) Treat as Public Interface
- 2) Do not treat as Public Interface

Ethernet Interface 1 -> [ 2 ] **2**

- 1) Interface Setting (Disable, DHCP or Static IP)
- 2) Set Public Interface
- 3) Select IP Filter
- 4) Select Ethernet Speed
- 5) Select Duplex
- 6) Set Port Routing Config
- 7) Back

Ethernet Interface 1 -> **4**

- 1) Ethernet Speed 10 Mbps
- 2) Ethernet Speed 100 Mbps
- 3) Ethernet Speed 10/100 Mbps Auto Detect

Ethernet Interface 1 -> [ 3 ] **3**

- 1) Interface Setting (Disable, DHCP or Static IP)
- 2) Set Public Interface
- 3) Select IP Filter
- 4) Select Ethernet Speed
- 5) Select Duplex
- 6) Set Port Routing Config
- 7) Back

Ethernet Interface 1 -> **5**

- 1) Enter Duplex - Half/Full/Auto
- 2) Enter Duplex - Full Duplex
- 3) Enter Duplex - Half Duplex

Ethernet Interface 1 -> [ 1 ] **1**

- 1) Interface Setting (Disable, DHCP or Static IP)
- 2) Set Public Interface
- 3) Select IP Filter
- 4) Select Ethernet Speed
- 5) Select Duplex
- 6) Set Port Routing Config
- 7) Back

Ethernet Interface 1 -> **3**

Current Active Filters

0. Use '0' for no selection	1. Private (Default)	
2. Public (Default)	3. External (Default)	
4. Firewall Filter for VPN Client (De		

> Select a Filter from the Table

Ethernet Interface 1 -> [ 0 ] **1**

- 1) Interface Setting (Disable, DHCP or Static IP)
- 2) Set Public Interface
- 3) Select IP Filter
- 4) Select Ethernet Speed
- 5) Select Duplex
- 6) Set Port Routing Config

7) Back

Ethernet Interface 1 -> 7

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	DOWN	10.2.4.67/255.255.255.0	00.03.A0.88.BA.94
Ether2-Pub	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): DNS Server Not Configured

DNS Domain Name:

Default Gateway: Default Gateway Not Configured

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Power Supplies
- 4) Back

Interfaces -> 4

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Back

Config -> 5

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 4

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

Main -> 6

Done

Login:

Now we can connect VPN 3005 concentrator's Ethernet 1 interface to our laptop's Ethernet interface via a cross-over CAT5 cable, set the laptop ip address to 10.2.4.100/24. Then uses the web interface to carry on our configuration, type the VPN 3005 Ethernet 1 ip address (10.2.4.67) in the "Address" field, then it will display the VPN login screen as follow.



Enter **admin** in the “Login” and “Password” boxes and click “Login” to login. After logging in, click “Click here to go to Main Menu” to start the configuration.

To configure Public interface:

- Click “Configuration”, then “Interfaces” on the left side of the screen.
- Click “Ethernet 2 (Public)” on the right.
- Click “Static IP Addressing” and enter IP address 142.32.1.67, subnet mask 255.255.255.224 in the boxes provided.
- Choose “2. Public (Default)” in the “Filter” drop down box.
- Click “Apply” at the bottom.
- Public interface configuration is completed and the following screen will appear.

The next step will configure external RADIUS authentication server (i.e. Microsoft IAS), it is used to authenticate remote VPN client’s user id and password.





- Expand “System” on the left, then click “Servers”
- Click “Authentication” and choose “Add”
- Pick “RADIUS” in the Server Type drop down box.
- Enter IAS server ip address **10.2.8.27** in the “Authentication Server” box.
- Enter **AaUuThEe** in the “Server Secret” and “Verify” boxes (this is the RADIUS authentication key between VPN 3005 and Microsoft IAS server).
- Click “Add”
- To enable RADIUS accounting, click “Accounting” on the left side, enter IAS server ip address **10.2.8.27** in the “Accounting Server” box, then enter **AaUuThEe** in the “Server Secret” and “Verify” boxes, this key is the RADIUS’ accounting server key.
- Click “Add” to complete.

VPN 3005 will use NTP to synchronize time with internal NTP server.

- Click “NTP” on the left side, pick “Hosts” and click “Add”. Enter the Cisco 4006 switch router interface ip address **10.2.4.1** in the “NTP Host” box.
- Click Add to complete.

We are going to use the local address pool database inside VPN 3005 to control the ip address that is going to assign to each successful authenticated client.

- Click “Address Management” on the left, click “Assignment” and then check “Use Address Pools”. Click Apply afterward.
- Click “Pools” on the left and enter **10.2.5.1** in the “Range Start” box and enter **10.2.5.254** in the “Range End” box. This will create a VPN client address pool from 10.2.5.1 to 10.2.5.254. Click Add to complete.

By default, VPN 3005 supports PPTP, L2TP and IPSec tunneling protocols. The GIAC remote access policy only allows IPSec tunnel between client and VPN 3005. The following step will show how to disable PPTP and L2TP.

- Expand “Tunneling Protocols” from the left. Click “PPTP” and uncheck “Enabled”. Click Apply to complete.
- Click “L2TP” on the right and uncheck “Enabled”. Click Apply to complete.
- Both PPTP and L2TP are now disabled. We are going to configure IPsec, expand “IPsec” on the left and click “IKE Proposals”. Choose “CiscoVPNClient-3DES-MD5” in the Active Proposals box, deactivate the rest of the proposals. The setting will allow Cisco VPN client using 3DES and MD5 to setup VPN tunnel with VPN 3005.

VPN 3005 supports dynamic routing protocol, OSPF (Open Shortest Path First) and static route. In our configuration, we will only use static route.

- Create a static route to route internal traffic to the Cisco 4000 switch. Click “IP Routing” on the left and click “Static Routes”, click “Add the route”. Enter **10.0.0.0** in the “Network Address” box, enter **255.0.0.0** in the “Subnet Mask” and enter **1** in the “Metric” box. Then check “Destination Router Address” and enter **10.2.4.1** in the box provided. Click “Apply” to complete.
- Use default gateway for the “public” interface to route traffic because the VPN clients can be anywhere in the internet. Click “Default Gateways” on the left, enter **142.32.1.65** (PIX external DMZ2 interface) in “Default Gateway” box, enter **1** in “Metric” box and enter **10.2.4.1** in the “Tunnel Default Gateway” box. Click “Apply” to complete.

VPN 3005 supports many different management protocols and we want to be make sure the connection between management workstation and VPN 3005 is secure, SSL is chosen.

- Expand “Management Protocols” on the left and click each of the protocols (FTP, TFTP, Telnet, SNMP, SSH and XML) to disable by unchecking the “Enable” box and click “Apply” at the bottom of each screen. Only leave HTTPS and SSL enable.

GIAC uses a centralized syslog server to store all network related syslog messages.

- Configure syslog message severity level. Click “Events”, then “General” on the left. Choose “1-5” in the “Severity to Syslog” drop down box to send syslog message that is “notifications” and high to syslog server. Click “Apply” to complete.
- Click “Syslog Servers” on the left, and click “Add” to add syslog server ip address. Enter the internal syslog server ip address **10.2.20.23** in the “Syslog Server” box. Click “Add” to complete.

Configure the VPN 3005 to support 100 connections (this is the maximum allowed connections).

- Expand “General” on the left and click “Sessions”.
- Enter **100** in the “Maximum Active Connections” box.
- Click “Apply” to complete.

