Global Information Assurance Certification Paper

Practical Assignment
For
GIAC Firewall and Perimeter Protection
SANS Security Conference
New Orleans, LA
January 28 – February 2, 2001

Prepared
By
Richard E. Cockrell

Author: Richard E. Cockrell
Date 03/25/2001
Firewalls, Perimeter Protection and VPNs
GFCW Practical
GIAC Assignment 1 – Security Architecture

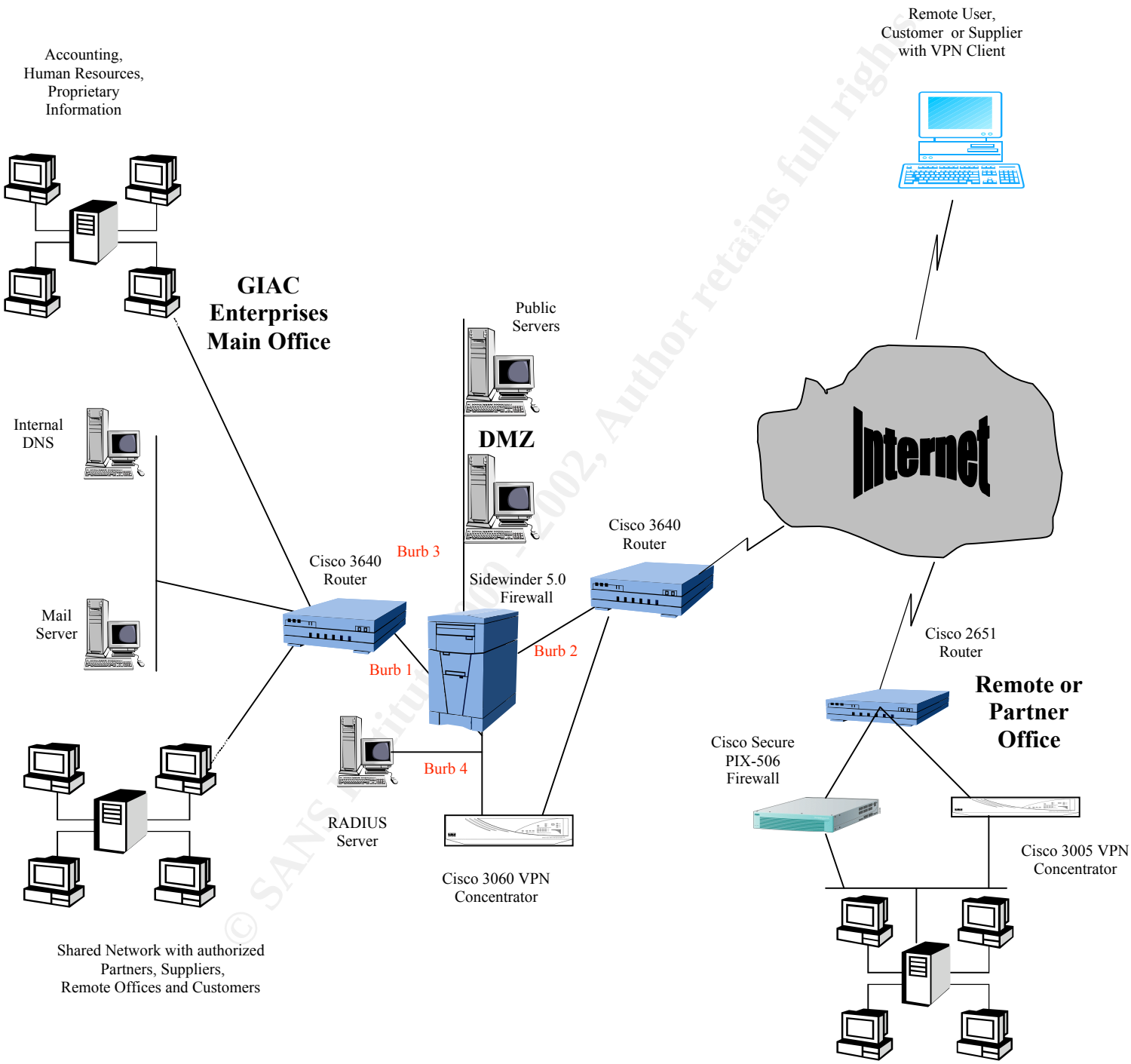
The security architecture of the GIAC Enterprises main office network is a VPN that connects suppliers, partners, customers and remote offices to the GIAC enterprise network. The VPN consists of a Cisco 3060 VPN concentrator at the main office. The Main office will be connected to the Internet via a Cisco 3640 router that will function as the outside perimeter filtering router and connects to the firewall.

The perimeter firewall will be a Secure Computing Sidewinder 5.0 firewall with four burbs. A burb is defined as a NIC on the Sidewinder that is also a separate type enforced network area. Burb 1 will be on the inside or trusted network, burb 2 will be the outside or Internet side, burb 3 will be in the DMZ and contain the public servers, and burb 4 will contain the VPN hardware. Each burb will be on a separate subnet. NAT is enabled on the Sidewinder firewall by default and the only addresses that will be visible on the Internet are the IP addresses on burb 2 and the public servers in burb 3. The firewall is configured for split-DNS, which will prevent anyone from seeing the trusted network.

The internal router will be a Cisco 3640 router, which will separate the GIAC Enterprise internal network into several subnets. One interface links the outside suppliers, partners, remote users and preferred customers to the Shared network. The mail, internal DNS, and other administration servers will be on a network called Admin. The Accounting, Human Resources and other critical applications that require confidentiality will be on a network called Private. The interior router will use access list to separate the Shared network from the Private network.

All access to the GIAC Enterprise network will be via the Internet and through the firewall. No modems or other backdoor connections to the Internet will be allowed inside the trusted networks. Partners and remote offices will be connected to the VPN using LAN to LAN connections. Other users such as suppliers, remote users and preferred customers will be connected using Client agents. The VPN will be authenticated using a Remote Authentication Dial-In User Service (RADIUS) authentication server. RADIUS authentication was chosen because there was an existing RADIUS server in place.

Security Architecture for GIAC Enterprises



Author: Richard E. Cockrell
Date 03/15/2001
Firewalls, Perimeter Protection and VPNs
GFCW Practical
GIAC Assignment 2 – Security Policy

BORDER ROUTER

The border router is the first line of defense of the GIAC Enterprise network. This router lies between the firewall and the Internet Service Provider (ISP). A Cisco 3640 is the border router and will act as screening router for the network. The primary security functions of the screening router are to prevent unauthorized network access, protect against spoofing, and control access to the router

The router must be physically secured. Anyone with physical access to the console port can reboot the router and do a password recovery procedure to take control of the router. The security policy will not allow any permanent hardwired terminal, modem, or terminal server connections to the console port. A password should be configured for the console port, by default there is no password.

Cisco IOS 12.0 will be installed on the routers so that remote connections can be made with Secure Shell (SSH). Unnecessary services that were on by default in Cisco IOS 11.x are now turned off by default in IOS 12.0. Remote access to the router will be made via the five virtual terminals (vty) ports. Remote access will be restricted by IP addresses to the vty ports. The routers will be configured for RADIUS authentication and SSH. Each router will have a warning banner that clearly states that this device is restricted to access by authorized personnel. Access to the routers is controlled by requiring a minimum of a password and username from each person authorized to access the router.

To prevent spoofing of IP addresses block all broadcast packets from external sources. Deny any packets from the Request for Comment (RFC) 1918, Internet Assigned Numbers Authority (IANA) reserved, test, multicast as a source, and loopback, net blocks to block attacks from commonly spoofed IP addresses. Deny first octet zeros, all ones, and loop back network. The IANA reserved three blocks of the IP address space for private intranets, (RFC 1918) block these from entering your router on the outside interface (S1) of the border route. Deny class D (multicast) and class E (reserved for future use). Deny your own IP address space from entering your network from outside.