### 2.3.2 Group and user Configuration

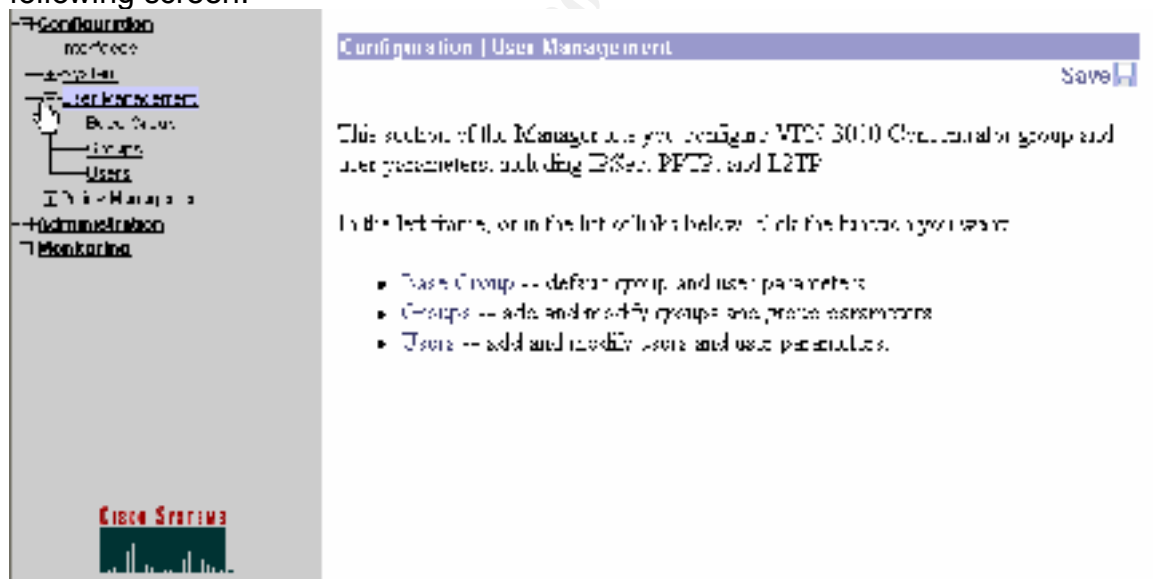
User is a member of a group, and group is a member of the Base group. Each Group and user has attributes, configurable parameters that determine their access to and use of the VPN. Base group parameters are common setting across all groups. Each group can “inherit” parameters from the Base group or set their own parameters.

The VPN 3005 checks authentication parameters in the follow order:

- User parameters. If any parameters are missing, the system looks at Group parameters.
- Group parameters. If any parameters are still missing, it looks at IPSec tunnel group if IPSec is being used.
- IPSec tunnel group parameter (IPSec user only). If any parameter is missing, it uses the Base group parameter.
- Base group parameters.

We are going to create a group called GIACVPN for remote access users through RADIUS to the Windows Domain for authenticating user's user id and password.

To start Group configuration, expand “User Management” as shown in the following screen.



- Click “Group” on the left, then click “Add Group”<sup>2</sup> to create a new group.

This section lets you add a group. Check the **Inherit?** box to set a default 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		Enter a unique name for the group.
Password		Enter the password for the group.
Verify		Verify the user's password.
Type	normal	Extended groups are configured on an external authentication server (e.g. RADIUS). Standard groups are configured on the VPN 3005 Concentrator's Internal Database.

Buttons: Add, Cancel

- Under the “Identity” button, enter the **GIACVPN** in the “Group Name” box and enter **GvlpAnC1** in the “Password” and “Verify” boxes.

To continue with the configuration, click the button “General”.

- “Access Hours”, we do not want to restrict our user access hours (they can be at different time zones), so choose **–No Restrictions–**.
- “Simultaneous Logins”, “Minimum Password Length” and “Allow Alphabetic-Only Passwords”, they are used for controlling internal VPN 3005’s user database attributes. This is not applied to us and can be ignored.
- “Idle Timeout”, set it to **20** means a session will disconnect if it is idle for 20 minutes. This setting will minimize the chance that the user forgets to logoff and have someone uses his/her PC to access GIAC without authentication again.
- “Maximum Connection Time”, set it to **180** means each session has maximum connection time equals to 3 hours.
- Choose **None** in the “Filter drop down box because we are not going to restrict remote user access to our internal network.
- Enter **10.2.8.23** in the “Primary DNS” and “Primary WINS” boxes, the parameters are used to assign/push to the client once it is authenticated successfully. Then the client can use internal DNS server 10.2.8.23 to resolve names.

<sup>2</sup> “Modify Group” will be used to modify an existing group. “Modify Auth. Servers”, “Modify Acct. Servers” and “Modify Address Pools” are used to configure new server to be used for this group only, no changes will be made because we are using the same server that we have configured under “System”. “Modify Client Update” is used to prompt users to update their client software if it is below certain version. “Delete Group” is used to delete a group.

- Check only “IPSec” under the “Tunneling Protocols”, this is the only protocol that GIAC will be used.
- Uncheck “Strip Realm”, it is not used in our implementation because we do not use realm qualifier in the user name.

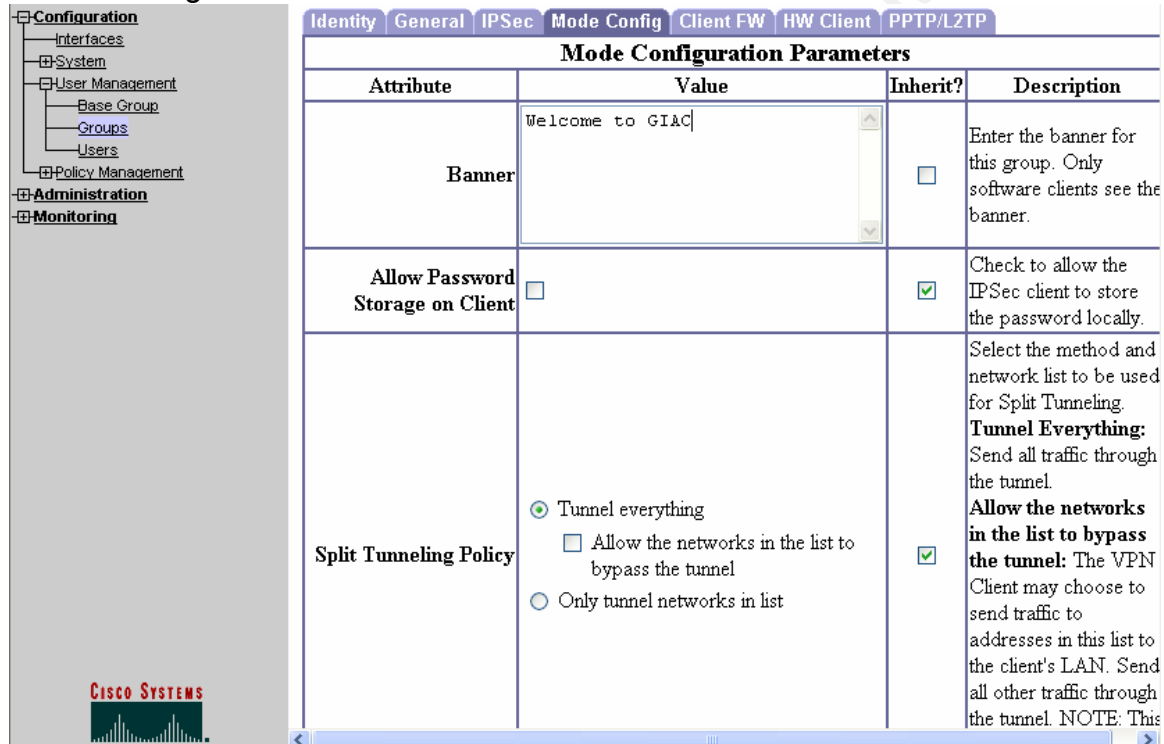
Next step will configure the group, GIACVPN, IPSec parameters

IPSec Parameters			
Attribute	Value	Enabled?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPsec Security Association
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's method
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives from remote clients
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the tunnel type for this group. Update the Remote Access parameters below as needed
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into the group
Authentication	RADIUS with Expiry	<input type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication
IP Tunnel	None	<input checked="" type="checkbox"/>	Select the IP tunnel type for members of this group
Handshake Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the handshake authentication (Phase 1) policy

- Click the “IPSec” button.
- Choose “ESP-3DES-MD5” in the “IPSec SA” drop down box, ESP and 3DES are defined in the GIAC remote access policy.
- Choose “If supported by certificate” in the “IKE Peer Identity Validation” drop down box because we are not going to use certificate to identify peer.
- Check “IKE Keepalives” to allow keepalives to be sent to remote client. If client becomes unresponsive, the VPN 3005 can drop the connection. This prevents hung connections when the IKE peer loses connectivity.
- Choose “Remote Access” in the “Tunnel Type” drop down box because we are not doing site-to-site VPN, all users are using Cisco VPN client software.
- “Group Lock” is not important because it is only used for internal user database.
- Choose “RADIUS with Expiry” in the “Authentication” drop down box to allow CHAP v2 to be used for transporting password related information between VPN 3005 and remote VPN client software. CHAP v2 enable the remote client software to prompt for new password if the password is expired in Windows 2000 domain.

- Choose “None” in the “IPComp” drop down box. Data compression will only help when user is using a very slow link and it will degrade the VPN 3005 performance.
- Uncheck “Reauthentication on Rekey” to stop the system to prompt user for re-entering password during IKE phase 1 re-negotiations.
- “Mode Configuration” is not important in our implementation because all client software is version 3.6.1 or higher.

Next step will configure miscellaneous parameters for the GIACVPN group under “Mode Configure”



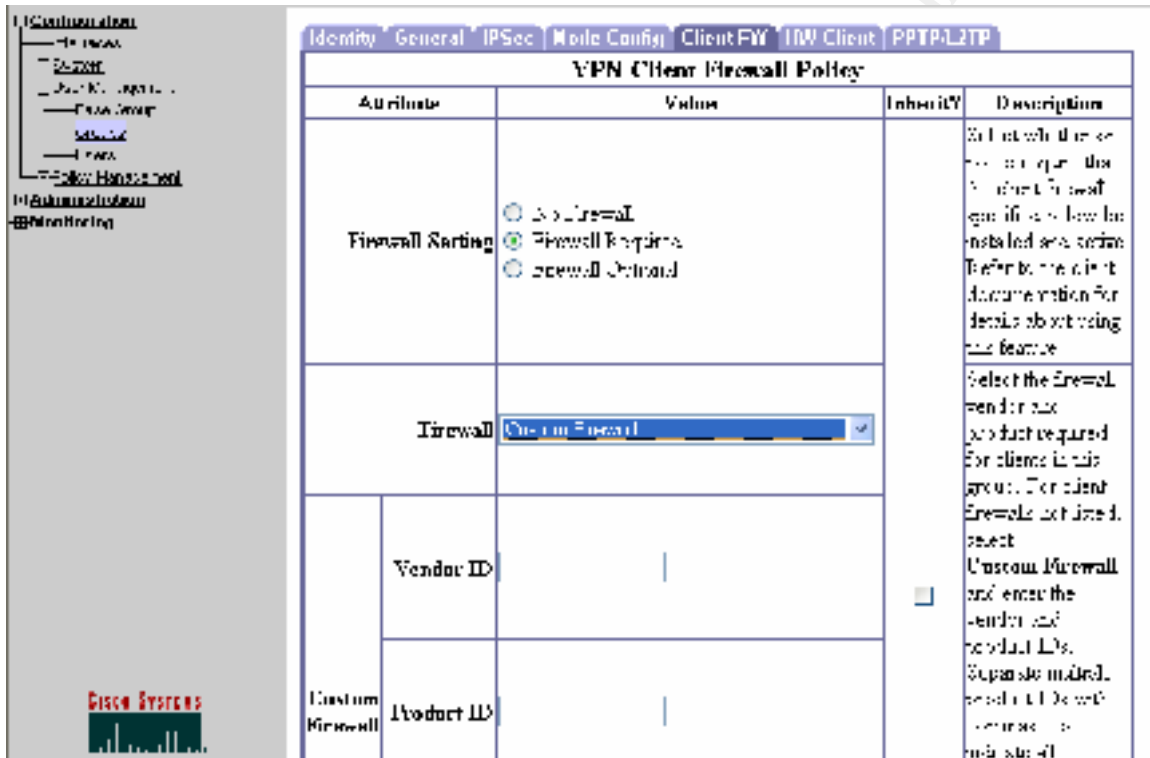
Mode Configuration Parameters			
Attribute	Value	Inherit?	Description
Banner	Welcome to GIAC	<input type="checkbox"/>	Enter the banner for this group. Only software clients see the banner.
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.
Split Tunneling Policy	<input checked="" type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in the list to bypass the tunnel <input type="radio"/> Only tunnel networks in list	<input checked="" type="checkbox"/>	Select the method and network list to be used for Split Tunneling. <b>Tunnel Everything:</b> Send all traffic through the tunnel. <b>Allow the networks in the list to bypass the tunnel:</b> The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This

- Click “Mode Configure”.
- Enter **Welcome to GIAC** in the “Banner box. Once the client is authenticated successfully, the client software will display Welcome to GIAC message in a pop up window.
- Uncheck the “Allow Password Storage on Client”, it is more secure to store and protect password in a centralize database.
- Check “Tunnel everything” and uncheck “Allow the networks in the list to bypass the tunnel” in the “Split Tunneling Policy”. GIAC remote access policy does not allow split tunnel (once the VPN tunnel is up, all traffic will be tunneled back to GIAC). This will stop attacker from hijacking the laptop during the VPN tunnel is up from internet and get access to GIAC internal network via the VPN tunnel.
- Enter **giac.com** in the “Default Domain Name” box to append domain suffix giac.com.

- Leave the “IPSec over UDP through NAT” and “Backup Servers” to default because GIAC does not support UDP through NAT at the moment and no backup VPN server is installed.

Even though the GIAC remote access policy requires users to have their personal firewall turn on at all time, there are parameters that can be set in VPN 3005 to reinforce this policy. If the personal firewall is disabled, the VPN connection will not start or drop during the session is running.

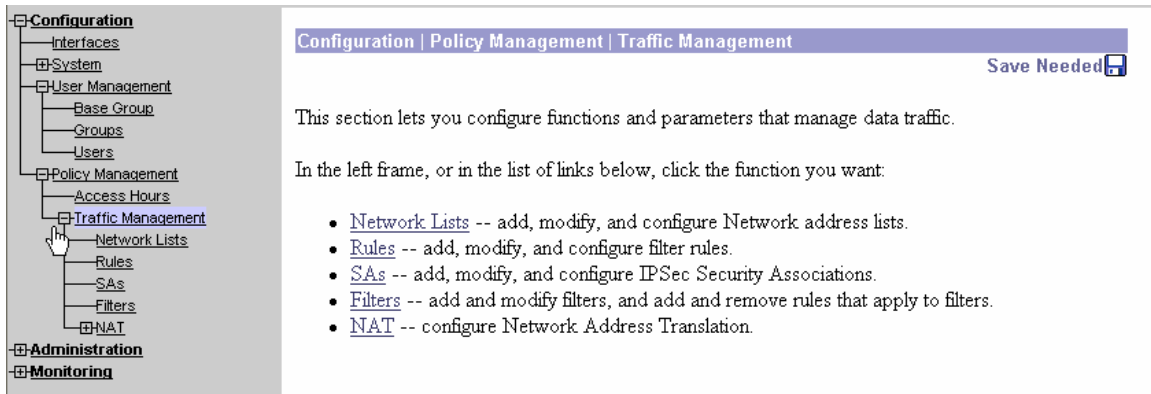
- Click the “Client-FW”.



- Check **Firewall Required** in the “Firewall Setting” box to make sure client has turned on the personal firewall while he/she is connected.
- Choose **Network ICE BlackICE Defender** in the “Firewall” drop down box. All remote client laptops have BlackICE personal firewall installed, and this parameter validates whether it is on or not. (Network ICE is bought by Internet Security Systems but Cisco still calls it Network ICE).
- Click “Apply” to complete “User Management”.