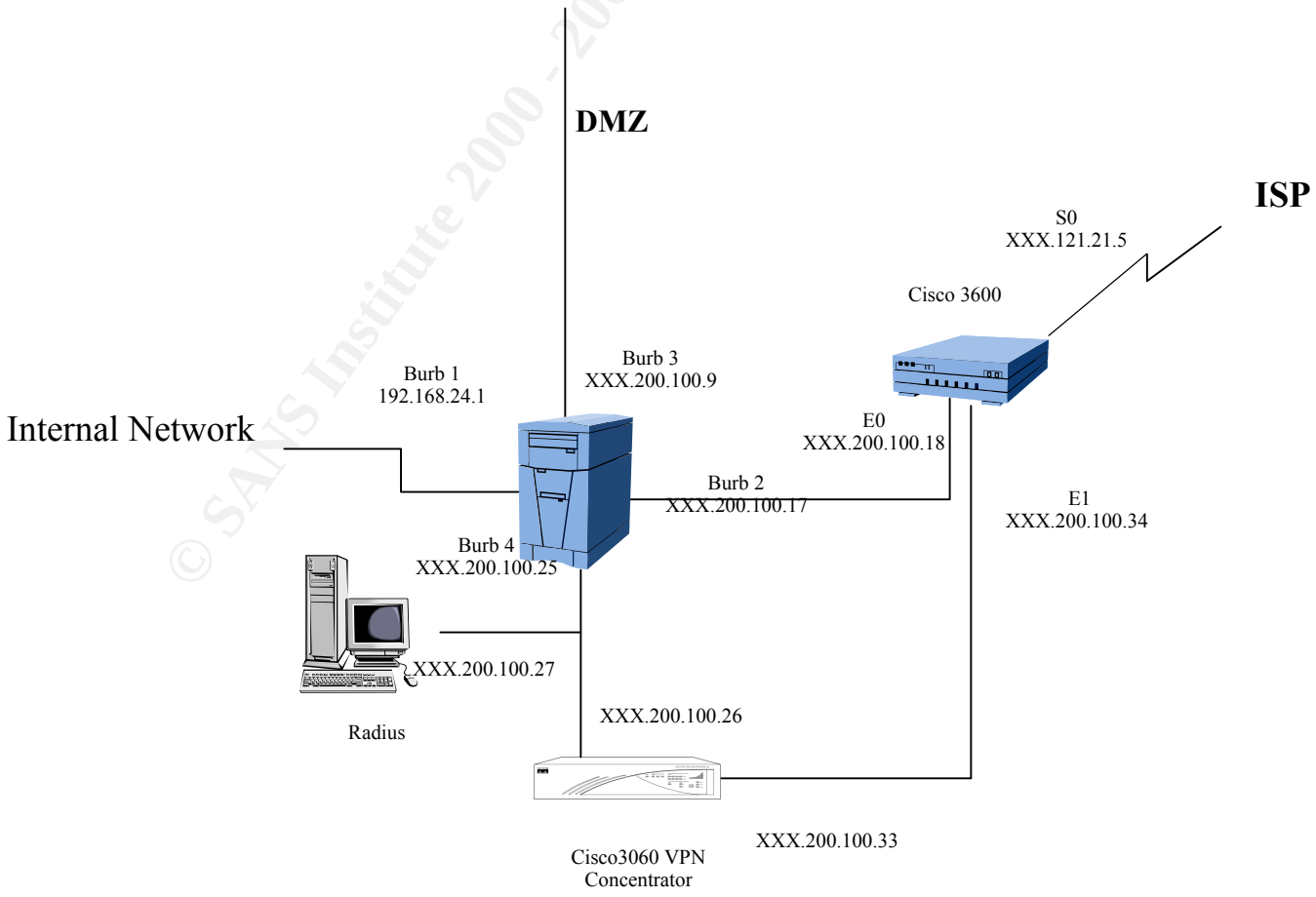
There will be no routing protocol on the border router, all routing is done using static routes. Only radius, radius-acct, L2TP, PPTP, SSH, and ESP protocols are allowed on the VPN network. The Border Router configuration is listed below:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
hostname border
```

```
!
aaa new-model
aaa authentication login default RADIUS local
aaa authentication login line RADIUS
enable secret 5 $1$EybT$oxiXywA2Me3/1/3CFGfdC/
enable password *****
username joeadmin password dsjHENxvjakL
ip subnet-zero
ip ssh time-out 60
ip ssh authentication-retries 5
!
ip subnet-zero
!
interface Ethernet0
 ip address XXX.200.100.18 255.255.255.248
 description to Sidewinder
 no ip directed-broadcast
 no ip route-cache
 media-type 10BaseT
!
interface Ethernet1
 ip address XXX.200.100.33 255.255.255.248
 description to VPN
access-group 102 in
 no ip directed-broadcast
 no ip route-cache
 media-type 10BaseT
 !
interface Serial2
! ip address XXX.121.21.5 255.255.255.252
 description to ISP
 access-group 101 in
 encapsulation ppp
 no ip directed-broadcast
 no ip route-cache
radius-server host XXX.200.100.27 auth-port 1812 acct-port 1813
radius-server key cisco
!
 ! default route goes to ISP
ip route 0.0.0.0 0.0.0.0 XXX.121.21.5
 ! route to Firewall and DMZ
ip route XXX.200.100.8 255.255.255.248 XXX.200.100.17
! route to radius server and VPN
ip route XXX.200.100.24 255.255.255.248 XXX.200.100.33
access-list 101 deny ip XXX.200.100.0 0.255.255.255 any
access-list 101 deny ip 0.0.0.0   0.255.255.255  any
access-list 101 deny ip 255.255.255.255   0.0.0.0  any
access-list 101 deny ip 10.0.0.0   0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.240.255.255 any
access-list 101 deny ip 192.168.0.0   0.0.255.255  any
access-list 101 permit ip any any
access-list 102 permit tcp any any eq 22
access-list 102 permit udp any any eq 1701
access-list 102 permit tcp any any eq 1812
access-list 102 permit udp any any eq 1812
access-list 102 permit tcp any any eq 1813
access-list 102 permit udp any any eq 1813
```

```
access-list 102 permit tcp any any eq 1723
access-list 102 permit udp any any eq 1723
access-list 102 permit 50 any any
access-list 102 permit 51 any any
ip classless
!
line console 0
      login
      password *******
line aux 0
 transport input all
access-list 12 permit 11 XXX.200.100.0 0.255.255.255
      line vty 0 4
      access-class 12 in
banner motd #
**WARNING**WARNING**WARNING**WARNING**

YOU ARE ACCESSING A RESTRICTED DEVICE.  IF YOU ARE NOT AUTHORIZED TO
LOG ONTO THIS DEVICE LOG OFF IMMEDIATELY.