### 2.3.3 Policy Management

This is where the access lists and access hours can be configured. The policy defines remote users can access VPN at any time, no time restriction is required. Next, go to access lists configuration for public and private interfaces.



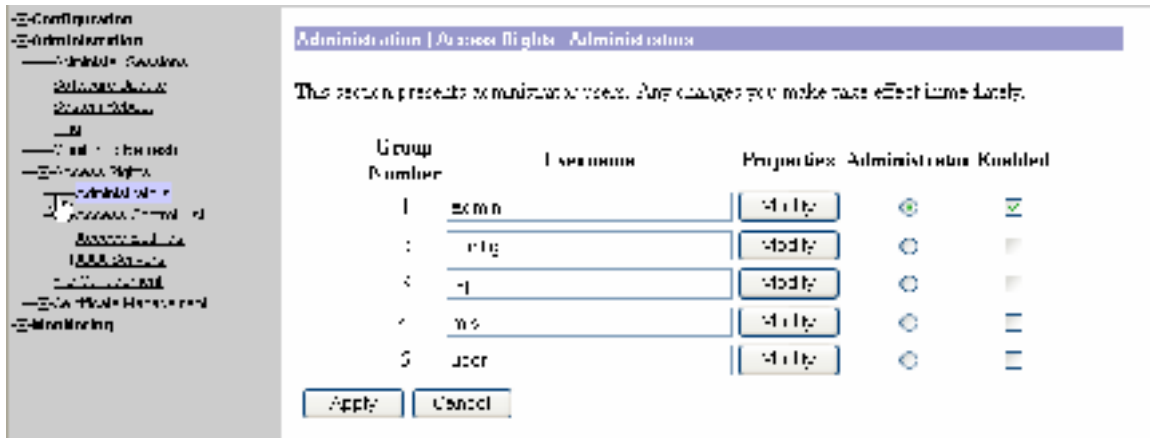
The screenshot shows the Mikrotik WinBox Configuration window. On the left is a tree view with categories: Configuration, System, User Management, Policy Management, Administration, and Monitoring. Under Policy Management, 'Traffic Management' is expanded, showing sub-items: Access Hours, Network Lists, Rules, SAs, Filters, and NAT. A mouse cursor is pointing at 'Filters'. The main panel on the right has a title bar 'Configuration | Policy Management | Traffic Management' and a 'Save Needed' button. Below the title bar, it says 'This section lets you configure functions and parameters that manage data traffic.' and 'In the left frame, or in the list of links below, click the function you want:'. A list of links is provided: Network Lists, Rules, SAs, Filters, and NAT, each with a brief description of its function.

- Expand the “Traffic Management” and click “Filters”.
- Highlight the “Private (Default)” and click “Assign Rules to Filter”.
- Keep “Any In (forward/in)” and “Any out (forward/out)” in the “Current Rules”, disable the rest of the rules. We don’t want any restriction to be set at this level (VPN user restriction is done at “Group” level).
- Click “Done” to complete private interface rules setup.
- Highlight the “External (Default)” and click “Assign Rules to Filter”.
- Keep “IPSec-ESP In (forward/in)”, “IKE In (forward/in)” and IKE Out (forward/out)”, disable the rest of the rules. These rules allow ip protocol 50 and udp port 500 to connect to the VPN 3005 public interface.
- Click “Done” to complete public interface rules setup.
- Click “Network Lists” to add server segment subnet because VPN users are allowed to access server segment only.
- Click “Add”, enter **server segment** in the “List Name” and 10.2.8.0/0.0.0.255 in the “Network List”. Click “Add”.
- Click “Rules” and then “Add”. Enter **Server Traffic** in “Rule Name”, choose Inbound in the “Direction”, choose Forward in the “Action”. “Protocol” is Any, “TCP Connection” is Don’t care. Source Address will be using default (IP Address 0.0.0.0, Wildcard-mark 255.255.255.255). Destination Address, Network List is “Server Segment”, leave the remaining configuration uses default value, click “Apply” to complete.
- Click “Filters” and click “Add Filter”. Enter **server farm** in Filter Name, choose Drop, uncheck “Source Routing”, check Fragments and enter **Server access** in the “Description”. Click Add to complete.
- We need to add the new access filter to the user group “GVRD VPN”, click “User Management” and click “General”. Scroll down to filter and choose **server farm** in the drop down box. Click Add to complete. Now authenticated VPN users can access to the Server segment

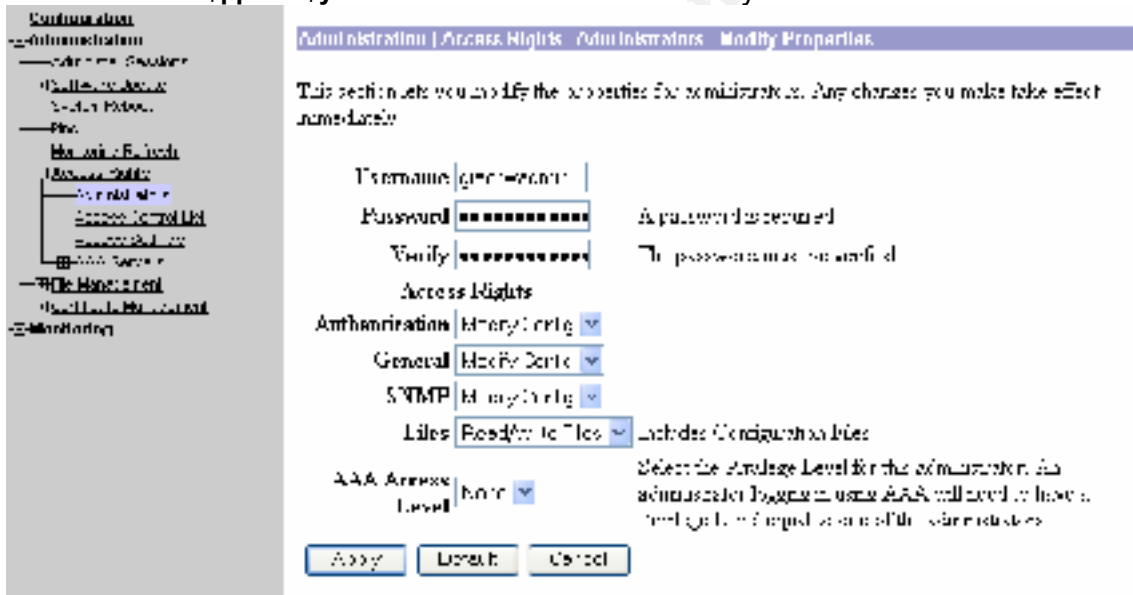
#### 2.3.4 Administration setting

We are going to change the default user name “admin” and password to minimize the chance that attacker can guess our administrator user name and password.





- Expand the “Administration” on the left and expand the “Access Rights”.
- Click the “Administrator”
- Click the “Modify” button next to the user name “admin”.
- Enter **giacnwadmin** in the “Username” box.
- Enter **h\$ppY2D\$y** in the “Password” and “Verify” boxes.



- Click “Apply”.
- Only the username “giacnwadmin” has “Administrator” and “Enabled” checked. Disable the rest of the default usernames.
- Click “Apply” to complete.

### 2.3.5 Save VPN 3005 configure

We have finished configuring the VPN 3005 concentrator, click “Save Needed” on the top right corner to save the configure to memory before logoff.

**-[- Configuration**  
**-[- Administration**  
    Administer Sessions  
    [- Software Update  
    System Reboot  
    Ping  
    Monitoring Refresh  
    [- Access Rights  
        Administrators  
        Access Control List  
        Access Settings  
    [- AAA Servers  
    [- File Management  
    [- Certificate Management  
**-[- Monitoring**

## Administration | Access Rights

Save Needed 

This section of the Manager lets you configure administrative access to the VPN 3000 Concentrator.