**WARNING**WARNING**WARNING**WARNING**
```

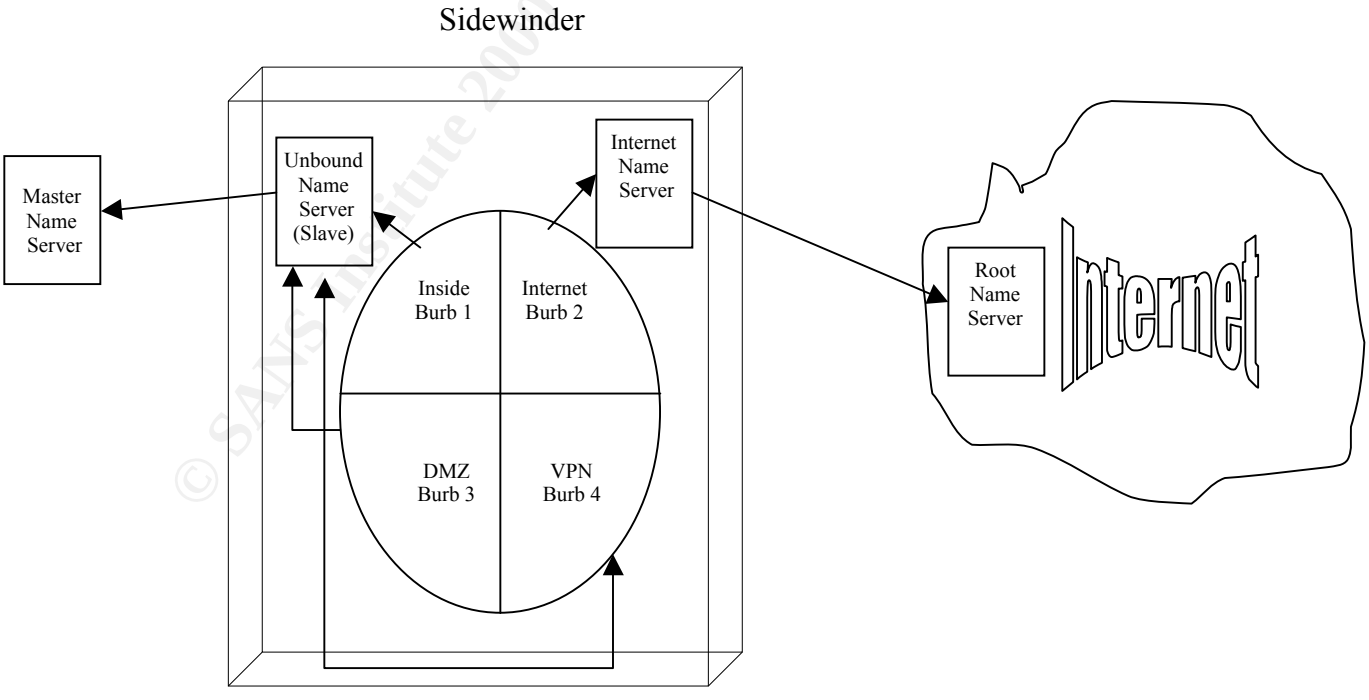
Network Diagram of Border Router, Firewall, VPN Concentrator and RADIUS Server



SIDEWINDER FIREWALL

The firewall will be the main line of defense for the security perimeter. All network traffic that flows from Internet to the trusted network and DMZ will go through the firewall. There will be no backdoors that circumvent the firewall. A Sidewinder 5.0 firewall was selected as the firewall because it uses type enforcement. Type enforcement was developed by the US Government for transferring classified message traffic between the Internet and other classified networks. Type enforcement forbids changes in critical security permissions by establishing mandatory protection. Type enforcement allows Sidewinder to execute standard software in independent compartments and prevents attacks from spreading across the firewall to the trusted network.

The Sidewinder will be configured with two name-servers. One name server is external and is the Internet Name Server. The other name server is internal and is an Unbound Name Server. The only IP addresses that are advertised on the Internet will be the external interface of the Sidewinder and the public servers. Hostnames and IP addresses that are stored in the unbound server are not accessible from the Internet. Damage to the Internet Name Server on burb 2 will not affect the Unbound Name Server on burb 1. No proxy is configured to pass DNS traffic via the firewall. All traffic DNS traffic will be handled by Sidewinders split-DNS.



The Sidewinder uses two UNIX sendmail servers to receive and send mail messages. The GIAC mail server sends all mail to the Sidewinders internal burb where an internal

sendmail server is running. The internal sendmail server uses a Simple Mail Transport Protocol (SMTP) gateway. The internal mail server passes the mail to the external mail server, which are both on the Sidewinder. All mail from the Internet is routed to the external sendmail on Sidewinders external burb. Type enforcement restricts sendmail so that any security flaws in sendmail cannot easily be exploited.

Sidewinder uses the following to criteria to allow or deny a connection:

- The source or destination burb
- The source or destination network object
- The type of connection agent either; Proxy or Server
- The type of network service requested

In order for traffic to go through the firewall all criteria must match.

To configure the Access Control List (ACL) network groups must be defined as one of the following; IP address, Host, Domain, Subnet, or Network group. A network group can consist of several groups. The following Network Groups will be configured:

GROUP	DESCRIPTION
Partners	A group of external Partners by IP Addresses or subnets. Burb 4
Suppliers	A group of external Suppliers by IP Addresses or subnets. Burb 4
Branch_Office	A group of external Branch_Offices by IP Address. Burb 4
Private	A group of internal private systems by subnet. Burb 1
Admin	A group of internal DNS, MAIL, and servers by IP address. Burb 1
Users	A group of internal users by subnet . Burb 1
Remote_User	A group of external GIAC remote users by host name. Burb 4
Customer	A group of external customers by IP address or host name. Burb 4
DMZ	A group of public servers in the DMZ by IP address. Burb 3
VPN	The VPN concentrator by IP address. Burb 4
Shared	A group of internal systems that are shared by the subnet Burb1
Remote_Private	Remote_User and Branch_Office groups
VPN_Users	Partners, Suppliers, Branch_Office, Remote_User, Customer groups

Proxies must also be defined before configuring the ACLs. A proxy is a program that controls communication between clients on one side of a firewall and servers on the other side. This means that the application client and application server on opposite sides of a firewall do not communicate directly. Instead, the client and server both "talk" to a proxy which forwards the data back and forth. Proxies provide additional security.

The following pre-configured proxies will be used:

http tcp/80
https tcp/443
ftp tcp/21
ssh tcp/22

Two proxies will need to be configured. One will control access to the Private GIAC network and the other will control access to the Shared Network. In a real network there would be would several proxies required, one for each service. The following proxies are created:

radius tcp/1812-1813
radius udp/1812-1813
giac tcp/22000-22012
private tcp/10000-10011

The following security policy will be used for creating ACLs on the Sidewinder:

Private, Admin, Users can use http, https, and ftp from burb1 to burb 2.

Admin have access to ssh between burb 2 and burb1.

Everyone has access to https, http, and ftp on burb 3.

VPN_Users group have full access giac services to the Shared network from burb 4 to burb 1.

Remote_Private group have access to private services to the Private group network from burb 4 to burb 1.

Private has will have access to private services access to Remote_Private group from burb 1 to burb 4.

Sidewinder reads the ACL's from top to bottom. This means that the most used ACL's will be placed at the top of the list in order to facilitate traffic flow. There must be a rule that allows the traffic or the packet is dropped at the last line that denies all. Any ACL placed below this line is ignored. By default new ACLs are place at the bottom of the list and must be moved above the deny all statement for the rule to take effect. To determine which order the ACLs should be listed use the following command:

/usr/sbin/gen_reports -r service_traffic

The following output is generated:

```
================================================================
Traffic Summary by Service Thu Mar 12 12:15:52 2001
================================================================
Traffic
summary by service
service    Kbytes read      Kbytes written  total Kbytes  connect
time
http         44.2             92.5           136.7
12:02:37
private      29.8             88.4           117.2
07:43:47
```

```
ftp             78.7            0.0             78.7
01:36:08
giac            86.4            5.4             91.8
01:23:42
ssh              6.4            0.1              6.5
00:00:25
```

This can be only be done after the firewall has been running long enough to gather useful information on how services are being accessed.

The ACLs are configured below:

NO	ENABLE	Name	Action (Deny/ Allow)	Source Burb or Type Enforced Area	Source Network Object	Destination Burb or Type Enforced Area	Destination Network Object	Agent (Proxy, Server, NAS)	Service	Times/ Redirect/ user groups	Description
1	☑	http_out	allow	burb 1	Users	burb 2	*	proxy	http	none	allow internal users to access the web
2	☑	https_out	allow	burb 1	Users	burb 2	*	proxy	https	none	allow https access to all internal users
3	☑	ftp_out	allow	burb 1	Users	burb 2	*	proxy	ftp	none	allow ftp access to all internal users
4	☑	ssh	allow	burb 2	Admin	burb 1	*	proxy	ssh	none	Allow ssh access to Admin Group
5	☑	https_dmz	allow	burb 2	Users	burb 3	DMZ	proxy	https	none	allow https access to DMZ Public Servers from internal users
6	☑	http_dmz	allow	burb 1	Users	burb 3	DMZ	proxy	http	none	allow http access to DMZ Public Servers from internal users
7	☑	ftp_dmz	allow	burb 1	Users	burb 3	DMZ	proxy	hftp	none	allow ftp access to DMZ Public Servers from internal users
8	☑	https_in	allow	burb 2	*	burb 3	DMZ	proxy	https	none	allow https access to DMZ Public Servers from external users
9	☑	http_in	allow	burb 2	*	burb 3	DMZ	proxy	http	none	allow http access to DMZ Public Servers from external users
10	☑	ftp_in	allow	burb 2	*	burb 3	DMZ	proxy	hftp	none	allow ftp access to DMZ Public Servers from external users
11	☑	Giac_services_in	allow	burb 4	VPN_Users	burb 1	VPN	proxy	giac	none	allow giac_services to VPN Users
12	☑	Private_services_in	allow	burb 4	Remote_Private	burb 1	Private	proxy	private	none	allow private_services to Remote_Private users
13	☑	Private_services_out	allow	burb 1	Private	burb 4	Remote_Private	proxy	private	none	allow private_services to Remote_Private users
14	☑	Radius_in	allow	burb 4	Radius	burb 1	VPN_Users	proxy	radius	none	allow radius from outside to inside
15	☑	Radius_out	allow	burb 1	VPN_Users	burb 4	radius	proxy	radius	none	allow radius from inside to outside
16	☑	Deny_in	deny	*	*	*	*	*	all	none	Denies all traffic not defined in the ACLs above

An * is a wildcard that allows all users or burbs that are defined within the burb to use the service.

The next section on Audit Your Security Architecture will explain how to test your ACLs on both the firewall and routers.

The following protocols will not be allowed to cross the security perimeter:

Incoming ICMP

All Routing Protocols, RIP, OSPF, EIGRP…
DNS UDP,TCP/53
SNMP UDP/161,162
POP2 TCP/109
POP3 TCP/110
Finger TCP/79
Rexec TCP/512
Rlogin TCP/513
Rsh TCP/514
Telnet TCP/23
TFTP UDP/69
NetBIOS TCP/137,138,139

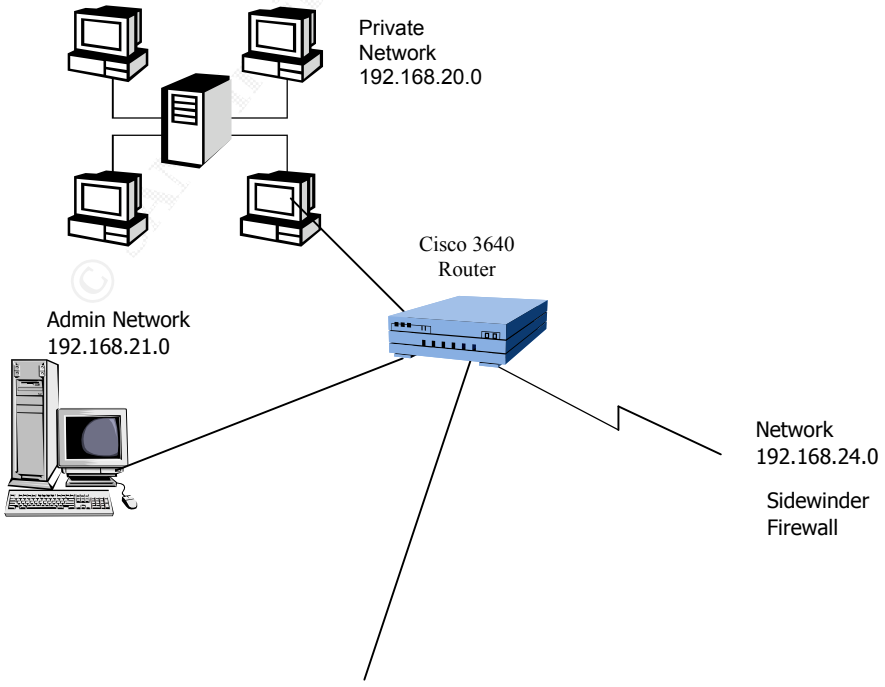
Although these protocols are blocked by the Sidewinder it must be made clear to the Security Administrators that these protocols are not to cross the security perimeter.

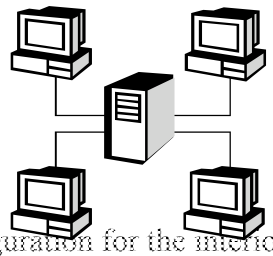
INTERIOR ROUTER

The interior router will be used to protect the Admin and Private network from the shared network. The security policy is as follows:

Deny any traffic from the Shared network to the Private Network, unless the Private network initiates the traffic.
Permit traffic from the Admin network to the Shared network.
Permit traffic from the Admin network to the Private network.
Permit traffic from the Shared to the Private.
Log all violations of the policies above.

See the following diagram:





The router configuration for the interior router follows:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname interior
!
enable secret 5 $1$EybT$oxiXywA2Me3/1/3CFGfdC/
!
ip subnet-zero
!
interface Ethernet0
 ip address 192.168.24.2 255.255.255.0
 description to Sidewinder
 no ip directed-broadcast
 media-type 10BaseT
!
interface Ethernet1
 ip address 192.168.20.1 255.255.255.0
 description to Private
 ip access-group 102 in
 no ip directed-broadcast
 media-type 10BaseT
!
interface Ethernet2
 ip address 192.168.21.1 255.255.255.0
 description to Admin
 no ip directed-broadcast
media-type 10BaseT
!
interface Ethernet3
 ip address 192.168.23.1 255.255.255.0
description to Shared
 no ip directed-broadcast
 media-type 10BaseT
!
 ! default route goes to Sidewinder
ip route 0.0.0.0 0.0.0.0 192.168.20.1

ip classless
!
line console 0
      login
      password *******
line aux 0
 transport input all
access-list 1 permit 192.168.21.0 0.0.0.255
 line vty 0 4
```

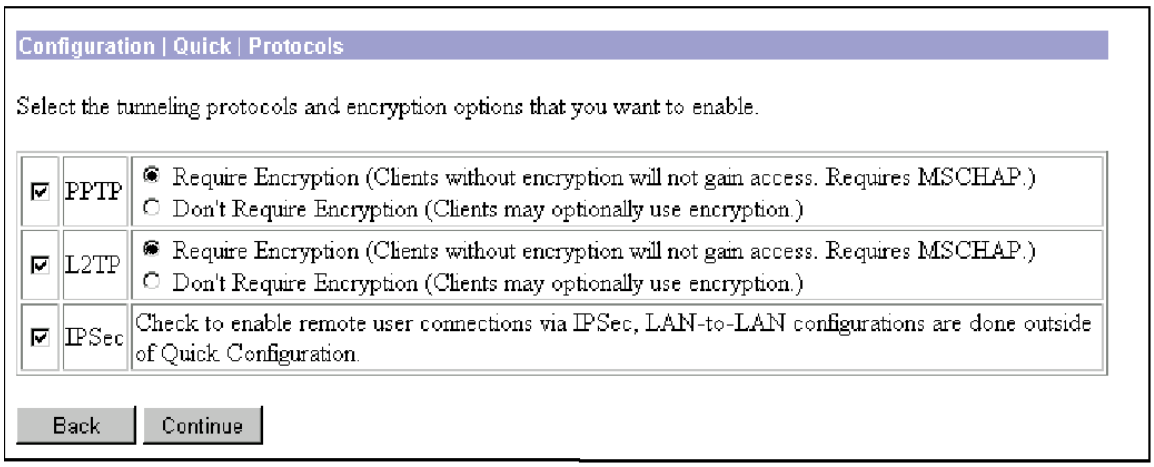
```
 access-class 1 in
!allows incoming TCP traffic if session was initiated from Private
Network
access-list 102 permit tcp any any established
 !Permit Admin Network Access
access-list 102 permit tcp 192.168.21.0 0.0.0.255 any
access-list 102 permit udp 192.168.21.0 0.0.0.255 any
! Permit remote sites access
access-list 102 permit tcp xxx.xxx.xxx.xxx any (Must be a line for
every IP Address and Network that is allowed access)
!log all access list violations
access-list 102 deny ip any any log
!all other sites will be blocked

banner motd #
**WARNING**WARNING**WARNING**WARNING**

YOU ARE ACCESSING A RESTRICTED DEVICE.  IF YOU ARE NOT AUTHORIZED TO
LOG ONTO THIS DEVICE LOG OFF IMMEDIATELY.

**WARNING**WARNING**WARNING**WARNING**
#
```