In the left frame, or in the list of links below, click the function you want:

- [Administrators](#) -- administrators, passwords, and access rights.
- [Access Control List](#) -- IP addresses and options for administrator access.
- [Access Settings](#) -- session timeout and limits.
- [AAA Servers](#) -- AAA servers for administrator access.

© SANS Institute 2000 - 2002, Author retains full rights.

### 3. Assignment 3 – Audit

When GIAC setup the corporate security policy, it defined full security audit must be done every 6 months which included servers, workstations, firewalls, VPN, routers and switches. It also specified that applications changes, software upgrade and network changes must be tested and documented before rolling out to the production network. This security policy document had been approved and signed by the GIAC management team.

The security audit is divided into 5 key areas: Firewall security, server security, network security, user desktop security and physical security. However, the main focus of this assignment is Firewall Security, the other security will not be discussed in this document.

#### 3.1 Plan Audit

The IS manager had budgeted \$30,000 this year for the overall security audit. Within the \$30k budget, \$15k is assigned to the firewall security audit (\$7.5k for each firewall security audit).

The firewall security audit team consists of two GIAC network specialists and a consultant. The team estimates the firewall audit process will take 82 hours to finish, the breakdown of time and cost is as follow.

Description	Internal			Consultant Hour
	# of staff	Hours (each)	Staff Hours	
Detail procedure, notification and setup	2	4	8	5
Implementation	2	8	16	12
Post-implementation review and documentation	2	4	8	8
Implement recommendation	1	30	25	0
Total hours			57	25
Hourly rate			\$60	\$150
<b>Total cost:</b>			<b>\$3,420</b>	<b>\$3,750</b>

##### 3.1.1 Select Audit schedule

The team and management has agreed the actual audit/testing will start on date A, Friday 21:00 and must be completed by the following Sunday date B at 12:00. It is because our partners and suppliers are not working during the weekends and the historical traffic data indicated that the traffic volume were low.

##### 3.1.2 Scope of work - consultant

The consultant has signed a non-disclosure agreement and states that the following tests will be done:

- Port scanning
- OS fingerprint

- Denial of Service
- Vulnerability

### 3.1.3 Notification

The team informs the partner and suppliers 2 weeks in advance that there will be network maintenance from date A to date B and the maintenance may cause performance degradation and/or service interruption.

### 3.1.4 Tools

- 4 laptops will be used. 3 of them will be running RedHat 7.2 with nmap 3.0 and Ethereal 0.9.6 ([www.ethereal.com](http://www.ethereal.com)). The other laptop is running Windows 2000 workstation with Etherpeek NX (from WildPacket Inc. at [www.wildpacket.com](http://www.wildpacket.com)).
- Nmap is responsible for port scanning and OS fingerprint.
- Etherpeek is responsible for capture and replay packet.
- Software vulnerability are reference to Cisco web site [www.cisco.com](http://www.cisco.com) and SecureFocus web site [www.securefocus.com](http://www.securefocus.com).

## 3.2 Implementation

### 3.2.1 Setup

An Ethernet switch is temporary installed between the Border Router and the PIX, audit laptops are connected to the switch.

Enable an Ethernet port in each of the DMZ1 switches for connecting the audit laptops. Enable an Ethernet port in the switch between PIX and Cisco 4006 switch for connecting audit laptop.

### 3.2.2 Port scan and OS fingerprint from PIX outside interface

Connect the 3 RedHat laptops to the switch outside the PIX firewall. Then connect the Windows' laptop to external DMZ1 switch and mirror the traffic from the PIX interface (edmz1) to the Windows laptop's Ethernet port. By reviewing the network traffic capture by Etherpeek in the DMZ1 network, we can confirm the allowed nmap traffic is really getting through the firewall and reach the right server in the DMZ.

The ip addresses for the test laptops are 142.32.1.20, 142.32.1.21 and 142.32.1.22 with subnet mask 255.255.255.224 and default gateway is 142.32.1.3 (PIX's outside interface).

First we do a simple scan for the subnet that ISP assign to us. This step is to make sure there is no misconfigure hosts or rules in the PIX firewall. From the past experience, the nmap's UDP port scan will take a long time and we will use

laptop1 to do this scan, laptop 2 & 3 for detail host scan. The scans are run simultaneously.

```
laptop1# nmap -sS -sU -O -P0 142.32.1.32-94
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
All 3069 scanned ports on (142.32.1.32) are: filtered
All 3069 scanned ports on (142.32.1.33) are: filtered
All 3069 scanned ports on (142.32.1.34) are: filtered
All 3069 scanned ports on (142.32.1.36) are: filtered
All 3069 scanned ports on (142.32.1.38) are: filtered
All 3069 scanned ports on (142.32.1.40) are: filtered
All 3069 scanned ports on (142.32.1.41) are: filtered
All 3069 scanned ports on (142.32.1.42) are: filtered
All 3069 scanned ports on (142.32.1.43) are: filtered
All 3069 scanned ports on (142.32.1.44) are: filtered
All 3069 scanned ports on (142.32.1.45) are: filtered
All 3069 scanned ports on (142.32.1.46) are: filtered
All 3069 scanned ports on (142.32.1.47) are: filtered
All 3069 scanned ports on (142.32.1.48) are: filtered
All 3069 scanned ports on (142.32.1.49) are: filtered
All 3069 scanned ports on (142.32.1.50) are: filtered
All 3069 scanned ports on (142.32.1.51) are: filtered
All 3069 scanned ports on (142.32.1.52) are: filtered
All 3069 scanned ports on (142.32.1.53) are: filtered
All 3069 scanned ports on (142.32.1.54) are: filtered
All 3069 scanned ports on (142.32.1.55) are: filtered
All 3069 scanned ports on (142.32.1.56) are: filtered
All 3069 scanned ports on (142.32.1.57) are: filtered
All 3069 scanned ports on (142.32.1.58) are: filtered
All 3069 scanned ports on (142.32.1.59) are: filtered
All 3069 scanned ports on (142.32.1.60) are: filtered
All 3069 scanned ports on (142.32.1.61) are: filtered
All 3069 scanned ports on (142.32.1.62) are: filtered
All 3069 scanned ports on (142.32.1.63) are: filtered
All 3069 scanned ports on (142.32.1.64) are: filtered
All 3069 scanned ports on (142.32.1.65) are: filtered
All 3069 scanned ports on (142.32.1.66) are: filtered
```

All 3069 scanned ports on (142.32.1.68) are: filtered  
 All 3069 scanned ports on (142.32.1.69) are: filtered  
 All 3069 scanned ports on (142.32.1.70) are: filtered  
 All 3069 scanned ports on (142.32.1.71) are: filtered  
 All 3069 scanned ports on (142.32.1.72) are: filtered  
 All 3069 scanned ports on (142.32.1.73) are: filtered  
 All 3069 scanned ports on (142.32.1.74) are: filtered  
 All 3069 scanned ports on (142.32.1.75) are: filtered  
 All 3069 scanned ports on (142.32.1.76) are: filtered  
 All 3069 scanned ports on (142.32.1.77) are: filtered  
 All 3069 scanned ports on (142.32.1.78) are: filtered  
 All 3069 scanned ports on (142.32.1.79) are: filtered  
 All 3069 scanned ports on (142.32.1.80) are: filtered  
 All 3069 scanned ports on (142.32.1.81) are: filtered  
 All 3069 scanned ports on (142.32.1.82) are: filtered  
 All 3069 scanned ports on (142.32.1.83) are: filtered  
 All 3069 scanned ports on (142.32.1.84) are: filtered  
 All 3069 scanned ports on (142.32.1.85) are: filtered  
 All 3069 scanned ports on (142.32.1.86) are: filtered  
 All 3069 scanned ports on (142.32.1.87) are: filtered  
 All 3069 scanned ports on (142.32.1.88) are: filtered  
 All 3069 scanned ports on (142.32.1.89) are: filtered  
 All 3069 scanned ports on (142.32.1.90) are: filtered  
 All 3069 scanned ports on (142.32.1.91) are: filtered  
 All 3069 scanned ports on (142.32.1.92) are: filtered  
 All 3069 scanned ports on (142.32.1.93) are: filtered  
 All 3069 scanned ports on (142.32.1.94) are: filtered  
 Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port  
 Insufficient responses for TCP sequencing (1), OS detection may be less accurate  
 Insufficient responses for TCP sequencing (3), OS detection may be less accurate  
 Interesting ports on (142.32.1.35):  
 (The 3067 ports scanned but not shown below are in state: closed)  