VPN CONFIGURATION

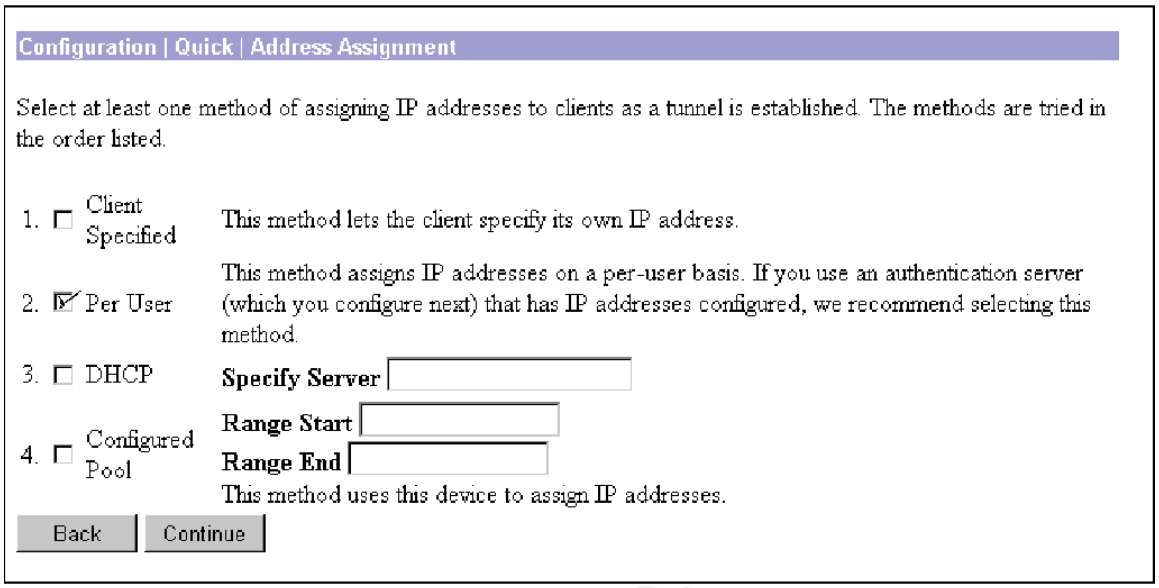
The VPN will be configured using IP Security (IPSec) Protocol for Remote_Private users. These are the users with access to the Private Network. The users will either use Client-to-LAN with Cisco VPN 3000 Client, or LAN-to-LAN, between peer VPN Concentrators. These users will also use Encapsulating Security Payload (ESP) with triple DES encryption. The VPN_users will be allowed to connect to the Shared network with PPTP or LT2P.

A RADIUS server will be used for authentication of both clients and Concentrators. External RADIUS servers can return group and user authentication parameters that match those on the VPN Concentrator.

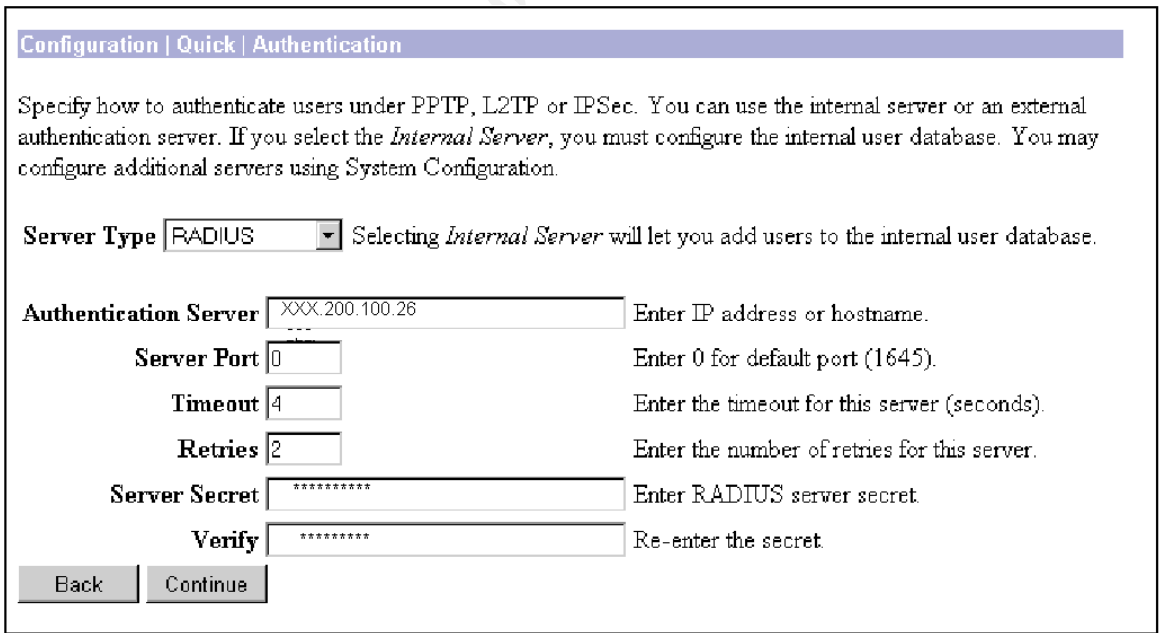
Encryption will be required and the VPN Client will be configured to support PPTP, L2TP and IPSec as follows:



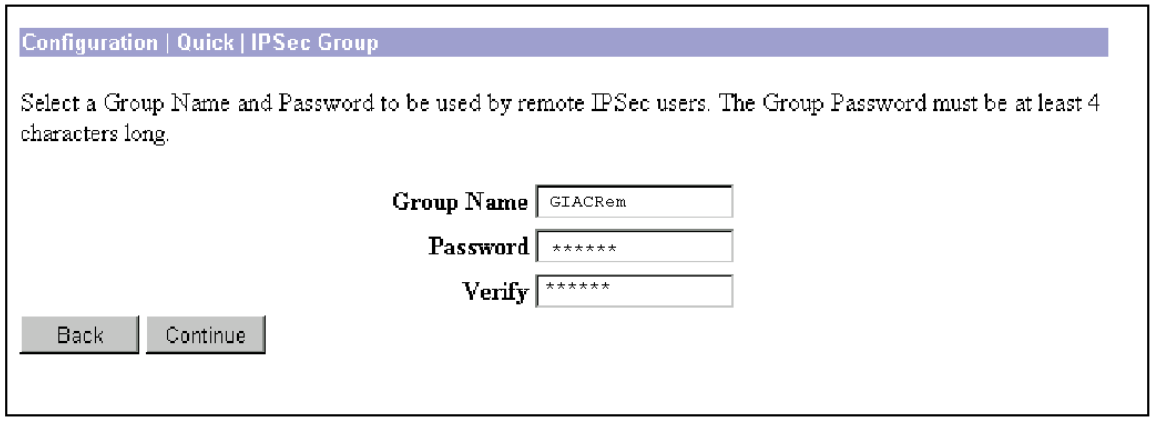
Assigning IP addresses will be based on a per-user basis:



The authentication server will be RADIUS:



Create a GIAC Remote_Private users Group for IPSec:



IPSec parameters will be configured to require Triple-DES authentication, which is the most secure configuration. The next command will set up the Security Association (SA) for the GIACRem group which will be used for users accessing the Private network.

Under **IPSec Parameters > IPSec SA**, select **ESP-3DES-MD5**

Do not check **Allow Password Storage on Client,** so that users must enter the password each time they log in. This option provides greater security.

Each user with access to the Private network will be configured for maximum security and use IPSec to access the VPN. Suppliers, customers and others that access the Shared network will be allowed to access the network by PPTP or L2TP. All users will be authenticated by the RADIUS server.

Author: Richard E. Cockrell
Date 03/15/2001
Firewalls, Perimeter Protection and VPNs
GFCW Practical
GIAC Assignment 3 – Audit Your Security Architecture

Assessing your Perimeter

There are several types of audits to check the security perimeter. The first step is to look at the network design. Does the network design implement the security policy? If yes move to the network implementation. Does the network follow the design? Are there backdoors? Are ACLs enabled on the firewall? Is the traffic to the VPN actually being encrypted? Are administrators using proper procedure? Is physical security being observed? Are the firewall and routers in a controlled area?

The first step of this assessment of this network is an NMAP scan. This will map the network and provide some information on what systems are on the network, what different operating systems are running, and what services are offered. The next step would be an internal audit using a security scanning tool such as, Internet Information Scanner, Nessus, or SARA. This audit is done at a time when network downtime will have minimum impact on the business. A security scanner set in an aggressive mode can bring servers down and deny service to the network. Scanning should be avoided during peak usage of the network. After running a security scanner on the network place sniffers on different locations of the perimeter and analyze real traffic. The final step is to check the Sidewinder audit and mail logs.

Before running a security scanner an NMAP scan should be done first. Source for NMAP material found at http://www.insecure.org. Below is an example of a NMAP SYN or "half-open" scan on a Sidewinder firewall:

```
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (0), OS detection will
be MUCH less reliable Interesting ports on sidewinder-
ext.giac.com (XXX.200.100.17):
(The 1510 ports scanned but not shown below are in state:
filtered)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
102/tcp    open        iso-tsap
110/tcp    open        pop-3
119/tcp    open        nntp
251/tcp    open        unknown
256/tcp    open        rap
443/tcp    open        https
```

```
515/tcp    open        printer
1812/tcp   open        radius
1813/tcp   open        radius-acct

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=4880 (Formidable)
Remote OS guesses: Mac OS X 1.1-1.2 (Rhapsody 5.5-5.6) on a G3,
BSDI BSD/OS 2.0 - 2.1
```

The way you can tell that this box may be a firewall is that the ports that were scanned and not opened are in the filtered state. Note that the OS guesses were wrong. The system is actually running a Secure Computing OS based on a BSD UNIX. Not all ports that are open are identified, because the scanner does not scan all 65536 tcp/udp ports. It only scans ports between 1 to 1024 and any ports listed in the services file that comes with NMAP. There are options that let you set which ports you want to scan.

An NMAP scan of a router looks like this:

```
Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (0), OS detection will
be MUCH less reliable
Interesting ports on (XXX.200.100.18):
(The 1519 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp    open         ssh

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=6640 (Worthy challenge)
Remote OS guesses: AS5200, Cisco 2501/5260/5300 terminal server
IOS 11.3.6(T1), Cisco IOS 11.3 - 12.0(9)
```

By running NMAP scans on the perimeter I have mapped the perimeter devices and determined what ports are opened. NMAP does not normally cause problems with the clients that are being scanned, so it can be used during business hours with due care.

If NMAP is ran on any IP address behind the Sidewinder firewall you will get the following results:

```
Insufficient responses for TCP sequencing (0), OS detection will
be MUCH less reliable Interesting ports on (192.168.21.8):
(The 1510 ports scanned but not shown below are in state:
filtered)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
102/tcp    open        iso-tsap
110/tcp    open        pop-3
119/tcp    open        nntp
251/tcp    open        unknown
```

```
256/tcp    open        rap
443/tcp    open        https
515/tcp    open        printer
1812/tcp   open        radius
1813/tcp   open        radius-acct

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=4880 (Formidable)
Remote OS guesses: Mac OS X 1.1-1.2 (Rhapsody 5.5-5.6) on a G3,
BSDI BSD/OS 2.0 - 2.1
```

The IP address 198.168.21.8 was chosen at random and no system has been assigned that IP address. The Sidewinder will return the same information for any address that is part of the address space defined inside burb 1. The output of this scan matches the output of the external side of the interface without giving the host name. This shows that Sidewinder is shielding the internal servers and hosts.

After running NMAP and determining that all host and services that are on the perimeter are authorized by the GIAC Security Policy it is time to run a security scanner. Nessus will be used to scan the network. Unlike NMAP, Nessus can cause problems when being used. The scanner checks vulnerabilities by trying exploits. This can cause problems on some systems and Nessus should only be used when there are administrators and network technicians that can fix things that get broke. So before you run your first scans have someone present who has access to the systems and can bring them back on line even if it means a full tape restore.

An example of a Nessus scan on a Sidewinder follows:

```
Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 1
Number of security warnings found : 4
Number of security notes found : 1

List of the tested hosts :

     XXX.200.100.17(Security holes found)

XXX.200.100.17:

List of open ports :

          ssh (22/tcp)
          ftp (21/tcp)
          smtp (25/tcp) (Security warnings found)
          domain (53/tcp) (Security warnings found)
          http (80/tcp) (Security hole found)
          general/tcp (Security notes found)
          general/udp (Security notes found)
          unknown (80/tcp) (Security hole found)
```

```
Warning found on port smtp (25/tcp)

The remote SMTP server allows the relaying. This means that
it allows spammers to use your mail server to send their   mails
to the world, thus wasting your network bandwidth.

     Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as
a relay any more.
     CVE : CAN-1999-0512

Warning found on port domain (53/tcp)

     The remote name server allows DNS zone transfers to be
performed. This information is of great use to a cracker who may
use it to gain information about the topology of your network and
spot new targets.

     Solution: Restrict DNS zone transfers to only the servers
that absolutely need it.

     Risk factor : Medium

Information found on port domain (53/tcp)

     The remote bind version is : LOCAL-990324.212218

     Risk factor : Serious
     CVE : CVE-2000-0023

Vulnerability found on port http (80/tcp)

     There is a buffer overrun in the 'cgitest.exe' CGI program,
which will allow anyone to execute arbitrary commands with the
same privileges as the web server (root or nobody).

     Solution : remove it from /cgi-bin.

     Risk factor : Serious

Information found on port general/tcp

     Nmap found that this host is running Mac OS X 1.1-1.2
(Rhapsody 5.5-5.6) on a G3, BSDI BSD/OS 2.0 - 2.1
```


Source for Nessus Scanner material found at http://www.nessus.org

There are reported security holes on port 80 which is HTTP. This is a false positive result. There is no HTTP server enabled on the Sidewinder but there will be Web Servers in the DMZ that use port 80. It is very important that the Web Servers are running the latest security patches and administrators keep current on any new vendor patches. There will always be security warnings if you are running protocols such as smtp, http, and DNS. These ports must be open to run mail, web servers and access the Internet. The way Sidewinder handles the mail and DNS minimizes the risk to the internal network.

The web servers are located in the DMZ where they are segregated from the production network, this also minimizes risk. No network will ever be risk free, but with adequate safeguards and attentive administrators, risk can be greatly reduced.