Port	State	Service
80/tcp	open	http
443/tcp	open	https

 No OS matches for host (test conditions non-ideal).  
 TCP/IP fingerprint:  
 SInfo (V=3.00%P=i686-pc-linux-gnu%D=9/27%Time=3D9547D8%O=80%C=-1)  
 TSeq (Class=TR%IPID=Z%TS=100HZ)  
 T1 (Resp=Y%DF=Y%W=16A0%ACK=O%Flags=AS%Ops=MNNTNW)  
 T1 (Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)  
 T2 (Resp=N)  
 T2 (Resp=N)  
 T3 (Resp=N)

```

T3 (Resp=N)
T4 (Resp=N)
T4 (Resp=N)
T5 (Resp=N)
T5 (Resp=N)
T6 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)

Warning: OS detection will be MUCH less reliable because we did not find at least 1 open
and 1 closed TCP port
Insufficient responses for TCP sequencing (1), OS detection may be less accurate
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on (142.32.1.37):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
25/tcp    open       smtp
No OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SInfo (V=3.00%P=i686-pc-linux-gnu%D=9/28%Time=3D955378%O=25%C=-1)
TSeq (Class=TR%IPID=Z%TS=100HZ)
T1 (Resp=Y%DF=Y%W=16A0%ACK=O%Flags=AS%Ops=MNNTNW)
T1 (Resp=Y%DF=Y%W=16A0%ACK=S+++%Flags=AS%Ops=MNNTNW)
T2 (Resp=N)
T2 (Resp=N)
T3 (Resp=N)
T3 (Resp=N)
T4 (Resp=N)
T4 (Resp=N)
T5 (Resp=N)
T5 (Resp=N)
T6 (Resp=N)
T6 (Resp=N)
T7 (Resp=N)
T7 (Resp=N)
PU (Resp=N)
PU (Resp=N)

T7 (Resp=N)
PU (Resp=N)
PU (Resp=N)

Interesting ports on (142.32.1.39):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
53/udp    open       domain

Interesting ports on (142.32.1.67):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
500/udp    open       isakmp

Nmap run completed -- 61 IP addresses (4 hosts up) scanned in 36732 seconds

```

#### Nmap options description:

- sS SYN Stealth scan
- sU UDP Stealth scan
- P0 Do not ping the target host
- O Guess target OS system.

The first scan result indicates that the external web server, external mail server, external DNS and VPN corresponding ports are opened (tcp port 80 and 443 for web, tcp port 25 for mail server, udp port 53 for DNS and udp port 500 for VPN) and nmap cannot confirm the exact OS version but it indicates the servers are

Linux machines running on Intel CPU. In addition, the options that we use in the nmap scan will only scan 3069 ports, a more detail scan for each hosts is done using laptop2.

The second laptop will scan each external server using port number range from 1 to 65536. This is to confirm the firewall only has the specific port open for corresponding servers.

```
laptop2 # nmap -P0 -sS -sU -p 1-65536 142.32.1.35
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (142.32.1.35):
(The 131072 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 15653 seconds

laptop2 # nmap -P0 -sS -sU -p 1-65536 142.32.1.37
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (142.32.1.37):
(The 131072 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 15153 seconds

laptop2 # nmap -P0 -sS -sU -p 1-65536 142.32.1.39
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (142.32.1.39):
(The 131072 ports scanned but not shown below are in state: closed)
Port      State      Service
53/udp    open       domain

Nmap run completed -- 1 IP address (1 host up) scanned in 15311 seconds

laptop2 # nmap -P0 -sS -sU -p 1-65536 142.32.1.67
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (142.32.1.67):
(The 131072 ports scanned but not shown below are in state: closed)
Port      State      Service
500/udp    open       isakmp

Nmap run completed -- 1 IP address (1 host up) scanned in 13911 seconds
```

The second scan result confirms that only tcp port 80 and 443 are opened on external web server, tcp port 25 is opened on external mail, udp port 53 is opened on external DNS and udp port 500 is opened on VPN 3005. For the external DNS, it does have a second rules in the firewall to allow tcp port 53 between the external DNS and the secondary external DNS in our ISP. But the



nmap does not detect it because the firewall only allows tcp port 53 with source ip address 142.32.100.99.

The third scan uses the laptop3 to scan from the internal network to the firewall internal interface. As expected, the nmap scan indicates all the ports are filtered because our rules only allow Exchange (tcp port 25), Internal DNS (udp port 53), Cisco 4006 switch (udp port 123), proxy server (tcp port 80 and 443) and application server (tcp port 443).

```
Laptop3# nmap -P0 -sU -sS 10.2.4.21
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
All 3069 scanned ports on (10.2.4.21) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 3367 seconds
```

In order to verify the firewall rules are setup correctly from internal to “idmz1” and “outside”, we will temporary disconnect each of the internal servers (Exchange, internal DNS, application server and proxy server) and make the laptop3 to use their ip addresses to do the nmap scan.

Laptop3 replaces Exchange server, laptop3 ip address 10.2.8.21:

```
Laptop3#nmap -sS -sU -P0 10.1.1.37
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.1.1.37):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
25/tcp    open       smtp

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3489
seconds
```

Laptop3 replaces internal DNS server, laptop3 ip address 10.2.8.23:

```
Laptop3#nmap -sS -sU -P0 10.1.1.39
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.1.1.39):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
53/udp    open       domain

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3689
seconds
```

Laptop3 replaces proxy server, laptop3 ip address 10.2.8.27:

```
Laptop3#nmap -sS -sU -P0 159.12.59.233
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (159.12.59.233):
(The 3067 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 addresses (1 hosts up) scanned in 3569
seconds
```

Laptop3 replaces applications server, laptop3 ip address 10.2.20.25:

```
Laptop3#nmap -sS -sU -P0 10.1.1.35
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.1.1.35):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
80/tcp    open       http

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3421
seconds

Laptop3#nmap -sS -sU -P0 159.12.59.233
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (163.3.1.5):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
443/tcp   open       https

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3391
seconds
```

Note: The applications server needs to communicate with the external web server's internal interface using tcp port 80 and to the bank at 159.12.59.233 using tcp port 443.

The result of the third scan indicates our rules are setup correctly, no additional port is opened.

The fourth scan will use laptop3, ip address 10.1.1.100 to scan from the idmz1 to internal network. As expected, there is no port opened because there is no permit rule for ip address 10.1.1.100 in the firewall. In order to test the each of the rules in the idmz1 interface, we need to make laptop3 temporary uses the server's ip address one by one before starting nmap to scan PIX idmz1 interface.

```
Laptop3# nmap -P0 -sU -sS 10.1.1.1
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
All 3069 scanned ports on (10.1.1.1) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 3367 seconds
! No response which is expected because the firewall filter out all traffic.
```

Laptop3 replaces External web server, laptop3 ip address 10.1.1.35:

```
Laptop3#nmap -sS -sU -P0 10.2.20.25
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.20.25):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
80/tcp    open       http

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3489
seconds

Laptop3#nmap -sS -sU -P0 10.2.20.23
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.20.23):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
514/udp    open       syslog

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3339
seconds

Laptop3#nmap -sS -sU -P0 10.2.4.1
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.4.1):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
123/udp    open       ntp

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3487
seconds
```

! The first destination of the scan (10.2.20.25) is application server, the second one (10.2.20.23) is syslog server, the third one (10.2.4.1) is the Cisco 4006 acts as ntp server. The firewall rules are setup correctly.