One of the easiest ways to audit Sidewinder is to check the Sidewinder logs. All ACL violations, attack attempts and bad proxy authentications are logged. Alarms can be enabled to notify the firewall administrator if certain thresholds of audit events are exceeded. To see network probes as they occur, type the following command:

```
tail –f /var/log/audit.network.probe.raw | act –a
```

To check the mail flow through Sidewinder type:

```
tail –20/var/log/maillog
```

To check traffic flow type:

```
tail –f/var/log/audit.asc
```

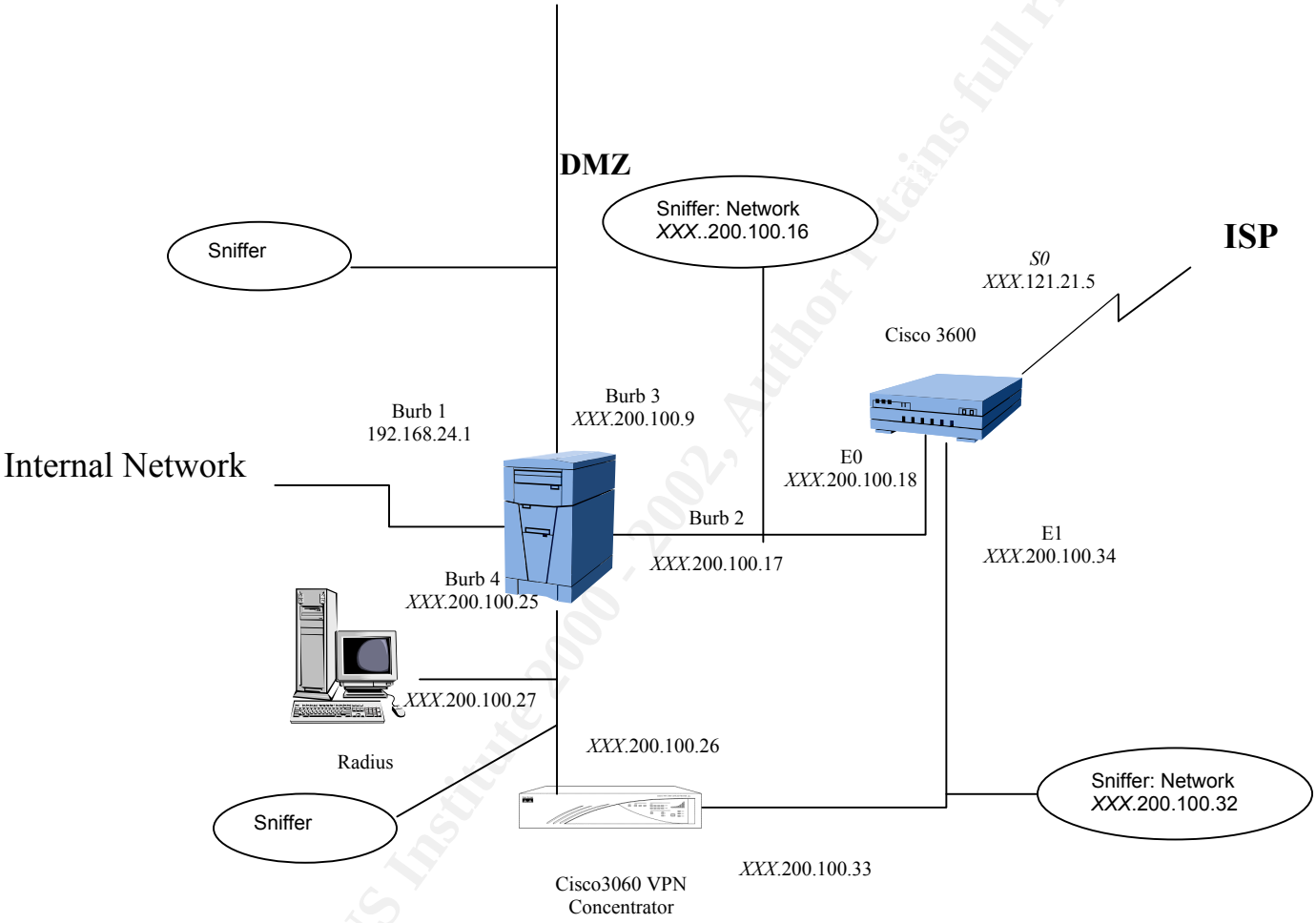
The review of audit log and mail files should occur daily on the Sidewinder. These logs will tell an experienced administrator almost everything that is occurring on the firewall.

The next step of the audit will be to use sniffer software to see what traffic is actually on the network. This can be done by inserting a sniffer like Etherpeek or using tcpdump on a shared media hub and looking at all the traffic on a segment. Collect the information and then analyze it to make sure only authorized traffic is being allowed on the proper subnet. If http traffic is occurring on *XXX*.200.200.32 network, or PPTP is occurring in the *XXX*.200.100.16 network, something is wrong with the implementation of the network. Sniffing the network is passive and can be done at different times of the day and night. Using tcpdump on a Linux system type:

```
tcpdump > dataname
```

The information from tcpdump can verify that the only services running on different network segments are legitimate and authorized traffic according to the Security Policy. Sniffers can be configured to run for a few minutes each hour and thus collect a good sampling of data over several days. From these samples traffic can be analyzed and the network administrators should have a good baseline of the network.

For placement of the sniffers on a network see the following diagram:



After an Internal audit has been performed it is always a good idea to bring in outside auditors to make sure the organization has not missed any obvious security flaws. Outsiders often see things that insiders never though about or even guessed could be a security problem.

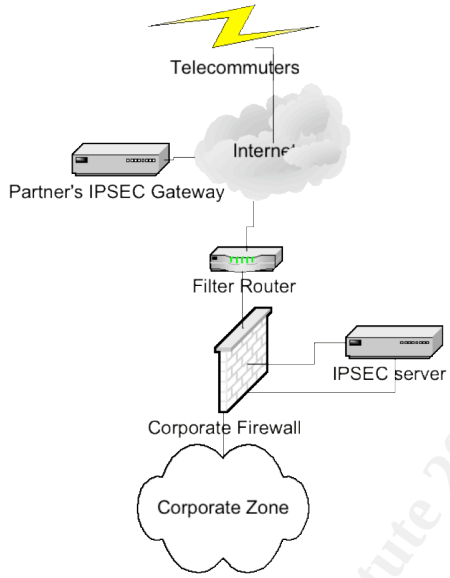
Author: Richard E. Cockrell
Date 03/15/2001
Firewalls, Perimeter Protection and VPNs
GFCW Practical
GIAC Assignment 4 – Design Under Fire

Attack Against Firewall

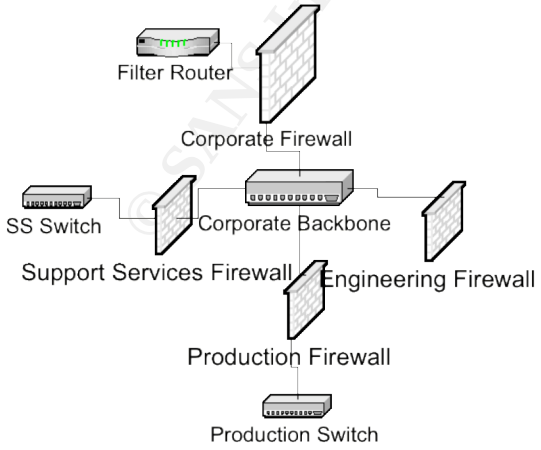
I will be putting the design of Jeremy Brown under fire. The design is located at:

http://www.sans.org/giactc/gcfw.htm (Jeremy_Browns_GCFW)
0096, Jeremy Browns, 9 February 2005

Perimeter Network



Internal Network



The corporate firewall is a Cisco PIX and version of the software is unknown with several FW-1 inside the network. The attack will concentrate on the perimeter PIX firewall.

Some recent vulnerabilities PIX from www.cisco.com:

Cisco Security Advisory: Cisco Secure PIX Firewall Mailguard Vulnerability

```
Revision 1.1

Updated, for public release 2000 October 5 04:00 PM US/Pacific
(UTC+0700)
```

Impact

The Mailguard feature is intended to help protect weakly secured mail servers. The workaround for this issue is to secure the mail servers themselves, or upgrade to fixed PIX firewall code.

In order to exploit this vulnerability, an attacker would need to also exploit the mailserver that is currently protected by the PIX. If that server is already well configured, and has the latest security patches and fixes from the SMTP vendor, that will minimize the potential for exploitation of this vulnerability.

The vulnerability was found at:

http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml

Cisco Secure PIX Firewall FTP Vulnerabilities

Revision 1.7
For public release 2000 June 27 12:30 PM US/Pacific (UTC+0800)

Summary

The Cisco Secure PIX Firewall interprets FTP (File Transfer Protocol) commands out of context and inappropriately opens temporary access through the firewall. This is an interim notice describing two related vulnerabilities.

The first vulnerability is exercised when the firewall receives an error message from an internal FTP server containing an encapsulated command such that the firewall interprets it as a distinct command. This vulnerability can be exploited to open a separate connection through the firewall. This vulnerability is documented as Cisco Bug ID CSCdp86352.

The second vulnerability is exercised when a client inside the firewall browses to an external server and selects a link that the firewall interprets as two or more

FTP commands. The client begins an FTP connection as expected and at the same time unexpectedly executes another command opening a separate connection through the firewall. This vulnerability is documented as Cisco Bug ID CSCdr09226.

Either vulnerability can be exploited to transmit information through the firewall without authorization.

Both vulnerabilities are addressed more completely in this updated interim security advisory.

The vulnerability was found at:

http://www.cisco.com/warp/public/707/pixftp-pub.shtml

To exploit this vulnerability go to http://www.monkey.org/~dugsong/. At this web site, there are firewall penetration tools such as tp-ozone, ftpd-ozone, that can be used to exploit this PIX vulnerability.

Another vulnerability was posted by Eric Budke on Bugtraq :

```
-----Original Message-----
From: Eric Budke [mailto:budke@budke.com]
Sent: Wednesday, March 03, 1999 5:11 PM
To: firewall-wizards@nfr.net
Subject: Pix crashing with ISS snmp checks


I'm trying to track down version numbers for this, but it appears
that with ISS 5.6.2 in the snmp check section that we
successfully killed a pix router (the OS version is in question).

Is there a habit of this happening? We weren't running DOS
checks, and I haven't been able to try other snmp checks against
it...client is a little hesitant until after their post-mortem.

Thanks.

-Eric
--
PGP Key can be found at
http://www.panix.com/~budke/pgp/budke_budke_com.txt
```

From the information obtained there are several ways to mount Dos attacks on a PIX Firewall.

The attack against the PIX Firewall will be a Syn Flooding type of attack using Synk4. The Synk4 code can be found at:

http://www.AntiOnline.com/cgi-bin/anticode/anticode.pl?dir=denial-of-service/syn-flooders

The Synk4 will be compiled on a Linux operating system. The attack should cause a DoS on the PIX. The following is from:

Pietrosanti, Fabio "*Firewall syn flood * EASY DOS WITH PIX*", 9 Mar 2001. URL: http://www.securityfocus.com/archive/1/168176:

> *With only 307 syn we made an efficient Syn Flood and Cisco PIX didn't manage it and the service go down.*
>
> *Sure, no SYN packets are received by 192.168.3.3 due to his "tcp intercept" feature: it makes a connection with the internal server only after the 3way handshake and thus the connection is completed. Syn flood protection doesn't work .*
>
> *Now we have either to wait for default 5 minutes timeout or we have to make a clear xlate to TearDown all connection and cleanup the PIX Connection Table .*
>
> *I think that everyone with a 14.4 modem could do a successfull syn flood against server "protected" by the pix.*

The attack was against a Web Server that was placed behind the PIX and the DoS was easily accomplished. This attack will take the server behind the firewall down in a few seconds.

Countermeasures of DoS

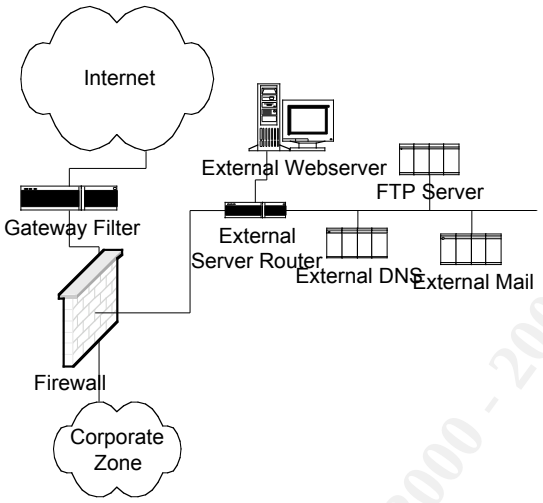
Several countermeasures can be put in place to stop a DoS attack or least mitigate the damage caused by an attack. On way to minimize DoS attacks is for all networks to prevent spoofing. This is done at the border router and blocks all internal to external traffic from passing through the router unless the IP address is a legitimate address from the internal network. This requires that all network administrators and ISPs cooperate. This is not likely to happen anytime in the near future.

If you have 50 systems flooding your network with TCP SYN, UDP or ICMP floods, you must have some way of blocking each attacking machine. A good IDS (Intrusion Detection System) should give you this option. There are several IDS systems on the market including, Cisco Secure IDS, SAFEsuite by Internet Security Systems, and Real Time Intrusion Detection by IBM. The IDS will also give you information on who is attacking your network so that the attacking systems can be blocked or shutdown. Most of the systems will have administrators or users that are unaware that their system is being used in a DoS attack.

The Cisco Secure IDS 4230 will be used because most of the perimeter hardware is Cisco and this IDS can mount proactive defense of the network. The system includes the capability to monitor the perimeter and looks for; exploit activity, DoS attacks, network mapping attempts, and internal misuse of the network. The system can also be configured to modify ACLs on Cisco routers to block certain traffic that is being used to mount a DoS attack. The Cisco Secure IDS also provides for centralized management and remote monitoring. The information is gathered by Cisco Secure IDS and used to consolidate management the security perimeter.

Attack on Internal System

To attack an internal system I would choose an attack on the External Mail Server.



The Corporate Zone of the network has additional protection of FW-1 firewalls so I would attempt to penetrate the DMZ and the external servers. A successful attack on one of these systems may lead to a successful attack on the Corporate Zone. Attacking the external mail server gives us a chance to pass Trojan packages inside the network via the external mail server. The vulnerability we will use is the **Cisco Secure PIX Firewall Mailguard Vulnerability**, which is recent enough so that there will be many systems that have not been patched.

To exploit this vulnerability use the directions on the following exploit on an email sent by Lincoln Yeoh, with the subject "Out of order SMTP DATA commands incorrectly allow pass-through mode in some firewall smtp filters/proxies.", that was posted on Bugtraq on 9 Jul 2000.

> *Basically if you wish to send arbitrary stuff to a mailserver protected by a vulnerable firewall's smtp proxy, what you do is send a DATA command followed by the stuff you want to send, all in the same tcp/ip packet, immediately on connection (before you even get the 220 response).*

e.g.
<begin packet>
DATA
VERB
EXPN postmaster
.
<end packet>

You may have to send consecutive DATA commands to get it to work
e.g
<begin packet>
DATA
DATA
VERB
EXPN postmaster
.
<end packet>

Note: In some versions you require the end . to receive the response.

If this exploit works on the mail server, an attempt to plant a Trojan via this system to the inside of the Corporate networks. Some type of buffer overflow may allow us to gain root access on a UNIX system, permitting us to grab the /etc/passwd and /etc/shadow files.

Reference Material:

Kaeo, Merike. Designing Network Security, Indianapolis: Macmillan Technical Publishing, 1999

Wait, John. Cisco IOS 12.0 Network Security, Indianapolis, Cisco Systems, Inc., 1999

Leinward, Allan. Cisco Router Configuration. Indianapolis: Macmillan Technical Publishing, 1998

Sidewinder Administration Guide, San Jose. Secure Computing Corp, 2000

Smith, E. Richard. "Sidewinder: Defense in Depth using Type Enforcement", 26 July 2000. URL: http://www.securecomputing.com/pdf/type_enforcement_wp.pdf

"3000 Concentrator Series User Guide." Jan 8, 2001. URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/vpn3kco/vcoug/usrguide/index.htm

"VPN Concentrator Getting Started Guides." July 2000. URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/vpn3kco/vcogs/index.htm

"Cisco Secure Intrustion Detection Family, Data Sheet." Oct 18, 2000. URL: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/idsf_ds.htm