Laptop3 replaces external mail server, laptop3 ip address 10.1.1.37:

```
Laptop3#nmap -sS -sU -P0 10.2.8.21
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.8.21):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
25/tcp    open       smtp

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3489
seconds
```

```
Laptop3#nmap -sS -sU -P0 10.2.20.23
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.20.23):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
514/udp    open       syslog

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3339
seconds

Laptop3#nmap -sS -sU -P0 10.2.4.1
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.4.1):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
123/udp    open       ntp

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3487
seconds
```

! The first destination of the scan (10.2.8.21) is the Exchange server, the second one (10.2.20.23) is syslog server, the third one (10.2.4.1) is the Cisco 4006 acts as ntp server. The firewall rules are setup correctly.

Laptop3 replaces external DNS server, laptop3 ip address 10.1.1.39:

```
Laptop3#nmap -sS -sU -P0 10.2.8.23
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
All 3068 scanned ports on (10.2.8.23) are: closed

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3489
seconds

Laptop3#nmap -sS -sU -P0 10.2.20.23
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.20.23):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
514/udp    open       syslog

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3339
seconds

Laptop3#nmap -sS -sU -P0 10.2.4.1
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (10.2.4.1):
(The 3068 ports scanned but not shown below are in state: closed)
Port      State      Service
123/udp    open       ntp

Nmap run completed -- 1 IP addresses (1 hosts up) scanned in 3487
seconds
```

! The first destination of the scan (10.2.8.23) is the internal DNS server, all ports are closed because the firewall does not allow External DNS server to initiate traffic to internal DNS server.

The second one (10.2.20.23) is syslog server, the third one (10.2.4.1) is the Cisco 4006 acts as ntp server. The firewall rules are setup correctly.

In addition to the nmap scan, we use telnet from the external network to our external web server and we have found the following.

```
Laptop3# telnet 142.32.1.35 80
Trying 142.32.1.35...
Connected to 142.32.1.35.
Escape character is '^]'.
http 1.1 /r/r/w/q
HTTP/1.1 400 Bad Request
Date: Sat, 28 Sep 2002 19:59:14 GMT
Server: Apache/1.3.23 (Unix) (Red-Hat/Linux)
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that this server could not understand.<P>
The request line contained invalid characters following the protocol
string.<P>
<P>
<HR>
<ADDRESS>Apache/1.3.23 Server at alf Port 80</ADDRESS>
</BODY></HTML>
```

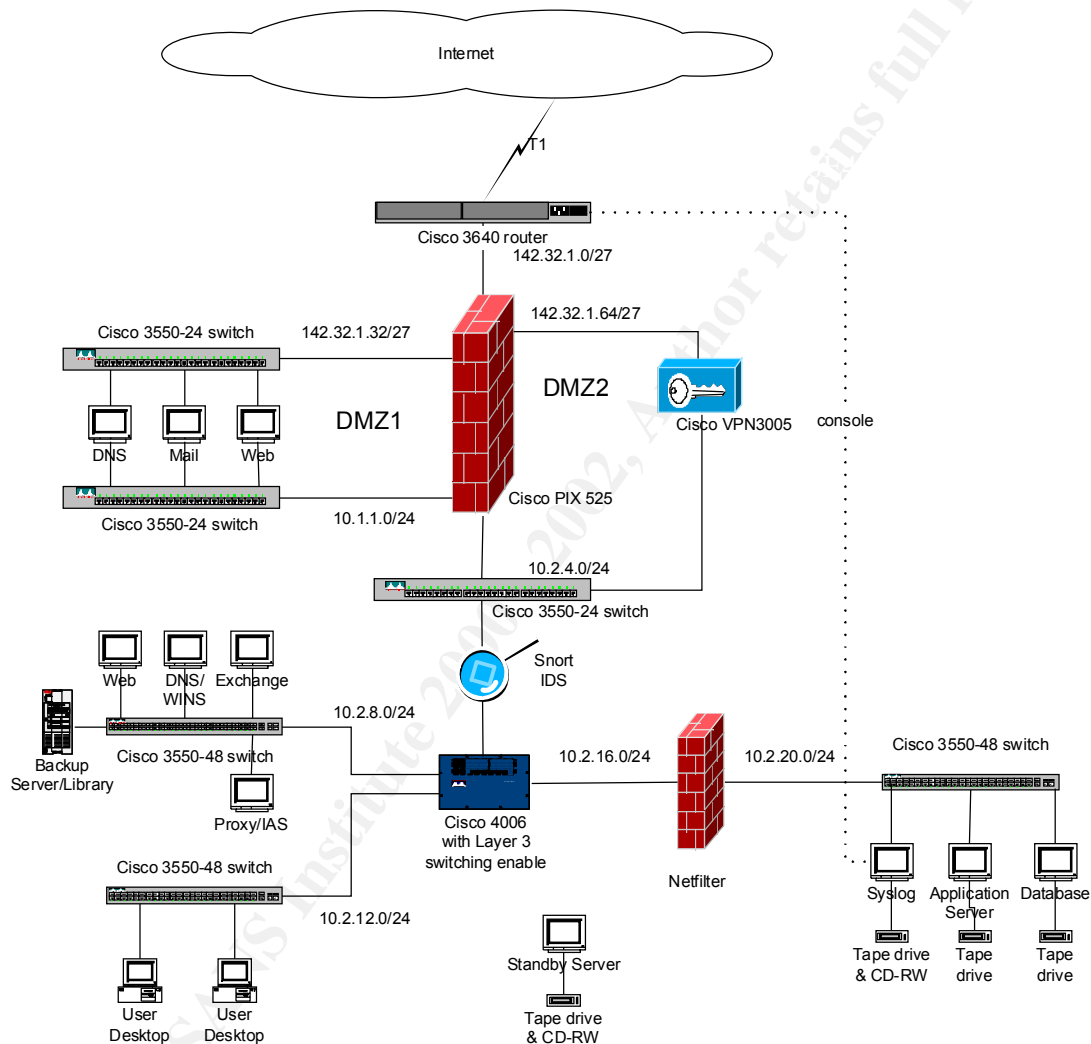
The command `http 1.1 /r/r/w/q` is rejected by the external web server which is expected. The most important is the external web server gives out a banner indicates that the server is using Apache 1.3.23. This information will help an attacker to concentrate his attack on the vulnerabilities of Apache 1.3.23.

### 3.3 Evaluate the audit.

- All PIX rules are function as defined.
- In order to further control firewall responses, we can disable icmp requests and permit unreachable messages at the outside interface.  
**icmp deny any echo-reply outside**  
**icmp permit any unreachable outside**
- Increase firewall redundancy by acquire a second PIX 515E, the redundant PIX is only ¼ of the primary PIX.
- Baseline the traffic pattern for trending analysis and security analysis.
- The Cisco switches in the DMZ are capable to create Private VLAN. Private VLAN is a layer 2 feature that allows one or more ports group together in the same VLAN, traffic from each port is only allowed to communicate with the promiscuous port only (normally one of the firewall interface). It is not allowed to exchange data with other ports even though

they are within the same VLAN. This setup will reduce the risk that a compromised server attacks other system in the same DMZ.

- Two factors authentication can be used for VPN authentication.
- IDS can be used to detect abnormal traffic and inform our security officers. IDS system can be placed as follow diagram.
- Change the banner for the web server in order to slow down the attacker to use the right exploit tools for particular software and its version.



## 4. Design Under Fire

After auditing the firewall rules, GIAC management wants the team to demonstrate the importance of providing a secure network to the corporation. Therefore, the team is going to use the network design from Emily Gladstone [http://www.giac.org/practical/Emily\\_Gladstone\\_GCFW.zip](http://www.giac.org/practical/Emily_Gladstone_GCFW.zip) to demonstrate attack to the firewall, DOS attack and compromise an internal system.

### 4.1 An Attack against the firewall itself

#### 4.1.1 Attack #1

Emily was using Cisco PIX firewall, software version 6.1. Since she did not provide which sub-version of the software that was running, the software may be vulnerable to SNMP attack. Steve Keifling assignment ([http://www.giac.org/practical/Steve\\_Keifling\\_GCFW.doc](http://www.giac.org/practical/Steve_Keifling_GCFW.doc)) has described a way to attack the SNMP vulnerability and I use it to demonstrate and get the same result.

#### 4.1.2 Attack #2

The second attack is reference to CERT vulnerability note VU# 290140 in June 27, 2002 (<http://www.kb.cert.org/vuls/id/290140>) – Multiple Cisco products consume excessive CPU resources in response to large SSH packets.

The advisory describes the impact includes PIX running 6.1.2 or earlier:

Multiple Cisco networking products contain a vulnerability that allows large SSH packets to cause excessive consumption of CPU resources. In some circumstances, this resource consumption may cause the affected device to reboot.

This vulnerability is a side effect of a Cisco patch for VU#13877, an SSH packet injection vulnerability. Please note that this patch does not constrain the integer overflow vulnerability described in VU#945216. However, according to Cisco's Security Advisory, this denial-of-service vulnerability may be triggered by attempts to exploit VU#945216.

Since Emily did not specify the detail of software that her PIX was running, it may be vulnerable to this attack because her configuration allowed SSH protocol in the inside interface. I am going to use the Etherpeek to capture a real SSH session, edit the packet to make it 1500 bytes and multiple fragmented packets. Then use the packet generator feature in Etherpeek to replay the packets to the firewall inside interface.

```
! The PIX CPU utilization before the attack start
testfirewall# sh cpu usage
CPU utilization for 5 seconds = 7% ; 1 minute: 4% ; 5 minutes: 5%
```

```
! After 2 minutes of the attack started.
```

```
testfirewall# sh cpu usage
```

CPU utilization for 5 seconds = 70% ; 1 minute: 65% ; 5 minutes: 39%

Although the attack does not crash the PIX but the CPU utilization dramatically increased.

## 4.2 A denial of service attack

### 4.2.1 Attack #1

50 hosts using cable modem have been compromised in the internet with Tribe Flood Network 2000 (TFN2k) installed. TRN2k can be download from <http://packetstorm.decepticons.org/distributed> (tfn2k.tgz) which can be used to launch TCP/SYN attack to port 80 of our External Web server.

Before launching the attack, we need to create a file to store all the ip address of the compromised hosts. Then the master control PC (my PC) will issue the following command to stimulate the compromised hosts to start the attack to the GIAC External Web server.

```
./tfn -f attackers -i www.giac.com -p 80 -c 5
```

Options:

- f Filename containing a list of hosts with TFN servers to contact
- i Target string
- p A TCP destination port can be specified for SYN floods
- c Command id. 5 is TCP/SYN flood.

After the attack starts, the External web server will experience high CPU consumption, slow response or crash. The attackers (compromised PCs) use tcp port 80 to attack the External Web server which is allowed to pass through the firewall, the number of sessions may be too many for the web server to handle.

There are 2 ways to minimize the impact of this attack:

- When negotiate the contract with the ISP, we can ask the ISP to provide rate-limit on their router for each of the protocol and port number that we specified before forwarding the traffic to our WAN circuit. In order to maximize the benefit of the rate-limit, we need to have a baseline of our requirement.
- Add the following command to the firewall configure to limit the number of concurrent sessions that is allowed to communicate with the External Web server. The following example is using 20 as the maximum concurrent sessions. Again, we need to understand our traffic pattern before we can decide what value will be used.

**Static (dmz, outside) 100.0.0.10 10.3.0.10 netmask 255.255.255.255 20**



### 4.3 An attack plan to compromise an internal system

In view of the DNS's resolver vulnerability describes in CERT Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver, I am going to plan for an attack to the internal DNS server.

#### CERT Advisory Overview

Buffer overflow vulnerabilities exist in multiple implementations of DNS resolver libraries. Operating systems and applications that utilize vulnerable DNS resolver libraries may be affected. A remote attacker who is able to send malicious DNS responses could potentially exploit these vulnerabilities to execute arbitrary code or cause a denial of service on a vulnerable system.

The following steps are my plan:

1. Pretend I am a GIAC customer, call the GIAC sales people instead of visiting their website. Talk to different Sales people and get their email addresses (more than one). In addition, try to find out who is the network specialist in GIAC, his/her email must be using the same format as the sales people.
2. Email an invitation to the network specialist for a network and operating systems survey. In order to attract the network specialist to response, he will be entered to a draw for a \$1000 gift if he completes all the questions. In the survey, there will be questions regarding firewall brand name, server hardware, operating systems and software version. From this survey, I can find out lots of useful information, in particular of what kind of firewall (Cisco PIX), server is Intel based and running RedHat Linux.
3. In September 9, 2002, CERT Advisory's released a revised vulnerability regarding to DNS resolver problem. Since Emily's network was setup in June, most likely, her DNS resolver is vulnerable.
4. Setup an authoritative name server for a domain (attacker.com).
5. Send an email to each of the sales persons and complain about their web site is slow and unable to access, an URL is included and pointed to the attacker.com. In general, sales person has little knowledge or awareness of network security. I bet one of the sales persons will click the URL and Emily's internal DNS will do a lookup for attacker.com.
6. The authoritative server for the attacker.com will send a malformed response to the DNS lookups. When the browser looks up a bad address in the cracker's domain, the browser will be either crashes or hijacked.

The malformed DNS responses look like healthy messages, they will not be detected by IDS. To resolve the problem, upgrade the DNS resolver libraries.

## References:

Improving Security on Cisco Routers

<http://www.cisco.com/warp/public/707/21.html>

Building Bastion Routers with IOS

<http://www.phrack.com/show.php?p=55&a=10>

Router Security Configuration Guide by National Security Agency

<http://nsa1.www.conxion.com/cisco/download.htm>

Top 50 Security Tools

<http://www.insecure.org/tools.html>

Red Hat Linux 7.2

<http://www.redhat.com/docs/manuals/linux/RHL-7.2-Manual/>

Cisco PIX firewall software version 6.2

<http://www.cisco.com/en/US/products/sw/secursw/ps2120/ps3917/index.html>

Cisco PIX Release Notes Version 6.2(1)

[http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod\\_release\\_note09186a00800f1efa.html](http://www.cisco.com/en/US/products/sw/secursw/ps2120/prod_release_note09186a00800f1efa.html)

VPN 3000 Series Client/Concentrators Software Samples and Tips

[http://www.cisco.com/cgi-bin/Support/browse/psp\\_view.pl?p=Hardware:Cisco\\_VPN\\_3000\\_Concentrator&s=Software\\_Configuration](http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Hardware:Cisco_VPN_3000_Concentrator&s=Software_Configuration)

Nmap network security scanner man page

[http://www.insecure.org/nmap/data/nmap\\_manpage.html](http://www.insecure.org/nmap/data/nmap_manpage.html)

SANS Firewalls, Perimeter Protection and VPNs courseware

Reference Sites:

[www.seucurityfocus.com](http://www.seucurityfocus.com)

[www.microsoft.com](http://www.microsoft.com)

[www.cisco.com](http://www.cisco.com)

[www.redhat.com](http://www.redhat.com)

[www.nsa.gov](http://www.nsa.gov)

[www.sans.org](http://www.sans.org)

[www.packetstormsecurity.com](http://www.packetstormsecurity.com)

[www.incidents.org](http://www.incidents.org)

© SANS Institute 2000 - 2002, Author retains full rights.